Defense Acquisition Guidebook

Production Date:16-September-2013

DEFENSE ACQUISITION GUIDEBOOK -
Foreword

The Defense Acquisition System exists to manage the Nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces. In that context, our objective is to acquire quality products that satisfy user needs with measurable improvements to mission capability at a fair and reasonable price. The fundamental principles and procedures that the Department follows in achieving those objectives are described in DoD Directive 5000.01 and DoD Instruction 5000.02 .

The Defense Acquisition Guidebook is designed to complement those policy documents by providing the acquisition workforce with discretionary best practice that should be tailored to the needs of each program.

Acquisition professionals should use this Guidebook as a reference source supporting their management responsibilities. As an "on-line" resource, the information is limited only by the users interest or need. Some chapters contain general content; they provide individual topic discussions and describe processes and considerations that will improve the effectiveness of program planning. Some chapters may provide a tutorial on the application of these topics to the acquisition framework. Depending on the subject matter, a chapter may contain general background information, tutorial discussions, and/or discussions of the detailed requirements for each milestone decision and phase. All chapters contain non-mandatory staff expectations for satisfying the mandatory requirements in DoD Instruction 5000.02.

Each chapter is designed to improve understanding of the acquisition process and ensure adequate knowledge of the statutory and regulatory requirements associated with the process. Discussions, explanations, and electronic links to related information enable the "reader" to be efficient, effective, innovative, and disciplined, and to responsively provide warfighting capability. Each chapter lists potential ways the program manager or assigned manager can satisfy mandatory process requirements and meet staff expectations for other activities. Differences of view regarding discretionary practice will be resolved by the Milestone Decision Authority.

The Guidebook is intended to be an electronic reference source rather than a "book." The "reader" "navigates" the information instead of "leafing" through hundreds of physical, collated pages. "Navigation" is electronic movement through the reference system.

Chapter 1, Department of Defense Decision Support Systems , presents an overview of the Defense Department's decision support systems for strategic planning and resource allocation, the determination of capability needs, and the acquisition of systems.

Chapter 2, Program Strategies , provides information and guidance needed to develop a Technology Development Strategy and to develop and maintain a program-level

Acquisition Strategy.

Chapter 3, Affordability and Life-cycle Resource Estimates, addresses acquisition program affordability and resource estimation and describes the concept of program life-cycle cost and the processes for conducting Analysis of Alternatives. The chapter discusses specific milestone review procedures, expectations, and best practices for a variety of topics related to acquisition program affordability, cost, and manpower. The chapter further describes the role of both DoD Component cost estimates and independent cost estimates in support of the DoD acquisition system.

Chapter 4, Systems Engineering, outlines DoD guidance on systems engineering, and explains expectations for completing the Systems Engineering Plan (SEP). The chapter describes standard systems engineering processes and how they apply to the DoD acquisition system. It addresses the systems engineering principles that a program manager should apply to achieve a balanced system solution.

Chapter 5, Life-cycle Logistics, provides the associated guidance the Program Manager (PM), Product Support Manager (PSM), and Life-Cycle Logisticians can use in influencing the design and providing effective product support.

Chapter 6, Human Systems Integration, addresses the human systems elements of the systems engineering process. It will help the program manager design and develop systems that effectively and affordably integrate with human capabilities and limitations; and it makes the program manager aware of the staff resources available to assist in this endeavor.

Chapter 7, Acquiring Information Technology, Including National Security Systems, explains how the Department of Defense complies with statutory and regulatory requirements for acquiring Information Technology and National Security Systems and in using a network-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter also provides descriptions and explanations of the Clinger-Cohen Act and many other associated topics and concepts, and discusses many of the activities that enable the development of net-centric systems.

Chapter 8, Intelligence Analysis Support to Acquisition, provides information to enable the program manager to use intelligence information and data to ensure maximum war-fighting capability at the minimum risk to cost and schedule.

Chapter 9, Test and Evaluation, supplements direction and instruction in DoDD 5000.01 and DoDI 5000.02 with processes and procedures for planning and executing an effective and affordable T&E program in the DoD acquisition model. The chapter is designed to assist the program manager in the development of a robust, integrated, and effective test and evaluation strategy to assess operational effectiveness and suitability, and to support program decisions.

Chapter 10, Decisions, Assessments, and Periodic Reporting, discusses major

program decisions and tailoring based on program type and acquisition category, executive-level decision forums and the tenets and processes of Integrated Product Teams (IPTs), program assessments, and periodic reporting. Additional chapter topics include exit criteria, independent assessments, Acquisition Baseline Plan development and management, and periodic reports for Major Acquisition Programs and Major Automated Information Systems programs. The chapter also addresses Should-Cost with a focus on controlling the cost of the actual work that the Department is doing and expects to do.

Chapter 11, Program Management Activities , explains the additional activities and decisions required of the program manager, not otherwise discussed in other chapters of this Guidebook.

Chapter 12, Business Capability Life Cycle , provides guidance for executing the Business Capability Lifecycle (BCL) and acquisition of defense business systems (DBS). BCL is the overarching framework for the planning, design, acquisition, deployment, operations, maintenance, and modernization of DBS.

Chapter 13, Program Protection , provides guidance and expectations for the major activities associated with Program Protection.

Chapter 14, Acquisition of Services , provides acquisition teams with a disciplined, three-phase, seven step process, for the acquisition of services.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 1 -- Department of Defense Decision Support Systems

1.0. Overview

1.0.1. Purpose

This chapter provides background information about the environment in which the Department of Defense must operate to acquire new or modified materiel or services.

1.0.2. Contents

Section 1.1 presents an overview of each of the three, principal, decision support systems used in the Department of Defense to acquire materiel and services, and describes the integration of those systems. Sections 1.2 through 1.4 provide details of each of these systems: Section 1.2 discusses the Planning, Programming, Budgeting, and Execution process, employed by the Department of Defense to conduct strategic planning and make resource allocation decisions; Section 1.3 discusses the Joint Capabilities Integration and Development System used to determine military capability needs; and Section 1.4 discusses the formal Defense Acquisition System used to acquire that capability.

1.1. Integration of the DoD Decision Support Systems

The Department of Defense has three principal decision-making support systems, all of which have been significantly revised over the past few years. These systems are the following:

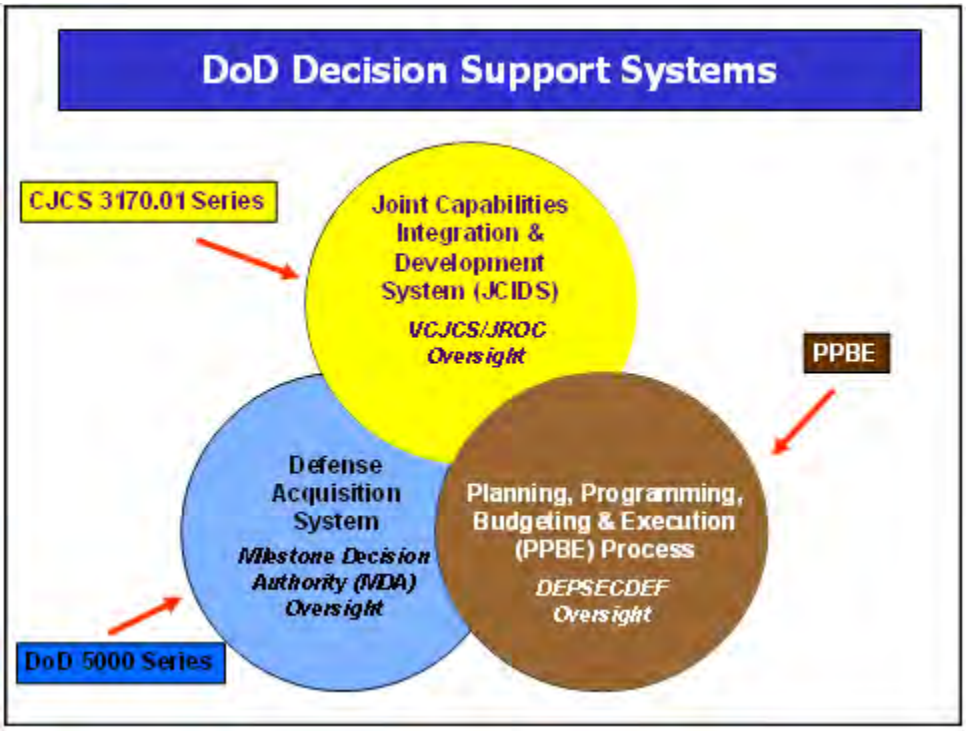
Planning, Programming, Budgeting and Execution (PPBE) Process - The Department's strategic planning, program development, and resource determination process. The PPBE process is used to craft plans and programs that satisfy the demands of the National Security Strategy within resource constraints.

Joint Capabilities Integration and Development System (JCIDS) - The systematic method established by the Chairman of the Joint Chiefs of Staff for identifying, assessing, and prioritizing gaps in joint warfighting capabilities and recommending potential solution approaches to resolve these gaps. CJCS Instruction 3170.01 and the JCIDS Manual describe the policies and procedures for the requirements process.

Defense Acquisition System - The management process by which the Department acquires weapon systems, automated information systems, and services. Although the system is based on centralized policies and principles, it allows for decentralized and streamlined execution of acquisition activities. This approach provides flexibility and encourages innovation, while maintaining strict emphasis on discipline and accountability.

Illustrated together in Figure 1.1.F1, the three systems provide an integrated approach to strategic planning, identification of needs for military capabilities, systems acquisition, and program and budget development. The next three sections provide brief introductions to each of these decision support systems.

Figure 1.1.F1. DoD Decision Support Systems



1.2. Planning, Programming, Budgeting and Execution (PPBE) Process

1.2. Planning, Programming, Budgeting and Execution (PPBE) Process

The purpose of the PPBE process is to allocate resources within the Department. It is important for program managers and their staffs to be aware of the nature and timing of each of the events in the PPBE process, since they may be called upon to provide critical information that could be important to program funding and success.

In the PPBE process, the Secretary of Defense establishes policies, strategy, and prioritized goals for the Department, which are subsequently used to guide resource allocation decisions that balance the guidance with fiscal constraints. The PPBE process consists of four distinct but overlapping phases:

Planning. The planning phase of PPBE is a collaborative effort by the Office of the Secretary of Defense and the Joint Staff, in coordination with DoD components. It begins with a resource-informed articulation of national defense policies and military strategy known as the Defense Planning Guidance (DPG). The DPG is used to lead the overall planning process.

Programming. The programming phase begins with the development of a Program Objective Memorandum (POM) by each DoD Component. This development seeks to construct a balanced set of programs that respond to the guidance and priorities of the DPG within fiscal constraints. When completed, the POM provides a fairly detailed and comprehensive description of the proposed programs, including a time-phased allocation of resources (forces, funding, and manpower) by program projected five years into the future. In addition, the DoD Component may have the opportunity to describe important programs not fully funded (or not funded at all) in the POM, and assess the risks associated with the shortfalls. The senior leadership in OSD and the Joint Staff, and Combatant Commands review each POM to help integrate the DoD Component POMs into an overall coherent defense program. In addition, the OSD staff ,the Joint Staff, and Combatant Commands can raise issues with any section of a POM and propose alternatives with adjustments to resources. Proposed programmatic changes are presented to the leadership for review, and decisions are documented in the Resource Management Decision (RMD) document. DoD Components use the RMD to update their POM data sets which are then incorporated into the Departments Budget and Future Years Defense Program (FYDP) and submitted to the Office of Management and Budget (OMB) as part of the President's budget request.

Budgeting. The budgeting phase of PPBE occurs concurrently with the programming phase; each DoD Component submit' s it's proposed Budget Estimate Submission (BES) simultaneously with its POM. The budget converts the programmatic view into the format of the congressional appropriation structure, along with associated budget justification documents. The budget is focused on one year, but with considerably more financial details than the POM. Upon submission, each budget estimate is reviewed by analysts from the office of the Under Secretary of Defense (Comptroller) and OMB.

Their review ensures that programs are funded in accordance with current financial policies, and are properly and reasonably priced. Proposed budget changes are presented to leadership for review and decisions are documented in the Resource Management Decision (RMD) document. DoD Components use the RMD to update their BES data sets which are then incorporated into the Departments Budget and FYDP and submitted to OMB as part of the President's budget request.

Execution. The execution review occurs simultaneously with the program and budget reviews. The execution review provides feedback to the senior leadership concerning the effectiveness of current and prior resource allocations. Metrics are used to support the execution review to measure actual output versus planned performance for defense programs. To the extent performance goals of an existing program are not being met, the execution review may lead to recommendations to adjust resources and/or restructure programs to achieve desired performance goals.

1.3. Joint Capabilities Integration and Development System (JCIDS)

1.3. Joint Capabilities Integration and Development System (JCIDS)

JCIDS plays a key role in identifying the capabilities required by the warfighters to support the National Security Strategy, the National Defense Strategy , and the National Military Strategy. Successful delivery of those capabilities relies on the JCIDS process working in concert with other joint and DOD decision processes. JCIDS procedures support the Chairman and Joint Requirements Oversight Council (JROC) in advising the Secretary of Defense on identifying and assessing joint military capability needs. JCIDS is a joint-concepts-centric capabilities identification process that allows joint forces to meet future military challenges. The JCIDS process assesses existing and proposed capabilities in light of their contribution to future joint concepts. The JCIDS process was created to support the statutory requirements of the JROC to validate joint warfighting requirements. JCIDS is also a key supporting process for the DOD acquisition and Planning, Programming, and Budget Execution (PPBE) processes . The primary objective of the JCIDS process is to ensure the capabilities required by the joint warfighter to successfully execute the missions assigned to them are identified with their associated operational performance criteria. This is done through an open process that provides the JROC the information they need to make decisions on required capabilities. The requirements process supports the acquisition process by providing validated capability needs and associated performance criteria to be used as a basis for acquiring the right weapon systems. Additionally, JCIDS provides the PPBE process with affordability advice supported by the capabilities-based assessment (CBA) , and identifies capability gaps and potential materiel and non-materiel solutions. While it considers the full range of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) solutions, for purposes of this Guidebook, the focus is on the pursuit of "materiel" solutions.

JCIDS acknowledges the need to project and sustain joint forces and to conduct flexible, distributed, and highly-networked operations. JCIDS is consistent with DoD

Directive 5000.01 direction for early and continuous collaboration throughout the Department of Defense. JCIDS implements a capabilities-based approach that leverages the expertise of government agencies, industry, and academia. JCIDS encourages collaboration between operators and materiel providers early in the process. JCIDS defines interoperable, joint capabilities that will best meet the future needs. The broader DoD acquisition community must then deliver these technologically sound, sustainable, and affordable increments of militarily useful capability to the warfighters.

JCIDS informs the acquisition process by identifying and assessing joint military capability needs which need a materiel solution; these identified capability needs then serve as the basis for the development and production of acquisition programs. JCIDS is fully described in CJCS Instruction 3170.01 , signed by the Director of the Joint Chiefs of Staff. This instruction establishes the policies for JCIDS, and provides a top-level description of the process. A supplementary on-line manual, the JCIDS Manual , provides the details necessary for the day-to-day work in identifying, describing, and justifying joint warfighting capabilities. The manual also includes the formats that describe the content required for each JCIDS document.

For major defense acquisition programs or major automated information systems subject to OSD oversight, the products of the Joint Capabilities Integration and Development System process directly support the Defense Acquisition Board (DAB) in advising the Milestone Decision Authority for major milestone decisions. Figure 1.3.F1 is a simplified portrayal of the nature of this support. JCIDS provides similar support to other acquisition programs, regardless of the milestone decision authority. Where appropriate, the JCIDS process and its products may be tailored when applied to automated information systems.

Figure 1.3.F1. JCIDS and Defense Acquisition

Capabilities-Based Assessment Users Guide

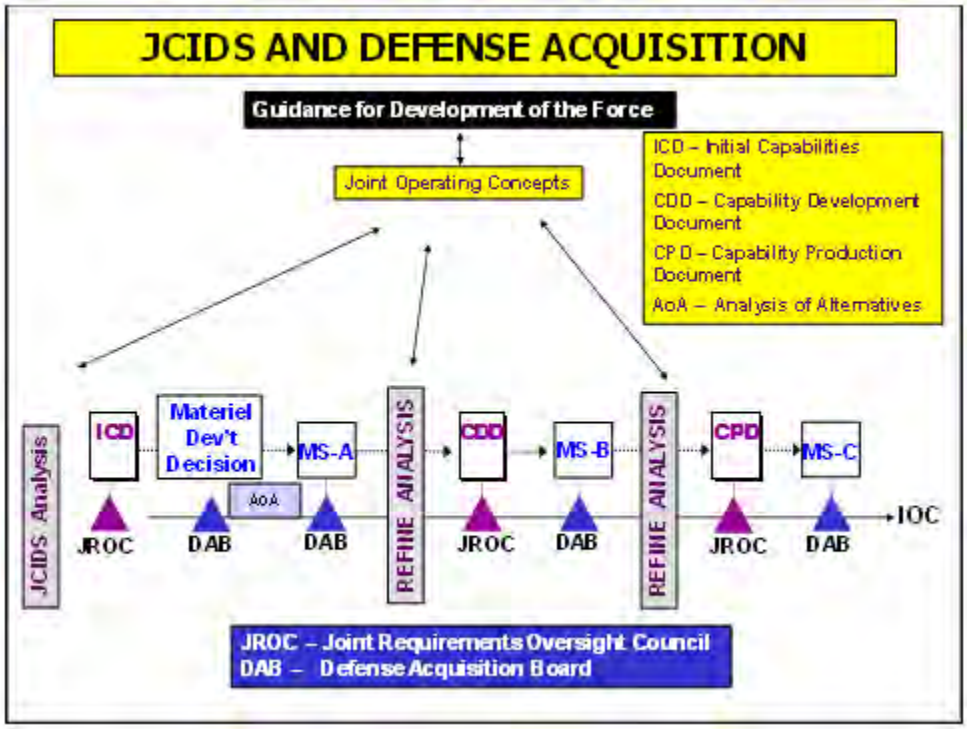


Figure 1.3.F1 depicts several key points. First, JCIDS is based on a series of top-down analyses ultimately derived from formal strategic-level guidance, including the National Security Strategy, National Defense Strategy, National Military Strategy and the Report of the Quadrennial Defense Review . Second, these analyses assess existing and proposed capabilities in terms of their contribution to emerging joint warfighting concepts. Moreover, rather than focusing on the capabilities of individual weapon systems in isolation, the analyses assess capabilities in the context of integrated architectures of multiple interoperable systems. Third, from these overarching concepts, the JCIDS analysis process identifies capability gaps or shortcomings, and assesses the risks associated with these gaps. These gaps may be addressed by a combination of materiel and/or non-materiel solutions (non-materiel solutions would be changes to doctrine, organization, training, leadership and education, personnel, and facilities). Fourth, recommended materiel solutions, once approved, lead to acquisition programs. JCIDS documents are provided for these programs at each acquisition milestone and guide the subsequent development, production, and testing of the program. Further information on Capabilities-Based Assessment , as well as the nature and role of the Initial Capabilities Document , Capability Development Document , and Capability Production Document can be found in the JCIDS Manual .

For Acquisition Category I and IA programs, and other programs designated as high-interest, the JROC reviews and validates all JCIDS documents under its purview. For Acquisition Category ID and IAM programs, the JROC makes recommendations to the

DAB, based on such reviews. Section 181 of title 10, United States Code , establishes JROC responsibilities. The Vice Chairman of the Joint Chiefs of Staff chairs the JROC, and is also a member of the DAB. The Vice Chiefs of each military service are members of the JROC. Section 841of the FY11 National Defense Authorization Act expanded the role of the combatant commanders (or when designated, their deputies) as members of the JROC on matters related to their area of responsibility or when functions of that command are being considered by the Council. The "Expanded JROC" staff brings together key stakeholders from across the department and Interagencies, when appropriate, to shape decisions in support of the Joint warfighter. These stakeholders provide advisory support to the JROC. This same Act specifically designated the following officials of the Department of Defense as civilian advisors:

- The Under Secretary of Defense (Acquisition, Technology, and Logistics)
- The Under Secretary of Defense (Comptroller)
- The Under Secretary of Defense (Policy)
- The Director of Cost Assessment and Program Evaluation
- The Director of Operational Test and Evaluation

Related Link: Capabilities-Based Assessment Users Guide

1.4. Defense Acquisition System

1.4. Defense Acquisition System

The Defense Acquisition System is the management process for all DoD acquisition programs. DoD Directive 5000.01, The Defense Acquisition System , provides the policies and principles that govern defense acquisition. DoD Instruction 5000.02, Operation of the Defense Acquisition System , establishes the management framework that implements these policies and principles. The Defense Acquisition Management System is an event-based process. Acquisition programs proceed through a series of milestone reviews and other decision points that may authorize entry into a significant new program phase. Details of the reviews, decision points, and program phases are found in Enclosure 2 of the DoDI 5000.02 . The Instruction also identifies the specific statutory and regulatory information requirements for each milestone and decision point.

One key principle of the defense acquisition system is the use of acquisition categories, where programs of increasing dollar value and management interest are subject to increasing levels of oversight. DoD Instruction 5000.02 Enclosure 3 identifies the specific dollar values and other thresholds for these acquisition categories. The most expensive programs are known as Major Defense Acquisition Programs (MDAPs) or Major Automated Information System (MAIS) programs. MDAPs and MAIS programs have the most extensive statutory and regulatory reporting requirements. Some elements of the defense acquisition system only apply to weapon systems, some element only apply to automated information systems, and some elements apply to both. DoD Instruction 5000.02, Enclosures 2, 3, and 4 provide specific details.

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Defense Acquisition Executive (DAE). The USD(AT&L) reviews ACAT ID and IAM programs and is the Milestone Decision Authority (MDA). A Defense Acquisition Board (DAB) , chaired by the USD(AT&L), provides advice on critical acquisition decisions. DAB members are senior officials from the Joint Staff, the Military Departments, and staff offices within OSD.

The DAE may delegate decision authority for an MDAP or a MAIS to the DoD Component Head, who may, and generally will, delegate decision authority to the Component Acquisition Executive. Such delegation makes an MDAP program an ACAT IC program and a MAIS program an ACAT IAC program.

The DAB is further supported by a subordinate group in OSD known as an Overarching Integrated Product Team (OIPT) . Each OIPT facilitates communication and vets issues before the DAB meets. At the Milestone Decision Review, the OIPT leader provides the DAB members with an integrated assessment of program issues gathered through the Integrated Product Team process as well as various independent assessments.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 2 - Program Strategies

2.0. Overview

2.0. Overview

This chapter discusses the development and management of program strategies (i.e., the Technology Development Strategy and the Acquisition Strategy (AS)) for Department of Defense acquisition programs. It addresses the information requirements that the Program Manager must consider in preparing the TDS and the AS, respectively.

2.0.1. Purpose

The purpose of this Chapter is to provide information and guidance needed to develop a Technology Development Strategy and to develop and maintain a program-level Acquisition Strategy. A programs strategy should be developed organically by the Program Management Office in collaboration with related communities and

stakeholders.

2.0.2. Content

Section 2.1 describes Program Strategies in the broad sense. Section 2.2 discusses Program Strategy Documentation Requirements; Section 2.3 discusses the relationship of the Program Strategy to other program documents; Section 2.4 discusses the relationship of the Program strategy to the Request for Proposal; Section 2.5 discusses Security Classification Markings for Program Strategies; Section 2.6 describes the Program Strategy approval process; and Section 2.7 is a high level summary of some fundamental differences between an acquisition plan and an Acquisition Strategy. Section 2.8 addresses the Technology Development Strategy/Acquisition Strategy outline .

2.1. Program Strategies-General

Program strategies include the Technology Development Strategy (TDS) and the Acquisition Strategy (AS).

Well-developed program strategies optimize the time and cost required to satisfy approved capability needs. Program strategies should be exploratory in nature. That is, they should express clearly the Program Managers approach to developing and/or procuring the material or service-from a business, contracting, and programmatic point of view. The focus of each strategy should be on the rationale for the approach, not solely a description of the source itself. ***The strategy should not be a repetition of statute, policy, or regulation. It should describe what actions are being taken-and to what end.***

2.2. Program Strategy Document Requirements

Program Strategies must satisfy statutory and regulatory information requirements noted in Department of Defense (DoD) Instruction 5000.02.

The Technology Development Strategy (TDS) must be approved prior to entry into the

Technology Development Phase and, in most cases, precedes the formal Acquisition Strategy (AS). Two exceptions are:

1. If program initiation is declared at Milestone A (currently a potential exception for shipbuilding programs only), information requirements for a TDS will be incorporated in the Acquisition Strategy.
2. If a program enters the acquisition decision process at Milestone B or later (the Milestone Decision Authority determines that technology development is not required for the program to proceed).

The TDS serves as the basis for program acquisition activities in the Technology Development Phase, moving toward a Milestone B decision. The TDS should serve as an information baseline for efforts that continually evolve during the progression through the acquisition management system and be incorporated into the initial Acquisition Strategy (AS), as appropriate.

Department of Defense (DoD) Instruction 5000.02 requires an approved AS prior to any final Request for Proposal (RFP) release for the Engineering and Manufacturing (EMD) Development phase and prior to final RFP release for Milestone C or Full Rate Production/Full Deployment Decisions. The Acquisition Strategy should be updated for all major decision points subsequent to the pre-EMD review and whenever the approved strategy changes. An initial MDA-approved Acquisition Strategy is required prior to program initiation (normally MS B). The AS is required to be updated as necessary, minimally at MS C (Low Rate Initial Production or Limited Deployment) and at Full Rate Production or the Full Deployment Decision.

When submitting TDS and AS documents, DoD acquisition policy and associated business practices require Program Managers to describe their business strategies in substantial detail to include overall approach, contract types, source selection procedures, expected competition and incentive structures.

The level of detail described below should be included in all TDS and AS documents to ensure that the Milestone Decision Authority may make well informed assessments of the efficiency and effectiveness of the business arrangements that are planned. If this information is not provided, program strategy approval will be delayed until it is made available.

1. **Business Strategy:** Address the main contracting approach to include contract types, how competition will be sought, promoted and sustained, source selection procedures, provisions, sources, and product support considerations and leasing arrangements.
2. **Contracting Strategy:** Explain and, to the extent necessary, provide the analysis and rationale for the contracting strategy. Justify the use of fixed-price or cost-plus vehicles. Explain why the incentives provided were chosen and why there is confidence that they will successfully motivate the contractor to provide the performance desired by the government.

3. **Major Contract(s):** Identify the number and type of contracts anticipated.
    - a. For each major contract planned (greater than $40 million [then-year dollars] for an Major Defense Acquisition Program and greater than $17 million for a Major Automated Information System program) describe: what the basic contract buys; how major deliverable items are defined; options, if any, and prerequisites for exercising them; and the events established in the contract to support appropriate exit criteria for the phase or intermediate development activity.
    - b. Indicate whether a competitive award, sole-source award, or multiple-source development with down select to one production contract is contemplated. Describe how the strategy changes from core (initial) to subsequent increments. If a sole source is chosen, identify the exception to full and open competition that applies and provide justification for the duration and timing of the sole-source procurement.
    - c. Identify any special contracting considerations. Discuss any unique clauses/special provisions that will be included in the contract. Identify any special test and evaluation, unique tooling, or other similar contractual requirements.
    - d. Identify any other pertinent information that may ensure understanding of the contracting strategy to include, but not limited to, projected use of Government Furnished Property, plans to re-use hardware and software, safety office review/involvement, period of performance/length of contract, and contract format.
    - e. If a cost-type contract is to be used, provide information (an explanation of technical risk and the steps required to remediate the risk) with supporting documentation to support the Milestone Decision Authority's mandatory assessment that:
        - i. The program is complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed price contract.
        - ii. The complexity and technical challenge of the program is not the result of failure to meet the requirements established in section 2366a of Title 10, United States Code.

          The text of items i and ii must be included verbatim in the strategy to meet the intent of statute.

    - f. If a warranty has been considered, summarize the reasoning. If a product warranty option is being considered, explain the results of the Cost Benefit Analysis to determine if the warranty will be cost beneficial.
4. **Incentives:** For each major contract, describe the contract incentives in detail. State how contract incentives are going to be employed to achieve required cost, schedule, and performance outcomes. If more than one incentive is planned for a contract, the Technology Development Strategy (TDS) and Acquisition Strategy (AS) should explain how the incentives complement each other and do not interfere with one another.

5. **Technical Data Management:** The strategy for Acquisition Category I and II programs shall assess the long-term technical data needs for the system and reflect that assessment in the Technical Data Rights Strategy that is included in both the TDS and the AS. The Technical Data Rights Strategy shall assess the data required to design, manufacture and sustain the system, as well as to support recompetition for production, sustainment or upgrades. It will also address the merits of a price-based option for the future delivery of technical data and intellectual property rights not acquired upon initial contact award and consider the contractors responsibility to verify any assertion of restricted use and release of data.
6. **Sustainment:** The AS should provide an overview of the sustainment-related contract(s) and performance-based agreements with government and industry providers describing how the integrated product support package will be acquired for the system being supported. The discussion should include the contract/agreement and length along with: major terms and conditions; performance measures being used; and the portion of the system covered with the associated sustainment-related functions, plus hardware and data covered in each contract/agreement.

2.2.1. Program Strategies for Increments and Subprograms

An evolutionary acquisition approach delivers capability in increments, recognizing, up front, the need for future capability improvements.

Each increment must be a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained. Block upgrades, pre-planned product improvement, and similar efforts that provide a significant increase in operational capability are managed as separate increments.

Each increment must be traceable back to an approved requirements document and have its own set of threshold and objective values. Each increment must also have an Acquisition Program Baseline establishing cost, schedule, and performance program goals.

If a major defense acquisition program requires the delivery of two or more categories of end items which differ significantly from each other in form and function, the Defense Acquisition Executive may designate such category of end item as a major subprogram for the purposes of acquisition reporting under title 10 Unites States Code. An example of the intended use for subprograms would be the designation of a satellite (subprogram #1) and the affiliated ground control station (subprogram #2) under a total program composed of both elements.

Increments represent operational capabilities; whereas subprograms represent end items that differ significantly from each other in form and function. The premise for establishing increments or subprograms is significantly different, but the reporting

mechanisms are very similar.

Department of Defense Instruction 5000.02 requires each increment or subprogram to have its own program strategy document (Technology Development Strategy or Acquisition Strategy), or minimally, have a distinctly separate annex from the core program strategy document. When appropriate, an annex for an increment can leverage the core program information.

2.3. Program Strategy Relationship to Other Program Documents

Program Documents should not duplicate content, but rather be managed as an integrated set. The Program Strategy (Technology Development Strategy (TDS) or Acquisition Strategy (AS)) should describe the integrated plans that identify the acquisition approach, the business strategy, overall program schedule, and risk management strategies to meet program objectives while balancing cost, schedule and performance.

Content of other documents, such as the Systems Engineering Plan, Life Cycle Sustainment Plan, Program Protection Plan, and Test and Evaluation Master Plan should all align with the TDS or AS content, with minimal overlap.

2.4. Relationship to Request for Proposal (RFP)

Department of Defense Instruction 5000.02 requires an approved program strategy as a prerequisite for final Request for Proposal (RFP) release: a Technology Development Strategy (TDS) prior to entry into the Technology Development phase and an Acquisition Strategy (AS) prior to entry into Engineering and Manufacturing Development, Low Rate Initial Production (or Initial Deployment), and Full Rate Production (or Full Deployment).

Until the Milestone Decision Authority has approved the program strategy (TDS or AS), the formal RFP cannot be released, nor any action may be taken that would commit the program to a particular contracting strategy.

The efforts defined in the approved program strategy for a given phase of the acquisition life cycle must align with efforts to be put on contract for that phase.

The TDS/AS Outline presented at 2.8 in this chapter of the Guidebook describes the structure for a Program Strategy document.

2.5. Program Strategy Classification Markings

Program Strategy documents must be marked for proper handling. Classified AS or TDS documents (and their appendices) should be appropriately marked and handled in accordance with security classification procedures. At a minimum, a TDS or AS should be marked "For Official Use Only (FOUO)" and handled as "controlled unclassified

information" in accordance with DoD Directive 5230.24 . Additionally, if the document contains proprietary information, or is competition sensitive, it should be so marked and appropriately handled.

In addition to displaying the correct markings, it is a good idea for a TDS or Acquisition Strategy to have a distribution statement. An example follows:

Distribution Statement Distribution authorized to U.S. Government Agencies and their contractors; other requests must be referred to [enter the appropriate Program Executive Officer/Program Management Office], Address, City, State, Zip Code.

2.6. Program Strategy Document Approval Process

A Technology Development Strategy (TDS) or Acquisition Strategy (AS) for an Acquisition Category (ACAT) ID or IAM program requires the concurrence of the Program Manager, the Program Executive Officer (PEO) and the Component Acquisition Executive (CAE) prior to submittal for final approval by the Milestone Decision Authority (MDA). The Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) is the MDA for ACAT ID programs-and for ACAT IAM programs (unless delegated to the Deputy Chief Management Officer or Department of Defense Chief Information Officer).

For ACAT IC and IAC programs, MDA is delegated to the appropriate CAE by the USD(AT&L).

For Major Defense Acquisition Programs (MDAPs), MDA approval of the Program Strategy document is required prior to release of a Final Request for Proposal. Programs may not proceed beyond a major milestone decision point (A, B, or C), the pre-Engineering and Manufacturing Development (pre-EMD) review, or the Full-Rate Production (FRP) Decision/Full Deployment Decision review without an MDA-approved Strategy.

For ACAT ID, ACAT IAM, and OSD Special Interest programs, program strategy documents are initially submitted to the office of the Director, Acquisition Resources and Analysis (ARA) within the office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L). ARA coordinates the documents with the appropriate stakeholders prior to submitting to the USD(AT&L) for final approval. Submittal of program strategies should be in accordance with the notional timelines specified in the Defense Acquisition Board Preparation section of Chapter 10 .

2.7. Acquisition Strategy versus Acquisition Plan

2.7.1. Federal Procurement Requirements

2.7.1.1. Distinctions between an Acquisition Strategy and an Acquisition Plan

2.7. Acquisition Strategy versus Acquisition Plan

An Acquisition Plan is prepared by the Contracting Officer and formally documents the specific actions necessary to execute the approach delineated in the approved Acquisition Strategy. The Acquisition Plan serves as the basis for contractual implementation as referenced in Federal Acquisition Regulation (FAR) Subpart 7.1 and Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 207.1 .

The Acquisition Strategy required by Department of Defense (DoD) Instruction 5000.02 is not the same as the acquisition plan required by FAR Subpart 7.1 and DFARS Subpart 207.1 . The Acquisition Strategy is a top-level description, in sufficient detail to allow senior leadership and the Milestone Decision Authority (MDA) to assess whether the strategy makes good business sense, effectively implements laws and policies, and reflects management's priorities. Once approved by the MDA, the Acquisition Strategy provides a basis for more detailed planning.

2.7.1. Federal Procurement Requirements

The Federal Acquisition Regulation requires acquisition planning for all Federal procurements, and the Defense Federal Acquisition Regulation Supplement requires Program Managers to prepare written Acquisition Plans (APs) for most acquisitions exceeding $10 million. An AP is execution-oriented and contract-focused-- normally relating to a singular contractual action; an Acquisition Strategy covers the entire program and may reflect the efforts of multiple contractual actions.

2.7.1.1. Distinctions between an Acquisition Strategy and an Acquisition Plan

As the Department of Defense (DoD) Instruction 5000.02 requirement for an Acquisition Strategy and the FAR/DFARS requirement for an Acquisition Plan (AP) both apply to program planning, questions often arise about how they differ and how they relate to each other.

There is no DoD-level rule that precludes the Program Manager from preparing a single document to satisfy both requirements. In fact, FAR 34.004 dealing with major systems acquisition requires that the Acquisition Strategy "qualify" as the AP. However, in practice, DoD Components often prefer to provide a more general Acquisition Strategy to the Milestone Decision Authority (MDA) for approval and choose to prepare a separate, more detailed AP. If a separate AP is prepared, it may not be approved until after the Acquisition Strategy has been approved.

The distinctions between the requirement for the Acquisition Strategy and the requirement for the AP are summarized in table **2.7.1.1.F1** .

Table 2.7.1.1.F1. Summary of Distinctions between the Acquisition Strategy and Acquisition Plan

	ACQUISITION STRATEGY	ACQUISITION PLAN
Required by	DoD Instruction 5000.02, Enclosure 2, paragraphs 5(c) and 6(a)	FAR 7.1
Required for	All acquisition categories	Contracting or procuring for development activities when the total cost of all contracts for the acquisition program is estimated at $10 million or more; procuring products or services when the total cost of all contracts is estimated at $50 million or more for all years or $25 million or more for any one fiscal year; and other procurements considered appropriate by the agency.
Approval Authority	Milestone Decision Authority	Component Acquisition Executive or designee in accordance with Agency FAR supplements.
Purpose	Describes overall strategy for managing the acquisition program. The Acquisition Strategy describes the PMs plan to achieve programmatic goals and summarizes the program planning and resulting program structure.	Comprehensive plan for implementing the contracting strategy.
Use	Required at program initiation. The Acquisition Strategy should be updated for all subsequent milestones, at the full-rate production decision review, and whenever the approved strategy changes.	Integrates the efforts of all personnel responsible for significant aspects of the contractual agreement. The purpose is to ensure that the Government meets it's needs in the most effective, economical, and timely manner.

Level of Detail	Strategy level. Needed by MDA for decision-making. Also planning level for some discrete information requirements.	Execution level. Provides the detail necessary to execute the approach established in the approved acquisition strategy and to guide contractual implementation and conduct acquisitions.
Content	Prescribed by DoD Instruction 5000.02 ; additional guidance in the Defense Acquisition Guidebook	Prescribed by FAR 7.1 ; DFARS 207
Individual Responsible for Preparing the Document	PM	Person designated as responsible.

2.8. Technology Development Strategy/Acquisition Strategy (TDS/AS) Outline

This guideline is intended as just that, a guideline. While it attempts to shed light on all relevant strategic business aspects of a program, it may fail to solicit information a Program Manager (PM) feels is vital to their chain-of-command. Therefore, PMs are empowered to add where necessary. Adherence to the spirit in which this guideline was crafted should yield a document that provides insight into the PMs thoughts and thought processes.

As directed in the April 20, 2011 Principal Deputy Under Secretary of Defense (Acquisition, Technology, and Logistics) memorandum " Document Streamlining - Program Strategies and Systems Engineering Plan ," the structure for the body of a Program Strategy document follows. Each program strategy should also include a title page, signature/approval page, and a table of contents. The primary sections included in the body of the outline are:

1. Purpose
2. Capability Need

3. Acquisition Approach
4. Tailoring
5. Program Schedule
6. Risk and Risk Management
7. Business Strategy
8. Resources
9. International Involvement
10. Industrial Capability & Manufacturing Readiness
11. Life-cycle Signature Support
12. Military Equipment Valuation

Detail on expected content for each of these topics is described in the following sections.

2.8.1. Purpose

State the reason the program strategy (i.e., the Technology Development Strategy or the Acquisition Strategy) is being prepared or updated (e.g., milestone review, full rate production decision, change in strategy, etc.).

2.8.2. Capability Need

Summarize the requirement. Indicate the key operational and sustainment requirements for this system (i.e., the time-phased capability requirements as described in the Initial Capabilities Document, Capability Development Document, Capability Production Document, Requirements Definition Package, and/or Capability Drop). Highlight system characteristics driven by interoperability and/or joint integrated architectures, capability areas, and family- or system-of-systems.

Summarize the expected operational mission of this program. Identify the user and summarize the users Concept of Operations (CONOPS). Indicate how the program fits into current and future integrated architectures.

Summarize the threat assessment in relation to the capabilities or operational concepts the system will support (see the applicable System Threat Assessment document for details). Specify which elements of the threat (if any) are not yet fully defined, and which elements of the threat (if any) will not currently be countered by the system capabilities or CONOPS. Include a projected plan/schedule to define and counter the remaining threat elements.

If TDS, also summarize the Net-Centric Data Strategy. [Starting with Milestone B, the Net-Centric Data Strategy is included in the Information Support Plan.]

CONSIDERATIONS

When summarizing the threat, consider the following:

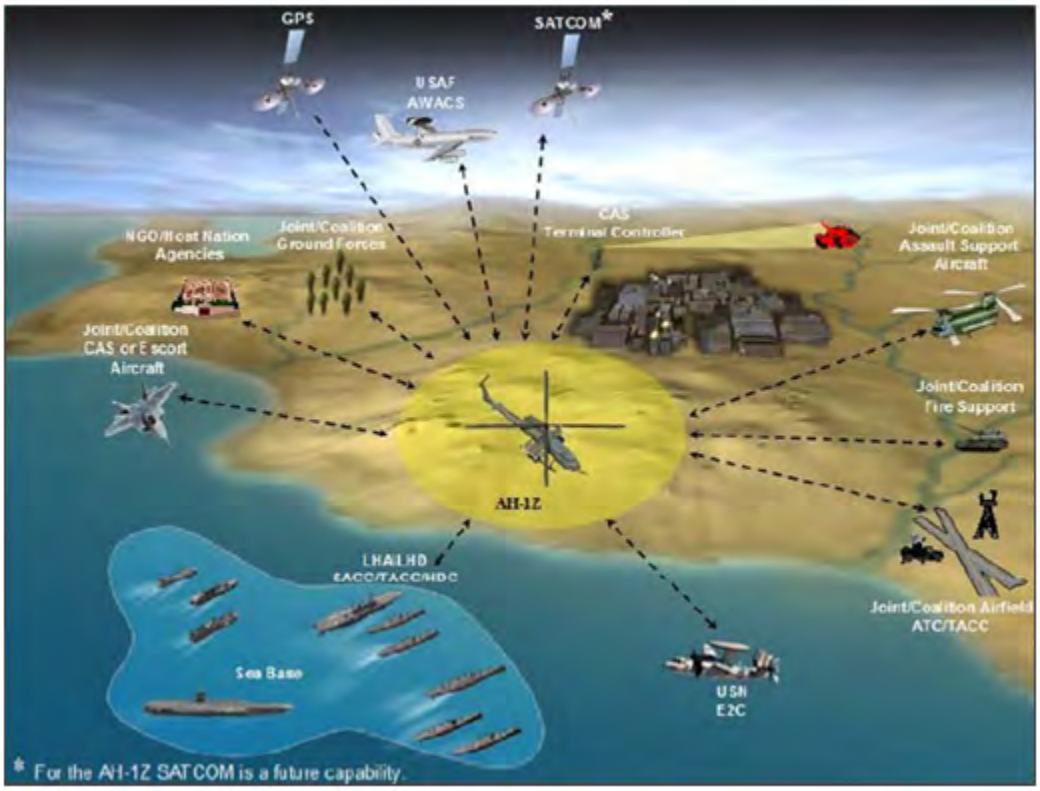
1. **Summarize the threat concisely while addressing it from the perspective of the capability areas and gaps in the validated capability document, including CONOPS considerations.**
2. **Threat elements that are not yet fully defined should be specified referencing scenario, timeframe and foreign systems. The timeline for defining these threats needs to be provided by the Services Intelligence Production Center in concert with the Defense Intelligence Agency.**
3. **Threat elements which will not currently be countered or that should be watched for foreign capability increases need to be identified as Critical Intelligence Parameters (CIPs) in the System Threat Assessment document, an should be highlighted here in the AS/TDS.**
4. **The projected plan/schedule to counter remaining threats needs to be addressed in terms of evolutionary acquisition increments, if applicable for the specific program-and should also be discussed in the Program Strategies Section 6.6 concerning risks deferred.**

NOTES

1. **In most cases, this section of the Technology Development Strategy (TDS) or (Acquisition Strategy (AS) should be classified and presented as a separate annex to the unclassified document. The classified annex should be emailed via the SIPRnet to the Milestone Decision Authority (MDA)s office of primary responsibility (OPR) for TDS/AS documents.**
    - **a. OUSD(AT&L/ARA/AM) is the OPR recipient for programs in which the DAE is the MDA and will distribute this section to OUSD(I), the OIPT leader organization, OSD Systems Engineering, OSD Developmental Test & Evaluation, Office of Operational Test & Evaluation, the Joint Staff J8 and any other OSD parties requesting and appropriately cleared with need to know.**
    - **b. A classified repository capability is anticipated to be set up by the end of FY 2012 that can replace this SIPRNET email process. If this section cannot be written at a level of SECRET (or below) then alternative means will have to be negotiated with the TDS/AS OPR.**
2. **The Program Management Office should work closely with their intelligence community colleagues in the Service Production Center(s) and Component staff intelligence organizations in order to complete this section of the TDS/AS template.**
3. **In this context, the term "threat" refers to the foreign systems and capabilities of a potential adversary in the context of military conflict; it does not include the foreign collection threat that needs to be addressed via the program protection planning process. This threat section is also not relevant to intelligence mission data or signatures data that is needed from the intelligence community for signature dependent systems this information is to be addressed in the *Life-cycle Signature Support Plan* and in summary later in this TDS/AS Outline.**

Include an Operational View (OV)-1 Illustration. (See example in Figure 1, below.)

Figure 1. Example OV-1 Illustration



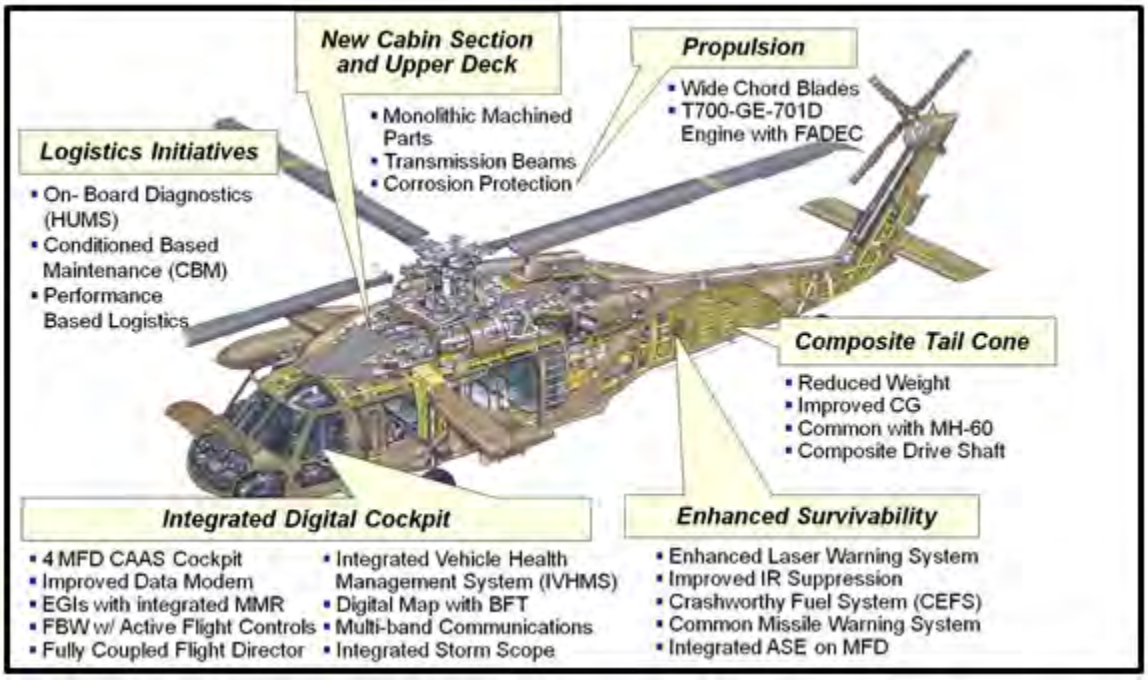
NOTES

1. **The purpose of the OV-1 is to provide a quick, high-level description of what the architecture is supposed to do, and how it is supposed to do it.**
2. **In general the OV-1 describes the business activities or missions, high-level operations, organizations, and geographical distribution of assets. The model frames the operational concept (what happens, who does what, in what order, to accomplish what goal) and highlight interactions to the environment and other external systems.**
3. **A textual description accompanying the graphic is crucial. Graphics alone are not sufficient for capturing the necessary architectural data.**

For Milestone B, provide a reference design concept for the product showing major subsystems and features (one or more drawings as needed to describe or illustrate the

expected features of the product; see the example in Figure 2).

Figure 2. Sample Drawing of the Reference Design Concept



2.8.3. Acquisition Approach

Indicate whether the program strategy will be evolutionary or single step to full capability and rationale for selection. **Note:** If this program employs an evolutionary acquisition approach, this strategy will primarily apply to the current increment, while occasionally addressing some topics in the context of the overall program.

If this program employs an evolutionary acquisition approach, summarize the cost, schedule, and performance drivers for the increment under consideration, and the plan to transition from the initial increment to later increments.

NOTES

The cost, schedule and performance drivers summarized here should align with the cost, schedule and performance parameters in the acquisition program baseline.

An evolutionary approach delivers capability in increments, recognizing, up front, the need for future capability improvements. If this program strategy is for an evolutionary approach, each increment must be a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained.

Each increment must be traceable back to an approved requirements document and have its own set of threshold and objective values. Each program or increment shall have an Acquisition Program Baseline establishing program goals.

Department of Defense Instruction 5000.02 requires each increment or subprogram to have its own program strategy document (TDS or AS), or minimally, have a distinctly separate annex from the core program strategy document. When appropriate, an annex for an increment can leverage the core program information.

Specify any unique program circumstances, such as transitioning from a technology project, selection as a special interest program, etc.

Indicate whether this program will replace an existing system, is a modification to an existing system, or is a new capability.

Indicate whether this is a New Start program. Verify that the appropriate Congressional notifications have been completed for a New Start. (Reference DoD 7000.14-R, *DOD Financial Management Regulation* , Volume 3, Chapter 6 for guidance on new start determinations.)

NOTES

1. **A new start is considered to be reprogramming actions which require prior approval of the congressional committees (DD 1415-1).**
2. **A new start program for RDT&E is a new program element or project, or a major component thereof, as determined by specific supporting information provided in the R-2 and R2A (RDT&E Budget Item/Project Justification) exhibit's not previously justified by the Department and funded by the Congress through the normal budget process.**
3. **A new start program for Procurement is a new procurement line item or major component thereof, as determined by specific supporting information provided in the P-5 (Cost Analyst) or P40A (Budget Items Just for Aggregated Items) exhibit's not previously justified. Congressional committees discourage the use of the reprogramming process to initiate programs. Except for extraordinary situations, consideration will not be given new start reprogramming requests for which the follow-on funding is not budgeted or programmed. Funding for new starts may not be obligated without prior approval or written notification.**

Indicate whether this is a joint program. If so, specify the joint nature and characteristics of the program. Identify the Service(s) or DoD Components involved, state the key Service-specific technical and operational differences in the end item deliverables, and provide the principal roles and responsibilities of each DoD Component in the management, execution, and funding of the program.

If this is a Technology Development Strategy, identify the feasible technical approaches for developing the approved materiel solution, the impact of prior acquisitions on those approaches, and any related preceding effort.

If this strategy supports the Milestone B or C decision, in a table showing quantity per year, indicate the total planned production quantity and provide the LRIP quantity. Summarize the Low-Rate Initial Production (LRIP) plan. If the planned LRIP quantity exceeds ten percent of the total planned production quantity, provide the justification. (Not applicable to software-intensive programs without production components.)

2.8.4. Tailoring

Consistent with statutory and federal regulatory requirements, the Program Manager (PM) and Milestone Decision Authority (MDA) may tailor the phases and decision points to meet the specific needs of the program. If tailoring is planned, state what is being

proposed and why.

List all requests for either regulatory policy waivers or waivers permitted by statute. Include a table similar to notional Table 1.

NOTE

The Table should contain proposed tailoring initiatives for MDA approval, as well as already approved (e.g., via Acquisition Decision Memorandum) tailored items, and the rationale should state why the policies, regulations or directives being proposed to be tailored are not relevant or applicable.

Table 1. Notional Table of Program Waiver Requests

WAIVER REQUESTS					
Requirement to Be Waived	Type (Regulatory or Statutory)	Granting Authority	Rationale	Required by (date or event)	Status

[2.8.5. Program Schedule]

[2.8.5.1. Interdependencies]

[2.8.6. Risk and Risk Management]

2.8.5. Program Schedule

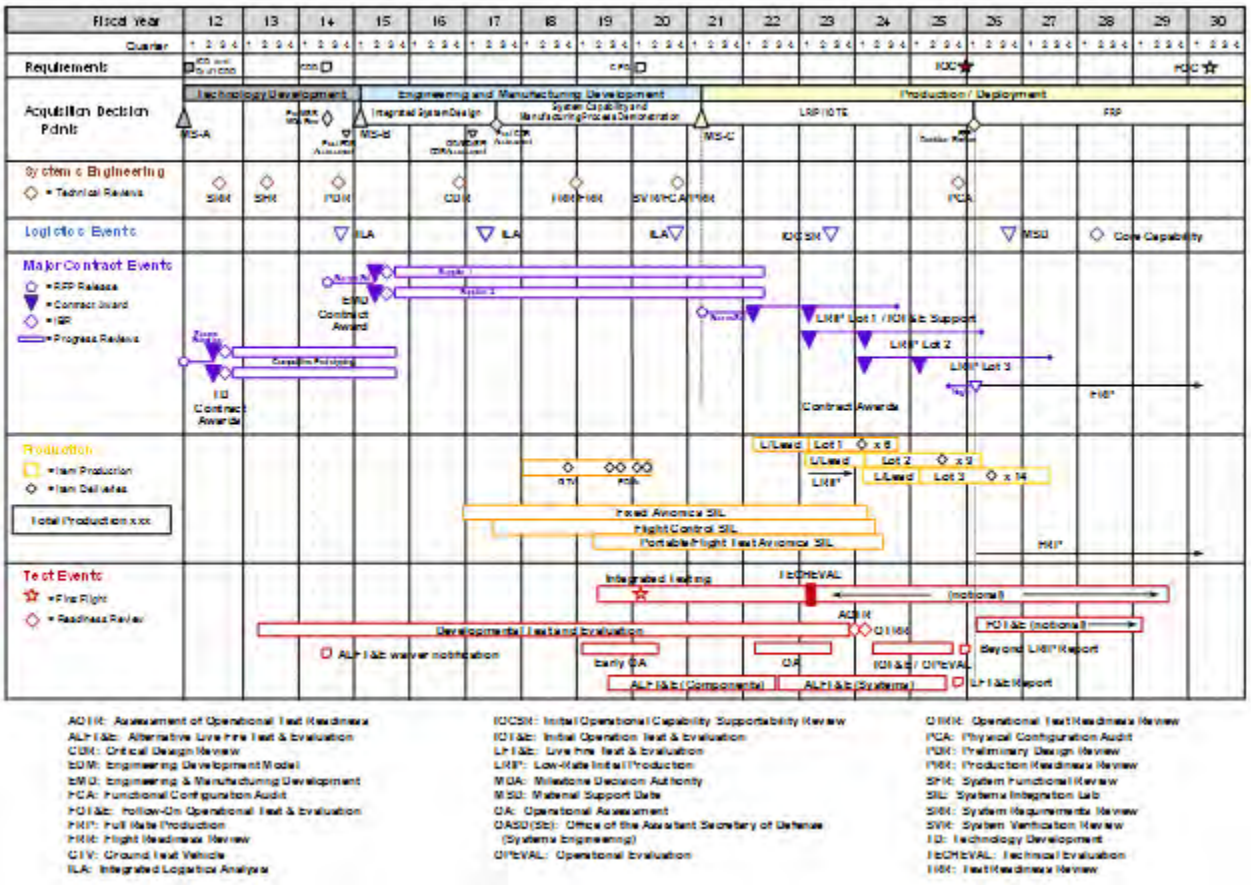
Provide a detailed graphic illustrating program milestones, phases, and events. Depicted events will vary by program, but will minimally include key acquisition decision points; principal systems engineering and logistics activities such as technical reviews and assessments; planned contracting actions such as request for proposal (RFP) release, source selection activity, and contract awards; production events and deliveries; and key test activities. (Figure 3 is a notional depiction of the expected level of detail. For example, contract details will vary with the contracting approach and the plan for competition and multiple suppliers; the use of options, re-competes, and/or new negotiated sole source; etc.)

Explain and justify any urgency if it results in needed tailoring for example if it

constitutes justification for not providing for full and open competition.

Summarize the analysis justifying the proposed program schedule (list analogous programs or models used to derive schedule).

Figure 3. Notional depiction of the Integrated Schedule for Program



CONSIDERATIONS

1. **If a Technology Development Strategy, the program schedule minimally needs to identify the following:**
    - **contract award dates for major contracts;**
    - **whole system reviews including system requirements review (SRR), system functional review (SFR), and the preliminary design review (PDR);**
    - **competitive prototyping activities;**
    - **major test events such as for prototypes of key systems;**
    - **the technology readiness assessment (TRA);**
    - **final draft pre-Engineering & Manufacturing Development (EMD) review Acquisition Strategy (AS);**
    - **draft RFP for EMD;**
    - **Milestone B; and,**
    - **Initial Operating Capability (IOC).**
2. **If for an EMD AS, the schedule minimally needs to identify the following:**
    - **contract events such as award dates, contract definitization, planned exercise of contract line item numbers, and Integrated Baseline Review (IBR);>**
    - **system level Critical Design Review (CDR), software specification review (SSR), Test Readiness Review (TRR) and Production Readiness Review (PRR);**
    - **key prototyping activities for technology maturation;**
    - **major test events such as operational assessments and integration tests, as well as the operation test readiness review (OTRR);**
    - **maintenance plans, depot maintenance core capabilities stand-up, Training Plan, Source of Repair Assignment Process (SORAP),**
    - **Environment, Safety, and Occupational Health (ESOH) plans events,**
    - **draft RFP for LRIP, final draft LRIP AS submission to MDA staff;**
    - **Milestone C; and,**
    - **Initial operating capability (IOC).**
3. **If for an LRIP AS, the schedule minimally needs to identify the following:**
    - **contract events such as award dates, contract definitization, planned exercising of contract line item numbers, and Integrated Baseline Review (IBR)**
    - **Physical Configuration Audit (PCA), and System**

Verification Review (SVR);
- **Operational and developmental test events including initial operational test and evaluation (IOT&E) and live fire test and evaluation (LFT&E);**
- **Production quantities for each year;**
- **maintenance plans, depot maintenance core capabilities stand-up, Training Plan, Source of Repair Assignment Process (SORAP),**
- **identify the activation schedule for each site in the supply chain required to support the system including the maintenance sites (including depots) and training sites**
- **Environment, Safety, and Occupational Health (ESOH) plans events**
- **draft RFP for LRIP, final draft FRP AS submission to MDA staff;**
- **Full-Rate Production Decision Review (FRP DR); and,**
- **initial operating capability (IOC) and full operational capability (FOC)**

4. **If for an FRP AS, the schedule should minimally include:**
   - **contract events such as award dates, contract definitization, planned exercising of contract line item numbers, and Integrated Baseline Review (IBR)**
   - **Production quantities for each year;**
   - **maintenance plans, depot maintenance core capabilities stand-up, Training Plan, Source of Repair Assignment Process (SORAP),**
   - **identify the activation schedule for each site in the Production quantities for each year;**
   - **maintenance plans, depot maintenance core capabilities stand-up, Training Plan, Source of Repair Assignment Process (SORAP),**
   - **identify the activation schedule for each site in the supply chain required to support the system including the maintenance sites (including depots) and training sites**
   - **planned or anticipated future increments;**
   - **post-implementation review (PIR); and,**
   - **initial operating capability (IOC) & full operational capability (FOC).**

2.8.5.1. Interdependencies

Specify programmatic interdependencies with other programs. Discuss the relationship

of the interdependencies with program activity on the critical path. If any memorandums of agreement are required to formalize these relationships/ interfaces, list them in the format presented in Table 2. Identify the interface (i.e., the system this product interfaces with); the agency that owns the other system; the authority (e.g., PEO, CAE, delegated PM) responsible for controlling the interface (i.e., the individual who can set the requirement; direct the solution to the interface issue; and direct who provides the funding for the solution); the required by date; and the impact if not completed.

Table 2. Notional table of Required Memoranda of Agreement

REQUIRED MEMORANDA OF AGREEMENT				
Interface	**Cooperating Agency**	**Interface Control Authority**	**Required By Date**	**Impact if Not Completed**

If using an evolutionary acquisition approach with concurrent increments, state the relationship between the milestones and activities in one increment to those in the other increment(s). Include criteria for moving forward to subsequent phases of the same or other increments.

2.8.6. Risk and Risk Management

Summarize the approach used to identify, analyze, mitigate, track, and control performance/technical/manufacturing cost, schedule, sustainment, and programmatic risk throughout the life of the program.

NOTES

1. **The Program Manager (PM) should establish a risk management process consistent with *Guidebook Chapter 4* , and summarize the process in the Acquisition Strategy.**
2. **For an EMD AS, if the program is so complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed-price type contract for EMD, the AS needs to include an explanation of the level of program risk as well as steps that have been taken, and are planned, to reduce risk. Finally a rationale for entry into EMD despite the high level of program risk should be included. This explanation of complexity, technical challenge, and risk will provide the MDA with the needed documentation if other than a fixed-price type contract is to be used for EMD.**
3. **ESOH Risks are assessed in accordance with MIL-STD-882D and reflected here when applicable.**
4. **Spectrum availability and supportability for applicable programs may pose for significant program risk. Spectrum analysis must be done for all applicable programs. (See DAG Chapter 7.)**
5. **The AS is an appropriate place to discuss cost, schedule and performance implications or trades related to risks and risk mitigation, but not for detailed mitigation plans with waterfalls, etc. The Systems Engineering Plan (SEP) is the appropriate document for details on mitigation plans for the noted key technology-related acquisition risks. The SEP or the programs Risk Management Plan is appropriate for detailed discussion of the risk management process, whereas the Acquisition Strategy should only contain a summary.**

List and assess any program interdependency issues that could impact execution of the acquisition strategy. If the program is dependent on the outcome of other acquisition programs or must provide capabilities to other programs, the nature and degree of risk associated with those relationships should be specified. Summarize how these relationships and associated risk will be managed at the PM, PEO, and DoD Component levels.

List the key program technologies, their current technology readiness levels (TRL), the basis for including a technology (e.g., available alternative or low-risk maturation path) if it is below the TRL 6 benchmark for Milestone B, and the key engineering and integration risks. **NOTE:** Key technologies should include those technologies that are

part of the system design and those associated with manufacturing the system.

- If conducted, summarize the results of the Technology Readiness Assessment.
- Summarize technology maturation plans and risks for each key technology, engineering risk, and integration risk identified.
- Briefly explain how the programs strategy is appropriate given the maturity of the system technology and design.

If the strategy is for the Technology Development Phase:

- Identify alternate technologies that could be employed if a technology chosen for the system does not achieve the maturity necessary to incorporate it into the baseline system design and define their impact on system performance and cost.
- Identify the specific prototyping activities that will be conducted during Technology Development and specify how those activities and any others planned for Engineering and Manufacturing Development will be used to reduce program cost, schedule, and/or performance risk.

Identify the principal programmatic risks (e.g., staffing, resources, infrastructure, industrial base, etc.) and summarize mitigation plans, including key risk-reduction events.

NOTES

The Program Manager should summarize the anticipated or existing key acquisition risks for the program and include the related Risk Reporting Matrix (risk cube). The Acquisition Strategy should describe how funding, schedule and performance are planned to be balanced and traded to manage/mitigate key risks.

- **The risk cube format and Likelihood and Consequence criteria should be taken from the " *Risk Management Guide for DoD Acquisition, 6th Edition, Version 1, August 2006* ."**

Identify any risks that have been deferred to future increments. Explain why these risks were deferred and whether any residual risks remain in this increment.

CONSIDERATION

This section should include, but not be limited to, the risks associated with threats as described in section 2.8.2.

The acquisition strategy at the Full-Rate Production/Full Deployment Decision Review

should identify principal manufacturing (if applicable), sustainment, and operational risks, and it should summarize mitigation plans, to include key risk reduction events.

2.8.7. Business Strategy

2.8.7.1. Competition Strategy

2.8.7.2. Market Research

2.8.7.3. Advance Procurement

2.8.7.4. Sustainment Strategy

2.8.7.5. Major Contract(s) Planned

2.8.7.5.1. Major Contract Table

2.8.7.5.2. Contract Incentives

2.8.7.5.3. Earned Value Management (EVM)

2.8.7.5.4. Source Selection Approach

2.8.7.5.5. Sources

2.8.7.5.6. Contract Bundling or Consolidation

2.8.7.5.7. Subcontracting Plan / Small Business Participation

2.8.7.5.8. Special Contracting Considerations

2.8.7.5.9. Special Test Equipment

2.8.7.5.10. Testing & Systems Engineering Requirements

2.8.7.5.11. Warranty

2.8.7.5.12. Multiyear Contracting

2.8.7.5.13. Leasing

2.8.7.5.14. Modular Contracting (Major Information Technology programs only)

2.8.7.5.15. Payment

2.8.7.5.16. Other Relevant Information

2.8.7. Business Strategy

2.8.7.1. Competition Strategy

Explain how a competitive environment will be sought, promoted, and sustained throughout all program phases.

Summarize the competition strategy for the upcoming phase.

NOTES

1. Competition is a key consideration for fostering innovation and affordability for defense applications. The Program Strategy document for all programs should describe the competition planned for the subject phase of the programs life cycle, or explain why competition is not practicable or not in the best interests of the Government.
2. Specify measures planned to be used to ensure competition, or the option of competition at both the prime contract level and the subcontract level (at such tier or tiers as are appropriate) of such program throughout the life-cycle of such program as a means to improve contractor performance; and adequate documentation of the rationale for the selection of the subcontract tier or tiers. Specify which of the following measure are planned to ensure competition:

- Competitive prototyping.
- Dual-sourcing.
- Unbundling of contracts.
- Funding of next-generation prototype systems or subsystems.
- Use of modular, open architectures to enable competition for upgrades.
- Use of build-to-print approaches to enable production through multiple sources.
- Acquisition of complete technical data packages.
- Periodic competitions for subsystem upgrades.
- Licensing of additional suppliers.
- Periodic system or program reviews to address long-term competitive effects of program decisions.
- Other

In situations where head-to-head competition is not possible, explain how dissimilar

competition or other competitive approaches will be used.

Indicate how the results of the previous acquisition phase impact the competition strategy for the approaching phase.

CONSIDERATIONS

If this is a Technology Demonstration Strategy specify the following with respect to Competitive Prototyping plans:

- Will the complete system be prototyped? If not, provide a supporting rationale.
- List the critical subsystems of the system that are to be competitively prototyped. If neither the complete system nor the critical subsystems are planned to be competitively prototyped, refer to the waiver section below.
- Specify the number of candidates anticipated to be in the competition for each complete system and/or critical subsystem. Indicate whether the candidates are expected to be commercial, government or academic sources.
- Specify the planned competitive criteria to be used to down-select for each complete system and/or critical subsystem (e.g. technical data rights, performance criteria).

NOTES

Competitive Prototyping Waivers: the Milestone Decision Authority may waive the requirement only on the basis that-

- A. the cost of producing competitive prototypes exceeds the expected life-cycle benefit's (in constant dollars) of producing such prototypes, including the benefits of improved performance and increased technological and design maturity that may be achieved through competitive prototyping; or
- B. but for such waiver, the Department would be unable to meet critical national security objectives.

P.L. 111-23, Weapon Systems Acquisition Reform of 2009 stipulates that whenever a Milestone Decision Authority authorizes a waiver the Milestone Decision Authority shall require that the program produce a prototype before Milestone B approval if the expected life-cycle benefit's (in constant dollars) of producing such prototype exceed its cost and its production is consistent with achieving critical national security objectives; and, shall notify the congressional defense committees in writing not later than 30 days after the waiver is authorized and include in such notification the rationale for the waiver and the plan, if any, for producing a prototype.

[The prototyping requirement may NOT be waived-only the competitive aspect of prototyping may be waived in the limited circumstances noted.]

2.8.7.2. Market Research

Summarize the research conducted and the results of market research. Indicate the specific impact of those results on the various elements of the program. Summarize plans for continuing market research to support the program throughout development and production.

Market research information provided in the strategy should be sufficient to satisfy the requirements of 10 United States Code (USC) 2366a and 10 USC 2366b. For more information, see Federal Acquisition Regulation (FAR) Part 10, *Market Research* , and Defense Federal Acquisition Regulation Supplement (DFARS) section 210.001).

CONSIDERATIONS

1. Market research is a primary means of determining the availability and suitability of commercial items and the extent to which the interfaces for these items have broad market acceptance, standards-organization support, and stability. In addition, market research is important in seeking small business capabilities.
2. Thorough market research needs to be performed to determine whether or not small businesses are capable of satisfying the requirements. Market research supports the acquisition planning and decision process, supplying technical and business information about commercial technology and industrial capabilities to arrive at the most suitable approach to acquiring, distributing and supporting supplies and services. Market research, tailored to program needs, should continue throughout the acquisition process and during post-production support.
3. Market research should yield an understanding of potential material solutions, their technology maturity, and potential sources, and should suggest strategies for acquiring them.
4. Market Research is required to support the 10 USC 2366b Milestone B certification. Compliance with 10 USC 2377, 15 USC 644, P.L.111-23, other statute & DFARs determine the outcome of the market strategy certification element.

2.8.7.3. Advance Procurement

Indicate whether advance procurement of long lead items is planned. List highest dollar value items. The Acquisition Strategy must clearly indicate the intention to employ advance procurement. ***[NOTE: The MDA must separately and specifically approve advance procurement if authorization is sought prior to the applicable milestone decision.]***

NOTES

1. DoD Financial Management Regulation 7000.14-R (Volume 2A, Chapter 1) requires that the procurement of end items be fully funded, i.e., the cost of the end items to be bought in any fiscal year should be completely included in that year's budget request. However, there are times when it is appropriate to procure some components, parts, materiel, or effort in advance of the end item buy. These items are referred to as advance procurements. Statutory authority for these advance procurements should be provided in the relevant authorization and appropriations acts.
2. Advance procurement funds are used in major acquisition programs for advance procurement of components whose long-lead times require purchase early in order to reduce the overall procurement lead-time of the major end item. Advance procurement of long lead components is an exception to the DoD "full funding" policy and must be part of the President's budget request. These expenditures are subject to the following limitations:
    - a. the cost of components, material, parts, and effort budgeted for advance procurement should be low compared to the total cost of the end item
    - b. the PM judges the benefits of the advance procurement to outweigh the inherent loss of or limitation to future MDA flexibility
    - c. the MDA approves the advance procurement
    - d. the procurement received statutory authority, as discussed above
3. As part of the milestone review, the MDA should approve specific exit criteria for advance procurement. These specific exit criteria should be satisfied before the PM releases any advance procurement funding for either the initial long lead-time items contract(s) or the contract(s) for individual, follow-on, long lead-time lots. The contracts office should initiate a separate contract action for advance procurement of long lead materiel.
4. The MDA must approve advance procurement in advance of Milestone C, and the intention should be clearly noted in the Acquisition Strategy. A template should be completed and provided for MDA approval prior to executing long lead advance procurement if the approved AS and current/appropriate year budget exhibit’s do not contain all of the equivalent content. The template can be included in the AS, or by separate memo for the MDA to approve.

2.8.7.4. Sustainment Strategy

The details of program sustainment planning are included in the Life Cycle Sustainment Plan, which will be prepared and approved as a separate document. This portion of the Program Strategy document should:

Specify the contracting strategy to provide product support throughout the system life cycle. The sustainment strategy should reflect the Maintenance or Support CONOPS and consider: impacts to system capability requirements; responsiveness of the integrated supply chains across government and industry; maintaining long-term competitive pressures on government and industry providers; and providing effective integration of weapon system support that is transparent to the warfighter and provides total combat logistics capability.

CONSIDERATIONS

Provide an overview of the sustainment related contract(s) including how the integrated product support package will be acquired. The discussion must include the:

- Type contract and length along with major terms and conditions
- Performance measures being used (including the extent to which it is traditional transaction based/process focused and performance-based/outcome focused)
- Sustainment related functions, hardware or data covered in each contract
- Portion of system covered by performance based product support strategy

State the assumptions used in determining whether contractor or agency support will be employed, both initially and over the life of the acquisition, including consideration of contractor or agency maintenance and servicing (see FAR Subpart 7.3), support for contracts to be performed in a designated operational area or supporting a diplomatic or consular mission (see FAR section 25.301); and distribution of commercial items.*

* ***Note:*** *Items marked with an asterisk (*) in this section are not required for the Technology Development Phase or Technology Development Strategy.*

Provide an overview of the sustainment-related contract(s) including how the integrated product support package will be acquired. The discussion should provide:

- The performance measures being used (including the extent to which it is traditional transaction based/process focused and performance-based/outcome focused);
- The portion of the system covered with the associated sustainment-related

functions;

- How the support concept ensures integration with other logistics support and combat support functions to optimize total system availability while minimizing cost and the logistics footprint;
- How the product support strategy will ensure the selection of best value support providers, maximize partnering, and advocate integrated logistics chains in accordance with DoD product support objectives;
- How manpower and spares will be optimized;*
- Efforts to ensure secure and integrated information systems across industry and government that enable comprehensive supply chain integration and full asset visibility;*
- Dedicated investments needed to achieve continuous improvement of weapon system supportability and reduction in operating costs;
- How performance expectations (as defined in performance agreements) will be compared to actual performance results (post Milestone C);*
- If Interim Contract Support (ICS) is planned, the ICS requirements, approach, and a plan to transition to normal sustainment support.*
- If the strategy includes contractor logistics support (CLS), indicate how CLS contract flexibility will support the sustainment concept;* and
- How the program will ensure product support integration throughout the system life cycle.

2.8.7.5. Major Contract(s) Planned

For each contract with an estimated total value greater than $40 million dollars for an MDAP or greater than $17 million dollars for a MAIS, including all options.

2.8.7.5.1. Major Contract Table

Provide a table (see example Table 3) that identifies the purpose, type, value, performance period, and deliverables of the contract.

Table 3. Notional Table of Major Contracts

MAJOR CONTRACTS					
Contract	**Purpose**	**Type**	**Value**	**Performance Period**	**Major Deliverables**

Specify what the basic contract buys; how major deliverable items are defined; options, if any, and prerequisites for exercising them; and the events established in the contract to support appropriate exit criteria for the phase or intermediate development activity.

Identify the contract type(s) and period(s) of performance. The acquisition strategy shall provide the information necessary to support the decision on contract type. (See FAR Part 16 and Section 818, Public Law (P.L.) 109-364 for additional direction.)

NOTES

1. Each major contract (greater than $40 million (then-year dollars) for a Major Defense Acquisition Program and greater than $17 million for Major Automated Information System) planned to execute the Acquisition Strategy must be addressed.
2. Per Section 818 NDAA FY 2007, for MS B approval, the Milestone Decision Authority (MDA) shall select a contract type that is consistent with the level of program risk. The MDA may select from a fixed-price, including fixed price incentive, or cost type contracts.
3. The law states that the "MDA may authorize the use of a cost type contract" upon determination that:
    - a. the program is complex and technically challenging that it would not be practicable to reduce program risk to a level that would permit the use of a fixed-price contract
    - b. the complexity and technical challenge of the program is not the result of a failure to meet the requirements established in section 2366a of title 10, United States Code.
4. These two (preceding) bullets must be included verbatim in the AS to meet the intent of Section 818, and for MS B approval, and combined with supporting documentation, if a cost type contract is to be used.
5. The MDA shall document the contract type selected, to include an explanation of the program risk level and the steps, if necessary, to reduce high program risk in order to proceed to MS B.

CONSIDERATION

Consider including an explanation of the level of program risk for the program and, if the Milestone Decision Authority determines that the level of program risk is high, the steps that have been taken to reduce program risk and reasons for proceeding with MS B approval despite the high level of program risk. (See also section 2.8.6.)

Address the alignment of the contract (s) with the overarching acquisition strategy and the competition strategy.

Indicate whether a competitive award, sole source award, or multiple source development with down select to one production contract is planned.

If expecting to use other than full and open competition, cite the authority and indicate the basis for applying that authority, identify source(s), and explain why full and open competition cannot be obtained.

Indicate how subcontract competition will be sought, promoted, and sustained throughout the course of the acquisition. Identify any known barriers to increasing subcontract competition and address how to overcome them.

Specify breakout plans for each major component or sub-system as well as spares and repair parts.

Assess the comparative benefits of awarding a new contract vice placing a requirement under an existing contract. (10 USC 2306 , 10 USC 2304 .)

If planning to award a new indefinite delivery contract, indicate how many contracts are planned to be awarded. If a single award is planned, explain why multiple awards are not feasible. Indicate the ordering period.

Undefinitized Contracts . Indicate if an undefinitized contract will be awarded and provide the rationale. Identify steps to avoid using an undefinitized contract, and list the planned incentives to motivate the contractor to achieve timely definitization.

2.8.7.5.2. Contract Incentives

Provide the planned contract incentives:

- Provide the specific incentive structure. Indicate how the incentive structure will motivate contractor behavior resulting in the cost, schedule, and performance outcomes required by the government for the contract and the program as a whole.
- If more than one incentive is planned for a contract, the strategy should explain how the incentives complement each other and do not conflict with one another.

2.8.7.5.3. Earned Value Management (EVM)

Summarize the financial reporting that will be required by the contractor on each contract, including requirements for EVM.

2.8.7.5.4. Source Selection Approach

Identify the source selection evaluation approach (e.g., Trade-off or Lowest Price Technically Acceptable) and briefly summarize planned procedures (10 USC 2305).

Highlight the considerations influencing the proposed source selection procedures. Indicate how these may change from phase to phase.

State the timing for submission and evaluation of proposals. Identify the criteria that will be used to select the winning bidder. Indicate how those criteria reflect the key government goals for the program.

2.8.7.5.5. Sources

List the known prospective sources of supplies or services that can meet the need. Consider required sources of supplies or services (see FAR Part 8), and sources identifiable through databases including the government-wide database of contracts and other procurement instruments intended for use by multiple agencies available at https://www.contractdirectory.gov/contractdirectory/ .

Based on results of market research, identify the specific opportunities for:

- small business,
- veteran-owned small business,
- service-disabled veteran-owned small business,
- HUBZone small business,
- small disadvantaged business, and
- women-owned small business concerns, and
- specify how small business participation has been maximized at both the direct award and subcontracting levels (see FAR Part 19).

2.8.7.5.6. Contract Bundling or Consolidation

If the contract is a bundled acquisition (consolidating two or more requirements for supplies or services, previously performed under smaller contracts, into a single contract that is likely to be unsuitable for award to a small business), indicate the specific benefit's anticipated to be derived from bundling. Reference FAR section 7.107 , *Acquisition Planning* . (15 USC 644)

If applicable, identify the incumbent contractors and the contracts affected by the bundling.

Per DFARS section 207.170 , if the acquisition strategy proposes consolidation of contract requirements with an estimated total value exceeding $6 million, provide: (1) the results of market research; (2) identification of any alternative contracting approaches that would involve a lesser degree of consolidation; and (3) a determination by the senior procurement executive that the consolidation is necessary and justified.

NOTES

1. Section 644, title 15, United States Code requires a Benefit Analysis & Determination when contract bundling is planned.
2. FAR 7.103(s) requires that acquisition planners, to the maximum extent practicable, avoid unnecessary and unjustified bundling that precludes small business participation as contractors. As a result of this direction, DoD Instruction 5000.02 requires a Benefit Analysis and Determination. The purpose of the benefit analysis is to determine the relative benefit to the government among two or more alternative procurement strategies. (See definitions at FAR 2.201 and DFARS 207.170-2)
3. DFARS 207.170 directs agencies not to consolidate contract requirements with an estimated total value exceeding $5.5million unless the acquisition strategy includes: (1) the results of market research: (2) Identification of any alternative contracting approaches that would involve a lesser degree of consolidation; and (3) a determination by the senior procurement executive that the consolidation is necessary and justified.

2.8.7.5.7. Subcontracting Plan / Small Business Participation

When FAR Subpart 19.7 applies, the acquisition strategy should establish maximum practicable individual socio-economic subcontracting goals, meaningful small business work, and incentives for small business participation.

Outline planned award evaluation criteria concerning small business utilization in accordance with FAR Subpart 15.3 , and DFARS Subpart 215.3 regarding source selection; and

Summarize the rationale for the selection of the planned subcontract tier or tiers.

Indicate how prime contractors will be required to give full and fair consideration to qualified sources other than the prime contractor for the development or construction of major subsystems and components.

CONSIDERATION

The Program Manager should consider consulting the local small business representative or Office of Small Business Programs website for additional information concerning this information requirement or any other small business-related related acquisition planning.

2.8.7.5.8. Special Contracting Considerations

Identify any special contracting considerations: list any unique clauses or special provisions (e.g., any contingent liabilities (i.e., economic price adjustment or business base clauses, termination liability, etc.)) or special contracting methods (see FAR Part 17) included in the contract; list any special solicitation provisions or FAR deviations required (see FAR Subpart 1.4).

2.8.7.5.9. Special Test Equipment

Identify any planned use of government-furnished special test equipment, unique tooling, or other similar contractual requirements.

2.8.7.5.10. Testing & Systems Engineering Requirements

Specify how testing and systems engineering requirements, including life-cycle management and sustainability requirements, have been incorporated into contract requirements.

Identify the engineering activities to be stated in the RFP and required of the contractor to demonstrate the achievement of the reliability and maintainability design requirements.

Provide a table (see example Table 4) to specify how the sustainment key performance parameter thresholds have been translated into reliability and maintainability design and contract specifications. Table 4, as presented here, is a sample. The actual format of this table may be varied to suit the nature of the procurement or to add additional requirements. The reliability threshold is often expressed as Mean Time Between Failure (MTBF). Use the appropriate life unit's (e.g., hours, cycles, etc.). "MTTR" is "mean time to repair;" "N/A" may be entered if an item is not applicable.

Table 4. Reliability and Maintainability Requirements

Reliability and Maintainability Requirements		
Parameter	**Threshold**	**Contract Specification Requirement**
Reliability (e.g., MTBF)		
Maintainability (e.g., MTTR)		

2.8.7.5.11. Warranty

Indicate whether a warranty is planned, and if so, specify the type and duration; summarize the results of the supporting Cost Benefit Analysis. (See FAR Subpart 46.7 and DFARS Subpart 246.7 .)

NOTES

1. The Program Manager (PM) should examine the value of warranties on major systems and pursue them when appropriate and cost-effective. If appropriate, the PM should incorporate warranty requirements into major systems contracts in accordance with FAR Subpart 46.7.
2. Warranty program data should be included in the Life-cycle Sustainment Plan (*see Guidebook Chapter 5*).

2.8.7.5.12. Multiyear Contracting

If this strategy is for Milestone C or later, indicate whether the production program is suited to the use of multiyear contracting (10 USC 2306b). Indicate any plans for multiyear contracting and address compliance with 10 USC 2306c and Office of Management and Budget (OMB) Circular A-11 .

NOTES

1. In accordance with 10 USC 2306b, the Acquisition Strategy should address the PM's consideration of multiyear contracting for full rate production, and address the PMs assessment of whether the production program is suited to the use of multiyear contracting based on the requirements in FAR Subpart 17.1. Similarly, the Acquisition Strategy should address the PMs consideration of the criteria of 10 USC 2306c when considering a multiyear contract for "covered" services.
2. If the acquisition strategy calls for a multi-year service contract (as distinguished from contracts that span multiple years, (see FAR Subpart 17.1 and DFARS Subpart 217.171), the strategy shall address compliance with 10 USC 2306c and OMB Circular A-11. OMB Circular A-11 requires that multiyear service contracts be scored as operating leases. Therefore, the Acquisition Strategy shall address the budget scorekeeping that will result from use of the proposed contracting strategy.

2.8.7.5.13. Leasing

Indicate whether leasing was considered (applies to use of leasing in the acquisition of commercial vehicles and equipment) and, if part of the strategy, economically justify that leasing of such vehicles is practicable and efficient and identify the planned length of

the lease.

NOTES

1. The Program Manager (PM) should consider the use of leasing in the acquisition of commercial vehicles and equipment whenever the PM determines that leasing of such vehicles is practicable and efficient. Leases are limited to an annual contract with no more than a 5-month lease option.
2. The PM may not enter into any lease with a term of 18 months or more, or extend or renew any lease for a term of 18 months or more, for any vessel, aircraft, or vehicle, unless the PM has considered all costs of such a lease (including estimated termination liability) and has determined, in writing, that the lease is in the best interest of the Government (10 USC 2401a and DFARS 207.4). It should be noted that a lease of more than 12 months does not permit the extension of one year funding authority.
3. Leases of equipment to meet a valid need under the provisions of CJCS Instruction 3170.01 will be categorized in accordance with the criteria in DoD Instruction 5000.02<GB 5000.02>.
4. For further guidance on leasing, see Office of Management and Budget (OMB) Circular A-11, Appendix B, Budgetary Treatment of Lease-Purchases and Leases of Capital Assets; and OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs.
5. Additionally 10 USC 2401 must be met for long-term services contracts where the contractor will use a vessel, aircraft or combat vehicle to perform the services. This statute (Section 2401) also applies to long-term leases and charters of vessels, aircraft and combat vehicles. This statute bars entry into such a contract unless the Secretary of a military department has been specifically authorized by law to enter the contract. Section 2401 requires the Secretary of the military department must notify Congressional committees before issuing a solicitation for such a contract. Section 2401 also requires the Secretary must notify the committees of detailed information regarding the proposed contract and must certify that certain criteria and laws have been satisfied (as set out in Section2401).

2.8.7.5.14. Modular Contracting (Major Information Technology programs only)

Quantify the extent to which the program is implementing modular contracting (41 USC 2308).

CONSIDERATION

1. The Program Manager should consider use of modular contracting, as described in FAR Section 39.103, for major IT acquisitions, to the extent practicable.
2. Similarly, before an agency can consolidate contract requirements with an estimated value exceeding $5.5M, DFARS 207.170-3 requires the Acquisition Strategy must contain the results of market research, alternative contracting approaches, and a determination by the senior procurement executive that the consolidation is necessary and justified.

2.8.7.5.15. Payment

Identify financing method(s) planned and whether these provision(s) will be flowed down to subcontractors. Indicate if early progress payments will be traded off for lower prices in negotiations.

2.8.7.5.16. Other Relevant Information

Provide any other pertinent information that may enhance understanding of the contracting strategy.

2.8.7.6. Technical Data Rights Strategy (formerly the Data Management Strategy)

2.8.7.6.1. Technical Data Analysis

2.8.7.6.2. Provision of Technical Data Rights in Sustainment

2.8.7.6.3. Business Case Analysis (BCA) with Engineering Tradeoff Analysis

2.8.7.6.4. BCA with Priced Contract Option for Future Delivery of Technical Data

2.8.7.6.5. Risk Analysis

2.8.7.6. Technical Data Rights Strategy (formerly the Data Management Strategy)

Summarize the Technical Data Rights strategy for meeting product life-cycle data rights requirements and to support the overall competition strategy.

NOTE

1. **The intent of the Government is the ensure there is a sufficient amount of product related technical data rights to allow DoD to use, modify, reproduce, release, perform, display, or disclose data for use only within the Government and to support the products lifecycle related acquisition activities. Program managers for major weapon systems and subsystems of major weapon systems are required to assess the long-term technical data needs of such systems and subsystems and establish acquisition strategies that provide for technical data rights needed to sustain such systems and subsystems over their life cycle. The Technical Data Rights Strategy must contain at least the content specified by statute as delineated by the following:**
    - **10 USC 2320**
    - **Public Law 109-364**
    - **DFARS part 227**
2. **If programs either do not secure the data rights that the Government is granted or do not acquire additional data rights needed to support the system the result could be programs tied to a specific contractor (i.e., vendor locked or sole sourced) for one solution over the entire system lifecycle with no opportunity for competition and associated competitive prices, and little opportunity to tap the innovation of other vendors.**

2.8.7.6.1. Technical Data Analysis

Analysis of the data required to design, manufacture, and sustain the system as well as to support re-competition for production, sustainment, or upgrade. The strategy should consider, but is not limited to, baseline documentation data, analysis data, cost data, test data, results of reviews, engineering data, drawings, models, and Bills of Materials (BOM).

NOTE

Summarize how long term needs for data were assessed, including data needed to support subsystems and components of the total system. This assessment should consider the needs of the entire life cycle, extending through operations to disposal. Potential competition/re-competition for procurement of the system, subsystems, components, logistics support including spare and repair parts should be included.

CONSIDERATION

Managers should consider, when cost effective, the acquisition (e.g. via necessary contract data requirements and data rights licensing agreements) of complete technical data packages to ensure competition, or the option of competition, at both the prime and subcontractor level throughout the products life cycle.

2.8.7.6.2. Provision of Technical Data Rights in Sustainment

Specify how the program will provide for rights, access, or delivery of technical data the government requires for the systems total life cycle sustainment. Include analysis of data needs to implement the product support life cycle strategy including such areas as materiel management, training, Information Assurance protection, cataloging, open architecture, configuration management, engineering, technology refreshment, maintenance/repair within the technical order (TO) limit's and specifically engineered outside of TO limit's, and reliability management.

CONSIDERATIONS

In this section the Program Manager should describe:

1. **The overall management approach to managing data acquired with other than unlimited rights.**
2. **The management approach for management data (i.e. data that is not software or technical data). It should include how contractor data needing protection will be identified, marked, and managed.**
3. **How the data deliverables will be reviewed for unjustified or non-conforming markings. It should include the process the program will follow to question or challenge contractor assertions or markings**
4. **The data deliverables specified in the RFP or contract, including the technical data, computer software documentation, and management data items.**
5. **The approach for maintaining the software and it's documentation once software maintenance is transferred from the OEM. It should include the contract provisions being put into place that will allow for a cost effective migration.**
6. **The degree to which data will be acquired to support future competitions. It should include the logic by which these elements were selected; the alternative solutions considered; and the criteria by which the decision to procure technical data was made.**
7. **The extent to which priced options and associated source selection criteria will be used to acquire additional licenses.**
8. **The intended use of other mechanisms such as deferred ordering, deferred delivery, and the use of withholding or incentives specific to performance in the area of data management.**
9. **How the use of an integrated digital environment and the repository system factors into the data strategy.**
10. **Any required interfaces to government data systems or repositories, and how those requirements will be satisfied.**
11. **The digital format standards to be used and why they were selected. The process (i.e., business case analysis, adherence to DoD Component policy, etc.) used to determine the deliverable form/format for all deliverables should be included.**

2.8.7.6.3. Business Case Analysis (BCA) with Engineering Tradeoff Analysis

The business case analysis calculation, conducted in concert with the engineering tradeoff analysis that outlines the approach for using open systems architectures and acquiring technical data rights.

CONSIDERATIONS

1. **Business case development for open systems architecture and data rights is a process of analyzing alternative acquisition decisions to be undertaken for a given system to derive quantifiable costs as well as benefit's for these alternative decisions. The business case should provide evidence that justifies an investment decision for the purposes of implementing (or not implementing) an open systems architecture or acquiring (or not acquiring) data rights for the program being examined.**
2. **Data needs must be established giving consideration to the: contractor's economic interests in data pertaining to items, components, or processes that have been developed at private expense; the Government's costs to acquire, maintain, store, retrieve, and protect the data; procurement needs; repair, maintenance and overhaul philosophies; spare and repair part considerations; and whether procurement of the items, components, or processes can be accomplished on a form, fit, or function basis.**
3. **A candidate business case analysis process includes these steps:**
    - **Step 1 - Stand Up the Business Case Project Team**
    - **Step 2 Identify and Analyze Assumptions and Alternatives**
    - **Step 3 - Evaluate Risk**
    - **Step 4 - Assess Overall Business Case and Key Alternatives**
    - **Step 5 - Address Uncertainty for Selected Alternatives**
    - **Step 6 - Package and Present Results**
    - **Step 7 - Business Case Closeout**

2.8.7.6.4. BCA with Priced Contract Option for Future Delivery of Technical Data

The cost benefit analysis of including a priced contract option for the future delivery of technical data and intellectual property rights not acquired upon initial contract award.

NOTE

1. **Data rights cost estimates can be secured using the following approaches:**
    - **Data rights costs can be requested before any milestone by placing a Request for Quote (RFQ) with the contractor/s. The responses to this RFQ can then be used to support a business case analysis for acquiring technical data rights in support of future product acquisition activities.**
    - **Prior to Milestones A & B, an option to acquire additional data rights can be included in the Request for Proposal (RFP) as part of the proposal evaluation process. The costs provided can then be used to support a business case analysis for acquiring additional rights.**
    - **For those programs which already have existing contracts, a task order can be issued under the current contract for the contractor to provide the cost estimate for additional data rights necessary to maintain the prospect for competition throughout the systems life cycle.**
2. **The cost benefit analysis information for this element of the Program Strategy document is candidate to be a result of the business case analysis referenced in the previous section.**

2.8.7.6.5. Risk Analysis

Analysis of the risk that the contractor may assert limitations on the governments use and release of data, including Independent Research and Development (IRAD)-funded data (e.g., require the contractor to declare IRAD up front and establish a review process for proprietary data).

CONSIDERATION

Types of Data Rights for consideration:

	Applies to These Types of TD or CS	Rights Criteria	Permitted Uses Within the Government	Permitted Uses by Third Parties Outside the Government
Unlimited Rights (UR)	Noncommercial TD and CS	Developed exclusively at Government expense, and certain types of data (e.g.,FFF, OMIT, CSD)	All uses; no restrictions	All uses; no restrictions
Government Purpose Rights (GPR)	Noncommercial TD and CS	Developed with mixed funding	All uses; no restrictions	For "Government Purposes" only; no commercial use
Limited Rights (LR)	Noncommercial TD only	Developed exclusively at private expense	Unlimited; except may not be used for manufacture	Emergency repair or overhaul
Restricted Rights (RR)	Noncommercial CS only	Developed exclusively at private expense	Only one computer at a time; minimum backup copies; modification.	Emergency repair/overhaul; certain service/maintenance contracts
Negotiated License Rights	Any/all TD and CS including commercial TD and CS	Mutual agreement of the parties; use whenever the standard categories do not meet both parties needs	As negotiated by the parties; however, must not be less than LR in TD and must not be less than RR in noncommercial CS (consult with legal counsel as other limit's apply)	
SBIR Data Rights	Noncommercial TD and CS	All TD or CS generated under an SBIR	All uses; no restrictions	Cannot release or disclose except to Government support

		contract		contractors
Commercial TD License Rights	Commercial TD only	TD related to commercial items (developed at private expense)	Unlimited in FFF and OMIT; other rights as negotiated	
Commercial CS Licenses	Commercial CS only	Any commercial CS or CS documentation	As specified in the commercial license customarily offered to the public	

TD = Technical Data

CS = Computer Software

2.8.7.7. Contract Management

2.8.7.7.1. Contract Administration

2.8.7.7.2. Priorities, allocations, and allotments

2.8.7.7.3. Delivery/Performance Period Requirements

2.8.7.7. Contract Management

2.8.7.7.1. Contract Administration

Summarize how the contract(s) will be administered. Include how inspection and acceptance corresponding to the work statements performance criteria will be enforced (see FAR Part 42).

2.8.7.7.2. Priorities, allocations, and allotments

When urgency of the requirement dictates a particularly short delivery or performance schedule, certain priorities may apply. If so, specify the method for obtaining and using priorities, allocations, and allotments, and the reasons for them (see FAR Subpart 11.6).

2.8.7.7.3. Delivery/Performance Period Requirements

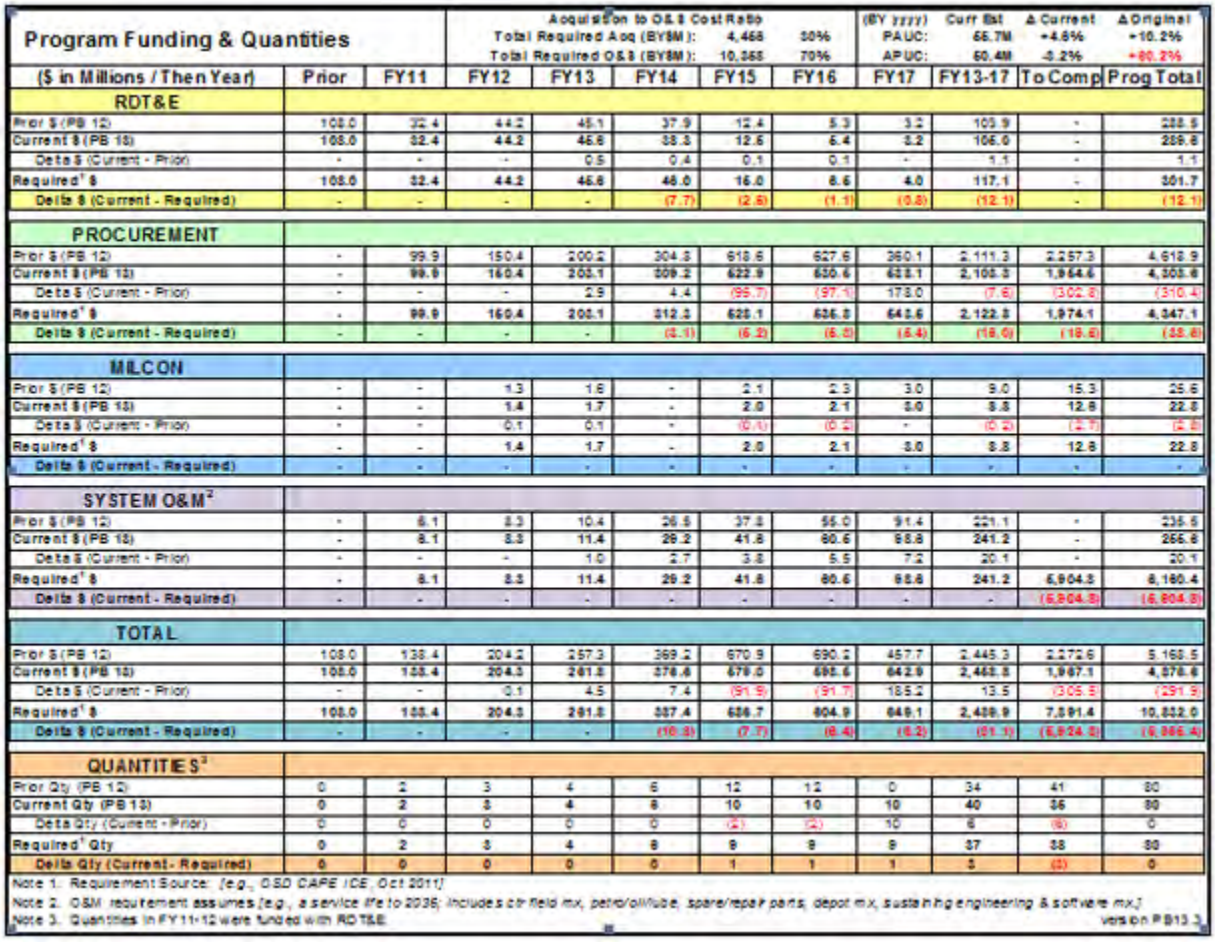
Indicate the basis for establishing delivery or performance-period requirements.

2.8.8. Resources

2.8.8.1. Investment Program Funding and Quantities

Provide a copy of the programs "Investment Program Funding and Quantities" Chart (see Figure 4), with a current "as of date." A template and instructions for the development of this chart are provided at: https://ebiz.acq.osd.mil/DABSchedule/Questions.aspx?text=IPT (login with password or Common Access Card required).

Figure 4. Example "Investment Program Funding and Quantities" Chart



Program Funding & Quantities			Acquisition to O&S Cost Ratio Total Required Acq (BY$M): 4,468 30% Total Required O&S ($M): 10,368 70%					(BY yyyy) PAUC: APUC:	Curr Est 65.7M 60.4M	Δ Current +4.8% -8.2%	Δ Original +10.2% +80.2%
($ in Millions / Then Year)	Prior	FY11	FY12	FY13	FY14	FY15	FY16	FY17	FY13-17	To Comp	Prog Total
RDT&E											
Prior $ (PB 12)	108.0	32.4	44.2	46.1	37.9	12.4	5.3	3.2	103.9	-	288.5
Current $ (PB 13)	108.0	32.4	44.2	46.6	38.3	12.5	6.4	3.2	106.0	-	289.8
Delta $ (Current - Prior)	-	-	-	0.5	0.4	0.1	0.1	-	1.1	-	1.1
Required[1] $	108.0	32.4	44.2	46.6	46.0	16.0	8.6	4.0	117.1	-	301.7
Delta $ (Current - Required)	-	-	-	-	(7.7)	(2.5)	(1.1)	(0.8)	(12.1)	-	(12.1)
PROCUREMENT											
Prior $ (PB 12)	-	99.9	150.4	200.2	304.3	618.6	627.6	360.1	2,111.3	2,257.3	4,618.9
Current $ (PB 13)	-	99.9	150.4	203.1	309.2	622.9	630.6	623.1	2,105.3	1,964.6	4,303.8
Delta $ (Current - Prior)	-	-	-	2.9	4.4	(95.7)	(97.1)	178.0	(7.6)	(302.8)	(310.4)
Required[1] $	-	99.9	150.4	200.1	312.3	628.1	636.8	643.6	2,122.8	1,974.1	4,347.1
Delta $ (Current - Required)	-	-	-	-	(3.1)	(5.2)	(6.2)	(6.4)	(16.6)	(10.6)	(33.8)
MILCON											
Prior $ (PB 12)	-	-	1.3	1.6	-	2.1	2.3	3.0	9.0	15.3	25.6
Current $ (PB 13)	-	-	1.4	1.7	-	2.0	2.1	3.0	8.8	12.8	22.8
Delta $ (Current - Prior)	-	-	0.1	0.1	-	(0.1)	(0.2)	-	(0.2)	(2.7)	(2.9)
Required[1] $	-	-	1.4	1.7	-	2.0	2.1	3.0	8.8	12.8	22.8
Delta $ (Current - Required)	-	-	-	-	-	-	-	-	-	-	-
SYSTEM O&M[2]											
Prior $ (PB 12)	-	8.1	8.3	10.4	26.5	37.3	55.0	91.4	221.1	-	235.5
Current $ (PB 13)	-	8.1	8.3	11.4	29.2	41.8	80.6	88.8	241.2	-	255.6
Delta $ (Current - Prior)	-	-	-	1.0	2.7	3.8	5.5	7.2	20.1	-	20.1
Required[1] $	-	8.1	8.3	11.4	29.2	41.8	80.6	88.8	241.2	6,904.8	6,160.4
Delta $ (Current - Required)	-	-	-	-	-	-	-	-	-	(6,904.8)	(6,904.8)
TOTAL											
Prior $ (PB 12)	108.0	138.4	204.2	257.3	369.2	670.9	690.2	457.7	2,445.3	2,272.6	5,168.5
Current $ (PB 13)	108.0	138.4	204.3	261.8	376.6	679.0	695.6	642.9	2,463.8	1,967.1	4,578.8
Delta $ (Current - Prior)	-	-	0.1	4.5	7.4	(91.9)	(91.7)	185.2	13.5	(305.5)	(291.9)
Required[1] $	108.0	138.4	204.3	261.8	387.4	686.7	804.9	848.1	2,488.9	7,891.4	10,832.0
Delta $ (Current - Required)	-	-	-	-	(10.8)	(7.7)	(8.4)	(5.2)	(31.1)	(5,924.3)	(6,266.4)
QUANTITIES[3]											
Prior Qty (PB 12)	0	2	3	4	6	12	12	0	34	41	80
Current Qty (PB 13)	0	2	3	4	6	10	10	10	40	36	80
Delta Qty (Current - Prior)	0	0	0	0	0	(2)	(2)	10	6	(6)	0
Required[1] Qty	0	2	3	4	6	9	9	9	37	38	80
Delta Qty (Current - Required)	0	0	0	0	0	1	1	1	3	(2)	0

Note 1. Requirement Source: *[e.g., OSD CAPE ICE, Oct 2011]*
Note 2. O&M requirement assumes *[e.g., a service life to 2036; includes cntr field mx, petro/oil/lube, spare/repair parts, depot mx, sustaining engineering & software mx.]*
Note 3. Quantities in FY11-12 were funded with RDT&E. version PB13.3

If the chart reflects funding shortfalls, indicate how they will be addressed and state the programmatic impact if they are not.

If the program is jointly funded, provide a separate chart reflecting the funding contributions required of each joint participant.

Provide and briefly explain funding support from the Working Capital Fund.

If multiple program increments are in progress, funding will be tracked separately for each increment (e.g., for subsets of the program that will be subject to a separate Acquisition Program Baseline). Provide separate charts for each increment.

2.8.8.2. Cost

Indicate the established cost goals for the increment and the rationale supporting them.

If a Technology Development Strategy, indicate the Affordability Target that has been

established for the program (initially, average unit acquisition cost and average operational support cost per unit). The affordability target should be presented in the context of the resources that are projected to be available in the portfolio(s) or mission area(s) associated with the program under consideration. For new start programs, provide the quantitative analytical basis for determining that the resources expected to be available in the portfolio/mission area can support the program under consideration. Employ a graphic to illustrate.

For Production Phase Acquisition strategies (including at Full-Rate Production) for ACAT I programs will specify (no more than one page) how the procurement rate and schedule were set, with reference to Economic Order Quantity (EOQ) and the affordability target set at Milestone A, as adjusted at Milestone B.

2.8.8.3. *Should-Cost*

Summarize the application of should-cost analysis to the acquisition. Identify the should-cost initiatives that have been planned for the program. Specify how the associated "should cost targets" will be used as a basis for contract negotiations and contract incentives, and to track contractor, PEO, and PM performance.

CONSIDERATIONS

1. **Explain if Should-Cost estimates were calculated using a Bottom Up approach, or if reductions were identified from "Will-Cost" estimates.**
2. **List discrete and measurable items or initiatives that were identified in the Should-Cost Estimate. Include the projected cost savings for each initiative. Initiatives should both be explained and presented in a chart that includes "Will Cost," Should Cost, and the Delta for each item. In the Acquisition Strategy, Should-Cost initiatives should be categorized as:**
    - **a. Near-term (within the program manager's tenure) or long-term initiatives; and,**
    - **b. Program driven (within program manager's control), "Service Driven (within the services control)," or "Externally Driven (outside service control)."**
3. **The presentation of each initiative should include a description, an implementation timeline identifying key events, associated risks, involved stakeholders and "help needed" of senior leaders.**
4. **Summarize the application of should-cost analysis to the acquisition. Identify the should-cost initiatives that have been planned for the program. Specify how the associated "should cost targets" will be used as a basis for contract negotiations and contract incentives, and to track contractor, PEO, and PM performance.**

2.8.8.4. Funds Management

Explain how the cost management approach adequately considers funds management. Identify any contingent liabilities (award fee, special incentives, economic price adjustment, business base clauses, termination liability, etc.) planned for or associated with the program. Identify which contingent liabilities have been funded. Summarize the plan to obtain approval for any unfunded contingencies (see DFARS 217.171.a.(4) and 217.172.(e)).

For acquisitions of Federal Information Processing resources with expected costs greater than $100 million, identify the key outcome performance measures. Indicate the tracking system that will be used to measure and report on selected outcome performance measures.

Summarize plans to control program costs, specifically Program Acquisition Unit Cost,

Average Procurement Unit Cost, and Life-Cycle Cost. List and describe cost control tools and processes.

Summarize the process to update estimates (e.g., x months before each decision review or x months before beginning each increment).

2.8.8.5. Program Office Staffing and Organization

2.8.8.5.1. Manning Profile

Provide a time-phased workload assessment identifying the manpower and functional competencies required for successful program execution. Considering the overall, technical, acquisition, sustainment, and management approach, specify the number of personnel, by functional area, that are required to manage this program for the next phase and through fielding. Include a projected manning profile based upon the overall approach and program schedule for government, Systems Engineering and Technical Assistance, and Federally Funded Research and Development Center(s) support.

2.8.8.5.2. Organization Chart

Provide an organization chart reflecting program manning requirements by functional area. Identify the Services filling billets for a joint program. Prepare a table to indicate whether billets are military, civilian, or contractor, the seniority level of the billets, and if the billets are currently filled or vacant. (See Table 5.)

Table 5. Notional table of Program Manning Requirements

PROGRAM MANNING REQUIREMENTS						
Billet ID	**Billet Name**	**(If Joint) DoD Component**	**Manning Type**	**Seniority Level**	**DAWIA Level**	**Fill Status**

2.8.8.5.3. Acquisition Chain of Authority

Indicate specific lines of programmatic authority. Show how the authority chain meets the requirements identified in DoD Directive 5000.01, paragraph E.1.1.26 .

2.8.8.5.4. Identify the Primary Stakeholders

Indicate the planned organization to effectively manage the program and ensure all stakeholders are involved (Integrated Product Teams (IPT), boards, reviews, etc.). If applicable, indicate how the contractor will be involved in program IPTs. Summarize the

anticipated business management relationship between (1) the program office and the contractor, and (2) the program office and other government agencies.

NOTE

This section must also address Requirements Community involvement and specify how the customer-representing organization will interface with the program management office and acquisition chain of command to provide for timely and effective review of requirements and/or cost trade-offs. Define levels of authority required to change requirements of various types should be defined.

2.8.9. International Involvement

2.8.9.1. Limitations on Foreign Contractors

2.8.9.2. International Cooperation

2.8.9.3. Foreign Military Sales

2.8.10. Industrial Capability and Manufacturing Readiness

2.8.10.1. Industrial Capability

2.8.10.2. Industrial and Manufacturing Readiness (not applicable to software-intensive programs without production components)

2.8.10.3. Sustaining Industrial Capabilities

2.8.11. Life-Cycle Signature Support

2.8.12. Military Equipment Valuation

2.8.9. International Involvement

2.8.9.1. Limitations on Foreign Contractors

Indicate any limitations on foreign contractors being allowed to participate at the prime contractor level.

NOTE

Restricting foreign competition for the program due to industrial base considerations requires prior USD(AT&L) approval.

2.8.9.2. International Cooperation

Identify needs for system or subsystems to be interoperable with international partners .

Summarize any plans for cooperative development with foreign governments or cognizant organizations. List the MOAs in place and identify the contracting activities.

Summarize plans to increase the opportunity for coalition interoperability as part of the developing DoD program.

Employ the AT&L-developed template [1] to provide a coalition interoperability section in the Acquisition Strategy. Using the template will satisfy the cooperative opportunities document requirement of 10 USC 2350a .

CONSIDERATIONS

Evaluate cooperative opportunities with NATO, NATO organizations, member nations of NATO, major non NATO allies and friendly foreign countries (hereafter referred to as "international partners".

Indicate whether or not a similar project in development, production or sustainment by the Department of Defense provides interoperability with international partners systems that military operations rely upon and should be maintained in the new program.

Identify any relevant cooperative project work already conducted or under current collaboration with potential international partners (including at subcomponent levels) that can be utilized as a basis for cooperation in the new development or production program.

Assess whether any of these projects could satisfy, or could be modified in scope so as to satisfy (at the system of component level), the military requirements of the project of the United States under consideration by the Department of Defense.

State the determination of whether the capability would be enhanced by engaging critical global or regional partners in the development or production of the system for which new cooperative relationships are needed.

Assess the advantages and disadvantages with regard to program timing, developmental and life cycle costs, technology sharing, and Rationalization, Standardization, and Interoperability (RSI) of seeking to structure a cooperative development program with one or more potential international partners.

Address how current political and strategic guidance for cooperation affects opportunities for cooperative development of the capability with coalition partners (QDR, GEF, NSS, NSPDs, etc.).

Address releasability of technical information and exportability to potential international partners.

Summarize any plans for cooperative development with potential international partners.

List any international agreements planned or existing (e.g. MOAs, MOUs, etc.) in place and identify any current contracting activities with potential international partners.

CONSIDERATION

Include a proposed time phased approach for cooperative opportunities to integrate with acquisition schedules and milestones.

2.8.9.3. Foreign Military Sales

Specify the potential (MS A) or plans (MS B; MS C) for Foreign Military and/or Direct Commercial Sale and the impact upon program cost due to program protection and incorporation of exportability features.

CONSIDERATION

For EMD AS and P&D AS: If Foreign Military and/or Direct Commercial Sale are anticipated, include Planned Timelines for the following:

- **Foreign Military Sales**
- **Direct Commercial sales**
- **Loans of equipment to support operations**

2.8.10. Industrial Capability and Manufacturing Readiness

2.8.10.1. Industrial Capability

Summarize the results of industrial capability analysis (public and private) to design, develop, produce, support, and, if appropriate, restart the acquisition program.

CONSIDERATIONS

1. **If a TDS, identify and address how and when the industrial capability analysis (public and private) to design, develop, produce, support, and, if appropriate, restart the acquisition program will be performed in the TD Phase. Summarize the relevant findings of the Analysis of Alternatives, when applicable.**
2. **For an AS, specify the impact of this programs acquisition strategy on the national technology and industrial base. Briefly summarize the analysis used to make this determination.**
    - **Specify the findings relevant to (1) a competitive marketplace; (2) the viability of any associated essential industrial/technological capabilities; and (3) the potential viability of non-selected firms as enduring competitors for defense products**
3. **For an AS - If the industrial capability analysis revealed constraints, summarize how they will be managed, and the plan for future assessment, including frequency.**

2.8.10.2. Industrial and Manufacturing Readiness (not applicable to software-intensive programs without production components)

CONSIDERATIONS

- **Estimate (Technology Development Strategy), define (Engineering & Manufacturing Development Acquisition Strategy), or update (Production &Deployment Acquisition Strategy) the risk of industry being unable to provide program design or manufacturing capabilities at planned cost and schedule.**
- **(For Acquisition Strategies only) Identify the Manufacturing management approach and Quality Management systems and summarize how they will contribute to minimizing cost, schedule, and performance risks throughout the product life cycle.**

2.8.10.3. Sustaining Industrial Capabilities

(For Acquisition Strategy only) Summarize the make-or-buy approach to establish

and maintain access to competitive suppliers for critical areas at system, subsystem, and component level (e.g., requiring an open-systems-architecture or a make-or-buy plan). **List critical items and their sources.**

When the analysis indicates that the needed industrial capabilities are in danger of being lost, the strategy should indicate whether government action is required to preserve the industrial capability. The strategy should also address product technology obsolescence, replacement of limited-life items, regeneration options for unique manufacturing processes, and conversion to performance specifications at the subsystems, component, and spares levels.

Identify any planned or completed MOAs.

NOTE

When appropriate, Program Managers should consider including industrial surge requirements and capability for operationally-expendable items such as munitions, spares, and troop support items in their Program Strategies. Production bottlenecks at both the prime and sub-tier supplier levels for high use/high volume programs in an immediate warfare construct should be cited. Surge capability can be included in evaluation criteria for contract award.

2.8.11. Life-Cycle Signature Support

If a Technology Development Strategy, provide a table (see example Table 6) that indicates the program life-cycle signature support requirements. Identify the mission data type (signatures, electronic warfare integrated reprogramming, order of battle, geospatial intelligence, and system characteristics and performance data sets); specific subcategories, if known (Radar, Thermal, Acoustic, etc.); the domain (Space, Air, Land, Naval, Missile Defense, etc.); subcategories within the domain (e.g., for Air domain: Fighter Aircraft); and data fidelity required, if known (e.g., dB, C, resolution, Hz, etc.). If additional or more-specific requirements have been identified, they should be included.

Table 6. Notional Table of Life-Cycle Signature Support Requirements

Life-Cycle Signature Support Requirements				
Mission Type	**Mission Type Subcategory**	**Domain**	**Domain Subcategory**	**Data Fidelity**

Life-cycle signature support funding requirements will be reflected in the program funding summary (see Paragraph 2.8.8.1 and Figure 4).

CONSIDERATION
In order to estimate the funding requirements, the Program Manager must identify the systems and subsystems of the program that require signature or intelligence mission data in order to deliver the intended capabilities.

NOTES

1. **A signature-dependent program is one that utilizes or is comprised of a sensor, system, or process that relies on signatures or signature data to successfully perform a task or mission. Signatures are defined as: a distinctive basic characteristic or set of characteristics that consistently re-occurs and uniquely identifies a piece of equipment, activity, individual, or event and could be defined in a variety of phenomenology such as acoustic, radio frequency, visible wavelengths, ocean wake, olfactory, etcetera.**
2. **New terminology is being developed to be used in lieu of signatures, specifically intelligence mission data, however their meanings and implications are the same.**
3. **Intelligence mission data is DoD intelligence used for programming platform mission systems in development, testing, operations and sustainment including, but not limited to, the following functional areas: signatures, EWIR, OB, C&P, and GEOINT. IMD does not include products or information regarding foreign threats or systems unless it is specifically to be used in mission systems such as a mission computer or sensors threat library. IMD does not include signatures, EWIR, OB, C&P, GEOINT or modeling and simulation data that is to be used in assessments, documents or simulations such as the Joint Country Force Assessment, System Threat Assessment Reports, or war fighting analysis performed for budget or requirements development.**
4. **Intelligence mission data, or signatures, are needed for an increasing number and frequently increasingly complex program system that are needed for target identification, non-cooperative combat identification, and blue force tracking, etcetera.**
5. **DoDD 5250.01 requires that developmental acquisition programs identify, capture, and address the signatures essential to the development, testing, fielding, operation, and maintenance of required weapons, smart munitions, sensors, and systems capabilities at each program milestone and prior to proceeding to the Low-Rate Initial Production (LRIP), production and/or fielding decision. Fielded systems that are signature-dependent but have deficiencies in data and their ability to discriminate friendly from adversarial targets should also consider engaging the Intelligence Community to attain needed data.**

2.8.12. Military Equipment Valuation

Federal accounting standards require military equipment to be capitalized on the Departments financial statements. For Milestone C and the Full-Rate Production Decision, provide the following information for any program, project, product, or system that has deliverable end items with a unit cost at or above $100,000 (the current capitalization threshold):

- A level 2 work breakdown structure (as described in MIL_HDBK-881A) for reporting Military Equipment Valuation and Accountability;
- The end item(s) meeting the unit cost threshold (i.e., $100,000);
- The government furnished property that will be included in the end item;
- Other deliverables that will accompany the end item (e.g., manuals, technical data, etc.); and
- Other types of deliverables that will be purchased with program funding (e.g., initial spares, support equipment, special tooling and test equipment, etc.), but cannot be directly attributed to a specific end item.

(***NOTE:*** *The unit cost can be calculated by summing the estimated cost of the end item with the estimated costs of all associated government furnished equipment, training manuals, technical data, engineering support, etc., NOT including spares and support equipment. For additional information, see:*

- http://www.acq.osd.mil/pepolicy/training_tools/quick_reference_tools.html ; or
- http://www.acq.osd.mil/pepolicy/training_tools/bfma_instructions.html .)

DEFENSE ACQUISITION GUIDEBOOK
Chapter 3-- Affordability and Life-Cycle Resource Estimates

3.0. Overview

3.0.1. Purpose

This chapter addresses acquisition program affordability and resource estimation. It provides explanations of the Office of the Secretary of Defenses Office of Cost Assessment and Program Evaluations (CAPEs) policies and procedures as well as information required by DoD Instruction 5000.02, *Operation of the Defense Acquisition System*. DoD Instruction 7000.14 establishes DoD 7000.14-R as the DoD-wide financial management regulation (FMR) to be used by all DoD Components for accounting, budgeting, finance, and financial management education and training. The link to the FMR is provided as a convenience to the reader.

3.0.2. Contents

Section 3.1 provides introductory background material intended for a general audience. It describes the concept of program life-cycle cost, and provides definitions of terms used by the DoD cost community. It also introduces the concepts of total ownership cost and fully burdened cost of delivered energy.

The next five sections are more specialized; they discuss the specific milestone review procedures, expectations, and best practices for a variety of topics related to acquisition program affordability, cost, and manpower:

Section 3.2 describes the basic policies associated with the consideration of affordability in the acquisition process and offers parameters for preparing affordability analyses and constraints on investments. This section also explains the Department's full-funding policy.

Section 3.3 describes the Analysis of Alternatives process.

Section 3.4 describes the role of both DoD Component cost estimates and independent cost estimates in support of the DoD acquisition system.

Section 3.5 describes the review procedures for manpower estimates.

Section 3.6 discusses procedures unique to economic analyses of major automated information systems.

Section 3.7 is intended for less experienced cost analysts working in the acquisition community. This section, which is tutorial in nature, provides a recommended analytic approach for preparing a life-cycle cost estimate for a defense acquisition program.

3.1. Life-Cycle Costs/Total Ownership Costs

3.1.1. Introduction

3.1.2. Life-Cycle Cost Categories and Program Phases

3.1.3. Life-Cycle Cost Category Definitions

3.1.3.1. Research and Development Costs

3.1.3.2. Investment Costs

3.1.3.3. Operating and Support (O&S) Costs

3.1.3.4. Disposal Costs

3.1.4. Implications of Evolutionary Acquisition

3.1.5. Total Ownership Costs

3.1.6. Fully Burdened Cost of Delivered Energy

3.1.1. Introduction

Both DoD Directive 5000.01, *The Defense Acquisition System*, and DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, make reference to life-cycle cost and total ownership cost. This section of the Guidebook explains the meaning for each of these terms. The terms are similar in concept but somewhat different in scope and intent. For a defense acquisition program, life-cycle cost consists of research and development costs, investment costs, operating and support costs, and disposal costs over the entire life cycle. These costs include not only the direct costs of the acquisition program but also indirect costs that would be logically attributed to the program. In this way, all costs that are logically attributed to the program are included, regardless of funding source or management control.

The concept of total ownership cost is related but broader in scope. Total ownership cost includes the elements of life-cycle cost as well as other infrastructure or business process costs not normally attributed to the program. Section 3.1.5 defines and describes this concept in more detail.

Program cost estimates that support the defense acquisition system normally are focused on life-cycle cost or elements of life-cycle cost. Examples of cases where cost estimates support the acquisition system include affordability analyses, establishment of program cost goals for Acquisition Program Baselines, independent cost estimates, or estimates of budgetary resources. However, for programs that are pre-Milestone A or in the Engineering and Manufacturing Development Phase, cost estimates that are used within the program office to support system trade-off analyses, such as evaluations of design changes or assessments of energy efficiency, reliability, maintainability, and other supportability considerations, may need to be broader in scope than traditional life-cycle cost estimates to support the purpose of the analyses being conducted. Moreover, for mature programs (in transition from production and deployment to sustainment), cost estimates may need to be expanded in scope to embrace total ownership cost concepts in order to support broad logistics or management studies.

3.1.2. Life-Cycle Cost Categories and Program Phases

3.1.3. Life-Cycle Cost Category Definitions

3.1.3.1. Research and Development Costs

3.1.3.2. Investment Costs

3.1.3.3. Operating and Support (O&S) Costs

3.1.3.4. Disposal Costs

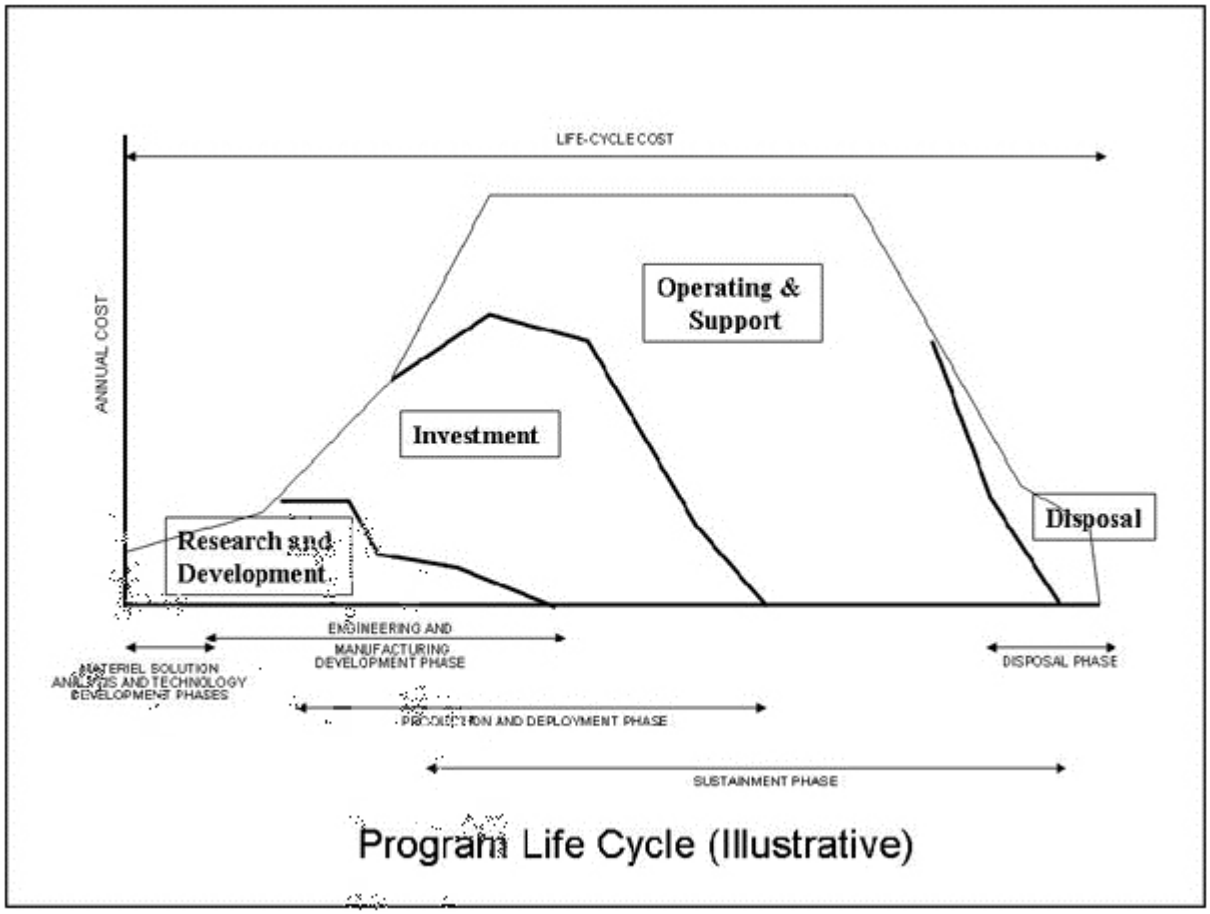
3.1.2. Life-Cycle Cost Categories and Program Phases

DoD 5000.4-M, *DoD Cost Analysis Guidance and Procedures*, provides the DoD definitions of cost terms used in describing system life-cycle costs. Life-cycle cost is the sum of the following four major cost categories, where each category is associated with sequential but overlapping phases of the program life cycle:

1. Research and development costs associated with the Materiel Solution Analysis phase, the Technology Development phase, and the Engineering and Manufacturing Development phase;
2. Investment costs associated with the Production and Deployment phase;
3. Operating and support costs associated with the sustainment phase; and
4. Disposal costs occurring after initiation of system phase out or retirement, possibly including demilitarization, detoxification, or long-term waste storage.

Figure 3.1.2.F1 depicts a notional profile of annual program expenditures by cost category over the system life cycle.

Figure 3.1.2.F1. Illustrative Program Life Cycle



3.1.3. Life-Cycle Cost Category Definitions

The following sections summarize the primary cost categories associated with each program life-cycle phase.

3.1.3.1. Research and Development Costs

Research and Development consists of development costs (both contractor and government) incurred from the beginning of the materiel solution analysis phase through the end of the Engineering and Manufacturing Development (EMD) Phase (excluding costs associated with Low-Rate Initial Production). This typically includes costs of materiel solution trade studies and advanced technology development; system design and integration; development, fabrication, assembly, and test of hardware and software for prototypes and/or engineering development models; system test and evaluation; systems engineering and program management; and product support elements associated with prototypes and/or engineering development models.

Research and Development costs are estimated and presented using the following categories:

Materiel Solution Analysis Phase

Technology Development Phase [Note: For programs with extensive prototyping and/or preliminary design activities that occur before Milestone B, the Technology Development Phase should be expanded with lower level cost categories, similar to the categories used in the EMD Phase]

Engineering and Manufacturing Development Phase:

- Prime Mission Product
- System Test and Evaluation
- Systems Engineering/Program Management
- Engineering Change Orders
- Peculiar Support Equipment
- Common Support Equipment
- Training
- Technical Publications and Data
- Initial Spares and Repair Parts
- Industrial Facilities
- Operational/Site Activation

Complete definitions and further details are provided throughout MIL-STD-881C, *Work Breakdown Structures for Defense Materiel Items*. Note the following:

- The Standard expands the Prime Mission Product category into more detailed elements. These lower level elements vary by product commodity (such as

aircraft, electronic system, missile system, sea system, or surface vehicle).

- Supportability analysis that defines the requirements for the logistics elements is part of Systems Engineering and planning and management associated with the logistics elements is part of Program Management.
- In most cost estimates, the Engineering Change Orders element is added to the Standard taxonomy to allow a contingency for design or other scope changes.
- In most cost estimates, the first four EMD elements shown above are subtotaled and displayed as Flyaway, Rollaway, Sailaway, or other similar term. The remaining EMD elements are often grouped together and labeled as "Acquisition Logistics," "Product Support Package," or other similar term.
- The Training element includes training equipment and devices, training course materials, and training services.
- Specialized facilities (fixtures, test chambers, laboratories, etc.) are considered part of the Work Breakdown Structure (WBS) element that they support. General brick and mortar type facilities are part of the Industrial Facilities element.
- Specialized contractor support is considered part of the WBS element that it supports. Contractor support associated with the service, maintenance or launch of prime mission systems is part of the Operational/Site Activation element.

An abbreviated version of the above format is used in Budget Exhibit R-3, RDT&E Project Cost Analysis, to display budget justifications and financial reporting for Research, Development, Test and Evaluation projects with budgets greater than $1 million in either budget year. *See* DoD 7000.14 R, Financial Management Regulation, Volume 2B, Chapter 5.

3.1.3.2. Investment Costs

Investment consists of production and deployment costs incurred from the beginning of low rate initial production through completion of deployment. This typically includes procurement costs associated with producing and deploying the primary hardware, systems engineering and program management, product support elements associated with production assets, military construction, and operations and maintenance associated with the production and deployment phase.

Investment costs are estimated and presented using the following categories:

Procurement

Prime Mission Product

System Test and Evaluation (if applicable)

Systems Engineering/Program Management

Engineering Change Orders

Peculiar Support Equipment

Common Support Equipment

Training

Technical Publications and Data

Initial Spares and Repair Parts

Industrial Facilities

Operational/Site Activation

Military Construction

Operations and Maintenance (acquisition-related during production and deployment)

Complete definitions and further details for the Procurement elements are provided throughout MIL-STD-881C, *Work Breakdown Structures for Defense Materiel Items*. Note the following:

- The Standard expands the Prime Mission Product category into more detailed elements. These lower level elements vary by product commodity (such as aircraft, electronic system, missile system, sea system, or surface vehicle).
- Supportability analysis that defines the requirements for the logistics elements is part of Systems Engineering, and planning and management associated with the logistics elements is part of Program Management.
- In most cost estimates, the Engineering Change Orders element is added to the Standard taxonomy to allow a contingency for design or other scope changes.
- In most cost estimates, the first four procurement elements shown above are subtotaled and displayed as Flyaway, Rollaway, Sailaway, or other similar term. The remaining procurement elements are often grouped together and labeled as "Acquisition Logistics," "Product Support Package," or other similar term.
- The Training element includes training equipment and devices, training course materials, and training services.
- Specialized facilities (fixtures, test chambers, laboratories, etc.) are considered part of the Work Breakdown Structure (WBS) element that they support. General brick and mortar type facilities are part of the Industrial Facilities element.
- Specialized contractor support is considered part of the WBS element that it supports. Contractor support associated with the service, maintenance or launch of prime mission systems is part of the Operational/Site Activation element.

An abbreviated modified version of the above format (procurement only) is used in Budget Exhibit P-5, Cost Analysis, to display budget justifications and financial reporting for procurement programs with budgets greater than or equal to $5 million in either

budget year. (See DoD 7000.14 R, Financial Management Regulation, Volume 2B, Chapter 4.)

3.1.3.3. Operating and Support (O&S) Costs

O&S consists of sustainment costs incurred from the initial system deployment through the end of system operations. This includes all costs of operating, maintaining, and supporting a fielded system. Specifically, this consists of the costs (organic and contractor) of manpower, equipment, supplies, software, and services associated with operating, modifying, maintaining, supplying, training, and supporting a system in the DoD inventory. This includes costs directly and indirectly attributable to the system (i.e., costs that would not occur if the system did not exist), regardless of funding source or management control. Direct costs refers to the resources immediately associated with the system or its operating unit. Indirect costs refers to the resources that provide indirect support to the system (including its manpower or facilities). For example, the pay and allowances for a unit-level maintenance technician would be treated as a direct cost, but the cost of medical support for the same technician would be an indirect cost.

Operating and Support costs are estimated and presented using the following categories:

Unit-Level Manpower

Operations Manpower

Unit-Level Maintenance Manpower

Other Unit-Level Manpower

Unit Operations

Operating Materiel

Energy (Fuel, Electricity, etc.)

Training Munitions and Expendable Stores

Other Operational Materiel

Support Services

Temporary Duty

Maintenance

Organizational Maintenance and Support

Intermediate Maintenance

Depot Maintenance

Sustaining Support

System Specific Training

Support Equipment Replacement

Operating Equipment Replacement

Sustaining Engineering and Program Management

Other Sustaining Support

Continuing System Improvements

Hardware Modifications or Modernization

Software Maintenance and Modifications

Indirect Support

Installation Support

Personnel Support

General Training and Education

Further details and complete definitions are provided in the Operating and Support Cost-Estimating Guide promulgated by the Director, Cost Assessment and Program Evaluation.

3.1.3.4. Disposal Costs

Disposal costs are the costs associated with demilitarization and disposal of a military system at the end of its useful life. Depending upon the characteristics of the system, demilitarization and disposal costs may be significant, so it is important to consider the costs early in the systems life cycle. Costs associated with demilitarization and disposal include disassembly, materials processing, decontamination, collection/storage/disposal of hazardous materials and/or waste, safety precautions, and transportation of the system to and from the disposal site. Systems may be given credit in the cost estimate

for resource recovery and recycling considerations.

The disposal cost category is intended to be used to ensure that design and other decisions made early in the program consider their effects on the specific long-term disposal costs that can be logically attributed to the program. Disposal costs of a more general nature, such as the removal of unexploded ordnance at a training range, would normally not be attributed to a specific aircraft program that in the future may participate in training exercises at that range.

Disposal costs may be estimated and presented using the following categories, subject to tailoring for the circumstances unique to each program:

Removal from Active Service

Demilitarization

Removal and Disposal of Hazardous Materials

Reclamation of Parts

Storage

Final Disposal or Salvage

3.1.4. Implications of Evolutionary Acquisition

3.1.5. Total Ownership Costs

3.1.6. Fully Burdened Cost of Delivered Energy

3.1.4. Implications of Evolutionary Acquisition

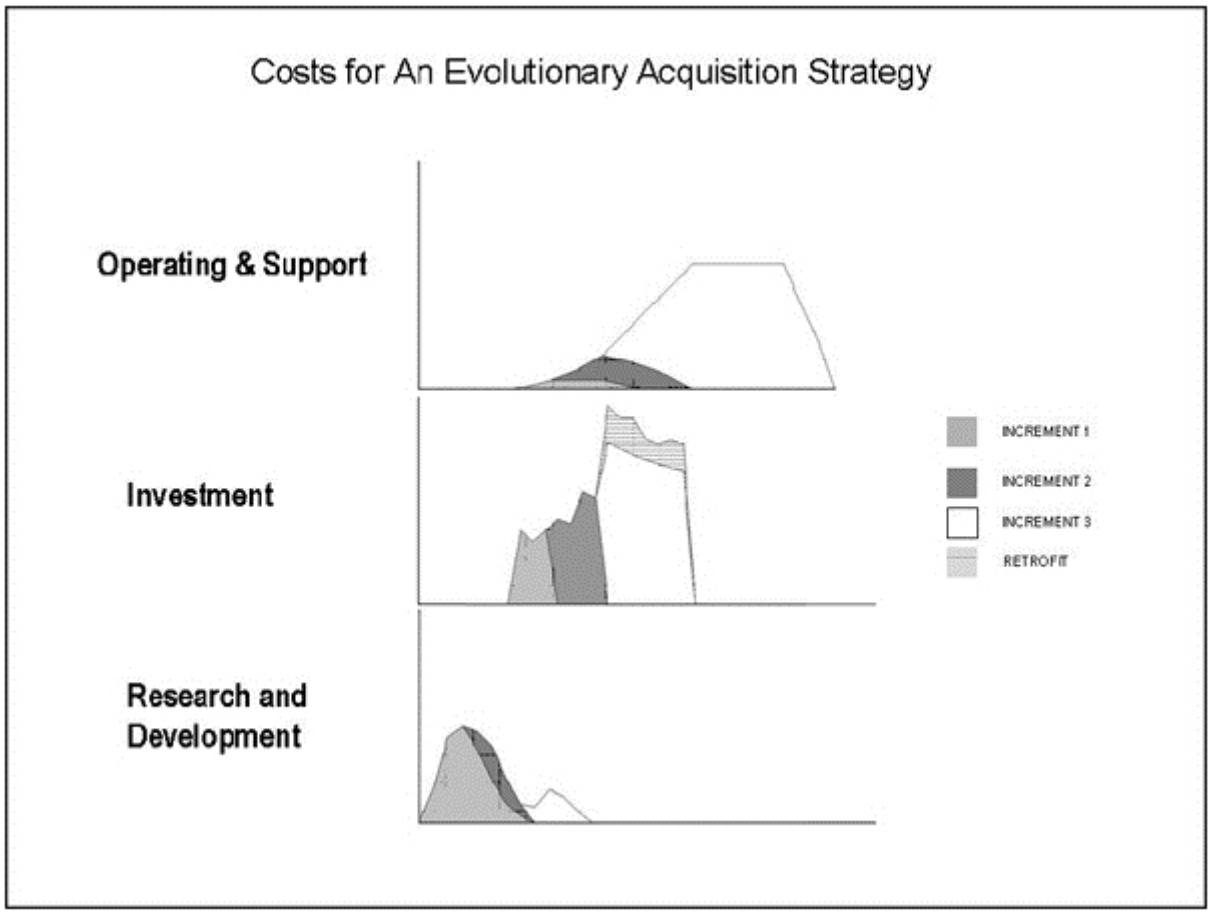
The application of life-cycle cost categories to program phases may need to be modified for programs with evolutionary acquisition strategies. DoD Instruction 5000.02, *Operation of the Defense Acquisition System*, Enclosure 2, paragraph 2, describes the evolutionary acquisition approach for acquisition programs. In an evolutionary approach, the ultimate capability delivered to the user is provided in increasing increments. Evolutionary acquisition strategies (1) define, develop, produce, and deploy an initial, militarily useful capability (Increment 1) based on proven technology, demonstrated manufacturing capabilities, and time-phased definition capabilities needs; and (2) plan up front for subsequent development, production, and deployment of increments beyond the initial capability over time (Increments 2 and beyond).

For a program with evolutionary acquisition, a question often arises concerning the

scope of the life-cycle cost estimate presented at a milestone review. Although the situation may vary somewhat depending on individual circumstances, the life-cycle cost estimate should attempt to address as much of the program, including known future increments, as can be defined at the time of the initial (Increment 1) milestone review. Any exclusions for portions of the program that cannot be defined at that time should be clearly identified.

The application of life-cycle cost categories and program phases (as described in Section 3.1.2) may need to be modified to account for the evolutionary acquisition strategy. Figure 3.1.4.F1 depicts a notional profile of annual program expenditures by cost category for a program with evolutionary acquisition.

Figure 3.1.4.F1. Illustrative Program Life Cycle under Evolutionary Acquisition



3.1.5. Total Ownership Costs

As explained earlier, total ownership cost includes the elements of a program's life-cycle cost as well as other related infrastructure or business processes costs not necessarily attributed to the program in the context of the defense acquisition system. Infrastructure is used here in the broadest possible sense and consists of all military department and

defense agency activities that sustain the military forces assigned to the combatant and component commanders. Major categories of infrastructure are support to equipment (acquisition and central logistics activities), support to military personnel (non-unit central "school-house" training, personnel administration and benefits, and medical care), and support to military bases (installations and communications/information infrastructure).

In general, traditional life-cycle cost estimates are often adequate in scope to support the review and oversight of cost estimates made as part of the acquisition system. However, depending on the issue at hand, the broader perspective of total ownership cost may be more appropriate than the life-cycle cost perspective, which may be too narrow to deal with the particular context. As discussed previously, for a defense acquisition program, life-cycle costs include not only the direct costs of the program but also certain indirect costs that would be logically attributed to the program. In a typical life-cycle cost estimate, however, the estimated indirect costs would include only the costs of infrastructure support specific to the program's military manpower (primarily medical support and system-specific training) and the program's associated installations or facilities (primarily base operating support and facilities sustainment, restoration, and modernization).

Many other important support or infrastructure activities such as recruiting and accession training of new personnel, individual training other than system-specific training, environmental and safety compliance, contract oversight support from the Defense Contract Management Agency and the Defense Contract Audit Agency, and most management headquarters functions, are normally not considered in the scope of a traditional acquisition program life-cycle cost estimate. In addition, important central (i.e., wholesale) logistics infrastructure activities such as supply chain management are implicitly incorporated in a traditional life-cycle cost estimate. The costs associated with central logistics infrastructure activities are somewhat hidden because the costs are reflected in the surcharges associated with working capital fund arrangements and are not explicitly identified. However, there could easily be cases where explicit consideration of such infrastructure activities would be important and would need to be recognized in a cost estimate or analysis. Examples of such cases are cost analyses tied to studies of alternative system support concepts and strategies; reengineering of business practices or operations; environment, safety, and occupational health considerations; and competitive sourcing of major infrastructure activities. In these cases, the traditional life-cycle cost structure may not be adequate to analyze the issue at hand, and the broader total ownership cost perspective would be more appropriate. For such instances, the typical life-cycle cost tools and data sources would need to be augmented with other tools and data sources more suitable to the particular issue being addressed.

One special case in which traditional life-cycle cost models and data sources need to be augmented is the inclusion of the fully burdened cost of delivered energy in trade-off analyses for certain tactical systems. This case is discussed in the next section.

3.1.6. Fully Burdened Cost of Delivered Energy

A Computational Framework for Acquisition Tradespace Analyses

Summary

In the acquisition process, the Fully Burdened Cost of Energy (FBCE) estimates the energy-related costs to sustain specific pieces of equipment, including procurement of energy, the logistics needed to deliver it where and when needed, related infrastructure, and force protection for those logistics forces directly involved in energy delivery. FBCE shall be applied in trade-off analyses conducted for all developmental Department of Defense (DoD) systems with end items that create a demand for energy in the battlespace. FBCE does not identify savings for programmatic purposes. It is an analytic input to the business case analysis designed to identify the difference in total energy-related costs among competing options. Consistent with Section 138c of title 10, United States Code, and DoDI 5000.02, FBCE estimates shall be made and reported for all acquisition category (ACAT) I and II systems that will demand fuel or electric power in operations and will be applied to all phases of acquisition beginning with the preparation of the Analysis of Alternatives (AoA). An FBCE estimate is also required as part of Total Ownership Cost (TOC) calculations. FBCE is not additive to Total Ownership Costs but rather is reported beside it. While TOC estimates are based on the total peace-time life of a system, FBCE estimates are based on short combat scenarios. They provide different but complementary insights.

Introduction

The energy required to field and sustain forces with current deployed systems poses significant operating costs and imposes several operational constraints on the larger force structure. First, growing logistics footprints can impede force mobility, flexibility, timing, and staging, especially for anti-access and irregular conflicts. Reducing the need for energy can have significant benefits for force deployability and the timeline of operations. Second, this logistics footprint presents a target for conventional, irregular, and catastrophic threats, creating demand for force protection and transportation forces. In the conflicts of the past decade, for example, adversaries have targeted U.S. fuel supply convoys, putting our forces and their missions at risk and redirecting combat power and dollars to fuel delivery.

Conversely, reducing system energy demand can make operational forces more agile and lethal by extending their range and reducing their dependence on logistics lines. These reductions can be achieved through different, better informed tradespace choices, design alternatives, technologies, and force structure concepts.

As outlined in the 2011 DoD Operational Energy Strategy, DoD is instituting procedures, frameworks, analytic tools and reporting requirements to better understand and manage how this energy demand affects force capability, vulnerability, and enterprise costs.

One of these frameworks, FBCE, is used to inform the acquisition tradespace by quantifying the per gallon price of fuel (or per kilowatt price of electricity) used per day for two or more competing materiel solutions. The FBCE estimate includes apportioned costs of the energy logistics forces needed to deliver and protect the fuel in a scenario. Calculating the FBCE gives DoD decision makers a way to more accurately consider the cost of a systems energy logistics footprint when making trades between cost, schedule, and performance. It has the added benefit of informing decisions on the size and focus of DoD investments in science and technology programs that affect the energy demands of the force such as engines and propulsion, light-weight structural and armor materials, power efficiency in electronics, mobile power production and distribution, and more innovative system design approaches.

FBCE includes the cost of the fuel itself and the apportioned cost of all of the fuel logistics and related force protection required beyond the Defense Logistics Agency-Energy (DLA Energy) point of sale. While most planning scenarios generally employ military forces for fuel delivery and protection, in some cases, contractor logistics and protection may be presumed. The cost estimation method is the same though the data sources required may vary. As a decision tool, FBCE is meant to inform technological and design choices as it is applied in requirements development, acquisition trades, and technology investments. Successful implementation will over time help DoD manage larger enterprise risks such as high and volatile fuel prices.

The FBCE is applied in trade-off analyses conducted for all deployable DoD systems with end items that create a demand for energy in the battlespace. This FBCE methodological guidance applies to ACAT I and II developmental systems as well as mid-life upgrade or modernization choices.

FBCE estimates shall be prepared concurrently with the AoA for each materiel solution being considered. The AoA should develop those estimates to sufficient fidelity to determine if the differences in energy demand and resupply costs are significant enough to meaningfully influence the final choice of alternatives. For developmental system with delivered energy requirements (i.e., most systems), the AoA shall examine alternative ways to reduce operational energy demand as a significant system capability factor. Even if FBCE does not significantly differ between alternatives, but shows sensitivity to change between sub-component or design choices within all alternatives, the Service sponsoring the program shall continue FBCE efforts after completion of the AoA to inform trades in the subsequent acquisition phases. This includes technology development, systems engineering, and design decisions, or even to incentivize bidders to offer more efficient systems. In all cases, FBCE shall be developed for all alternatives remaining in the trade space at the end of the AoA and not just for the alternative favored/chosen by the Service sponsor.

FBCE has a wide range of applications beyond system design. For example, it can be used for site specific investments such as efficiency improvements at a contingency base to reduce fuel deliveries.

Commercial vehicles such as buses or cars used in support of routine fixed base operations normally should not be regarded as "deployable" and are addressed in other regulations and guidance.

Fully Burdened Cost of Energy Computational Framework

This section outlines a basic framework developed by the Office of the Assistant Secretary of Defense for Operational Energy Plans and Programs (OASD(OEPP)) and the Office of the Secretary of Defense (OSD), Cost Assessment and Program Evaluation (CAPE), to calculate the FBCE. This framework is oriented towards liquid fuels but extends to other forms of energy demands (e.g., fuel cells, hybrid-electric engines, and nuclear and solar energy sources). The specific analytic tools and methods to estimate FBCE are being refined within the analytic, acquisition and costing communities. This approach was informed by analytical work started by a Defense Science Board task force in 2001, applied by the Office of Program Analysis and Evaluation in 2006 and 2007 in a ground system case study, and revisited by OSD while assessing several major defense acquisition programs (MDAPs) and their approach to fuel issues. This framework is intended to give DoD Components flexibility in developing methodologies tailored to their various domains and force planning methods. Alternative methods or interpretations may be allowed, but DoD Components should consult iteratively with appropriate OSD offices, especially the OASD(OEPP) before delivering a final product at a milestone review or similar decision point.

Calculation of the FBCE differs from most other cost factors in two main ways. First, it is scenario-based. The FBCE analysis should be based upon a range of operational scenarios or use conditions from those specified in the programs AoA guidance or in the approved programs analysis base to ensure comparability within program tradespace discussions. Further, in order to estimate operationally realistic costs, all scenarios have to be of sufficient duration to account for demanded logistics and force protection. In addition, the FBCE calculation requires participation from Component force planning and analytic organizations to appropriately calculate the estimates. The appropriate organizations vary by Service.

There is no definitive, "correct" answer for a given systems FBCE estimate. However, DoD Components should present a realistic and analytically defensible scenario and cost elements. The proponent’s scenario assumptions for fuel logistics must be consistent with Service future force plans and Concepts of Operation. Consistency enables the Services and DoD to evaluate their assumptions relative to strategy and doctrine and make better informed risk decisions. DoD Components should use existing analytic tools, planning data, and costing methodologies where possible to develop FBCE values. If Components find their analytic tools are inadequate to make the necessary estimates, Components should approach OASD(OEPP) at the earliest opportunity to help identify potential solutions.

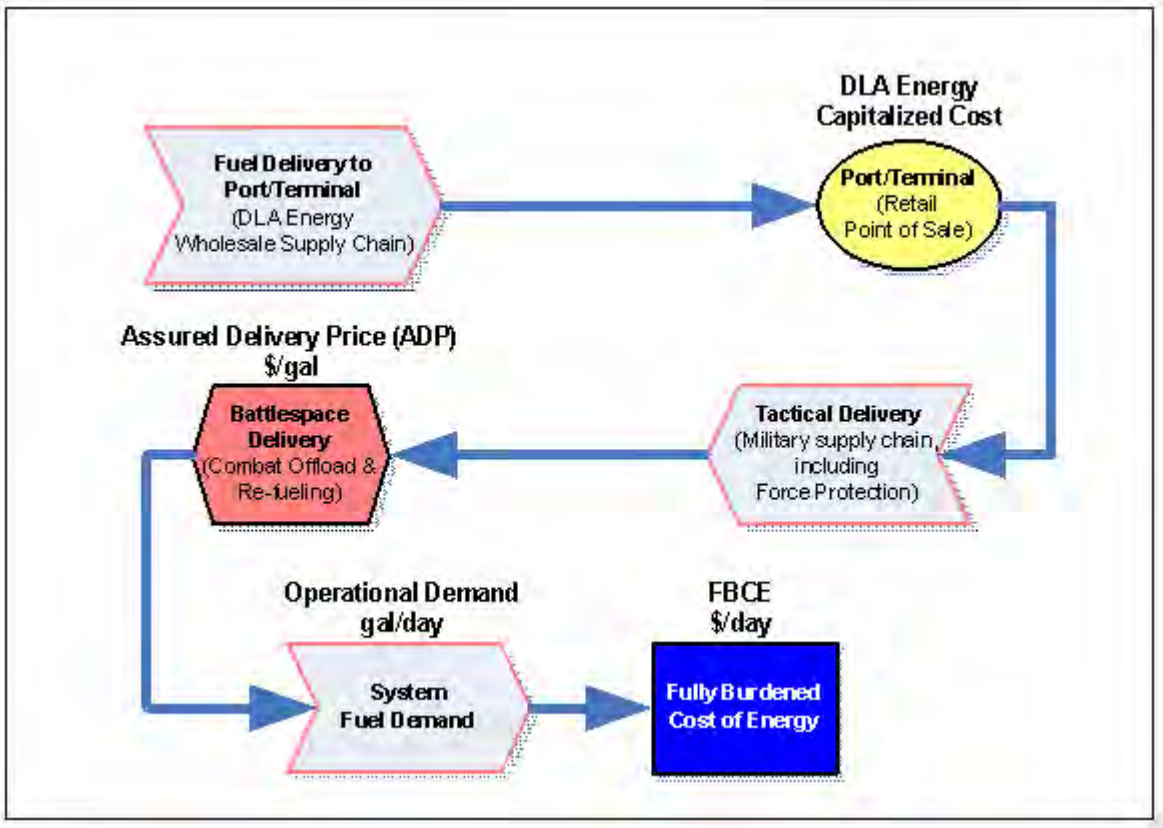
There are two key analytical components essential to developing a FBCE value:

1. **Scenarios.** Services decide upon a representative set of future operational scenarios or vignettes. However, to ensure the results of the FBCE calculations are comparable to other analytic measures, the same scenarios used in the programs AoA or analysis base shall be used in calculating the FBCE. The DoDs approved joint Defense Planning Scenarios (or Integrated Security Construct scenarios) and the Components supporting future force plans should provide the general guidance and analytic assumptions needed to identify appropriate scenarios. For purposes of computing the FBCE, scenarios must be of sufficient duration to require logistical re-supply of energy. Once the FBCE is calculated for the chosen scenarios, a simple mean average of the results will be computed.

2. **Apportionment.** Services determine what proportion of the fuel logistics footprint identified in the selected scenarios is attributable to the platform or system in question. Is it drawing 5% of the fuel from the fuel logistics units in the scenario or 20% or 50%? This percentage should inform how one attributes the logistics footprint to this one developmental system. Because no single system in any operation takes 100% of the fuel, it is inappropriate to attribute 100% of the logistics tail cost to one system when calculating FBCE.

DoD Component organizations with responsibilities for scenario-based force planning, campaign model development, and force structure analysis should collaborate with responsible acquisition organizations to agree on a manageable subset of operational scenarios from the AoA that best represent the missions or duty cycles the system is being built to support. In the process of selecting scenarios, the force structure will determine the proper level of apportionment. Component organizations are encouraged to prepare fuel logistics and logistics force protection baselines for each common scenario to provide a starting point for AoAs and other acquisition trades that follow. As more acquisition programs perform these analyses and expertise builds, refinements to guidance and oversight criteria will be developed.

Figure 3.1.6.F1. FBCE Scenario Fuel Delivery Process Diagram



Assured Delivery Price Computation

The first item needed to compute the FBCE is the Assured Delivery Price (ADP). The price elements described in Figure 3.6.1.F2 (below) provide a framework for determining the ADP of fuel within a given scenario. It is a measure of the burdened cost of the fuel in $/gallon or $/barrel and all the tactical delivery assets and force protection needed to assure the fuel is safely delivered out to a given location. The ADP is the same for all users of fuel in that location using a given source of fuel and delivery method.

Price Elements to Determine Assured Delivery Price

Figure 3.6.1.F2. Summary of Price Elements to Apply within Each Scenario to Determine the Assured Delivery Price

Element #	Price Element	Burden Description
1	Fuel	Most recent DLA Energy "standard price" plus OMB-direct price inflation to the fiscal year of the scenario. In some cases, one may substitute a location-specific contract delivery price.
2	Tactical Delivery Assets*	Includes all of the following:
	Fuel Delivery O&S Price	Per gallon price of operating service-owned fuel delivery assets including the cost of military and civilian personnel dedicated to the fuel mission.
	Depreciation Price of Fuel Delivery Assets	Captures the decline in value of fuel delivery assets with using straight-line depreciation over total service life. Combat losses due to attack or other loss (terrain, accident, etc.) should be captured as a fully depreciated vehicle.
	Infrastructure, environmental, and other miscellaneous costs over/above and distinct from the DLA Energy capitalized cost of fuel	Per gallon price of fuel infrastructure, regulatory compliance, tactical terminal operations, and other expenses as appropriate.
3	Security*	Potential per gallon price associated with delivering fuel, such as convoy escort and force protection. Includes the manpower, O&S, asset depreciation costs, and losses associated with force protection.

*These prices vary by Service and delivery method (ground, sea, air).

Although this figure provides a framework for calculating ADP, the elements must be tailored to a selected supply chain, system or platform type, and larger force structure context. In all cases, the results are scenario or unit-type-specific, and are not applicable for all situations. Each of the elements is discussed further in the following sections.

Fuel

The first price element for consideration is the fuel itself. DLA Energy serves as DoDs single supply center for petroleum products worldwide and for coal, natural gas, and electricity services within the continental United States. DLA Energy not only procures the energy products but serves as DoDs Integrated Materiel Manager for all petroleum

products. DLA Energy charges the Services for the fuel delivered through a reimbursable arrangement known as the Defense Working Capital Fund.

The Standard Price established by DLA Energy is the rate that is charged to military customers at the retail point of sale worldwide. To simplify cost planning and accounting, the Standard Price for a given fuel is the same globally and does not represent the full capitalized costs DLA Energy incurs to deliver the fuel out to the point of sale. For purposes of calculating ADP, the Standard Price shall be used, referencing the most recent price update from DLA Energy. The Standard Price should then be inflated, using the most recent Office of Management and Budget inflation factors for fuel prices, to the year in which the AoA scenarios in the analysis are set (e.g. 2018 or some future year at or after Initial Operational Capability).

In certain circumstances, particularly for current-day, site-specific calculations, DoD Components may use the actual contracted delivery price if it is available instead of the Standard Price. DLA Energy maintains a database of capitalized costs to purchase and deliver fuel at various supply points around the world. Site-specific fuel prices may only be used to inform rapid fielding and related procurement choices, as they represent market pricing in a specific operational situation. It is DLA Energy's responsibility to provide this data to DoD Components if required for these analyses. Since the FBCE is used for business case analyses and not to inform programming and budgeting for operation of platforms, the Services should not be concerned that this capitalized cost does not match the Standard Price it will be charged during actual operation of the platform under consideration.

Tactical Delivery Assets

The second price element captures the burdens associated with the tactical delivery assets used by the Services to deliver fuel from the point of sale to the system that will consume it. It includes the Operating and Support (O&S) costs, the cost of depreciation of the actual delivery assets, and any significant infrastructure costs needed to operate these assets.

Once the Services take over possession of fuel from DLA Energy at the point of sale, they must employ Service-owned delivery assets. For the purposes of ADP estimates, fuel delivery assets means major items of fuel delivery equipment, such as Navy oilers (T-AOs), aerial refueling aircraft (KC aircraft) for fixed-wing and rotary-wing aircraft, and tanker trucks and trailers for ground vehicles. It also includes C-130s airdropping palletized fuel and rotary-wing aircraft carrying fuel by sling load for delivery.

The O&S cost for the fuel delivery assets is measured in $/gallon and consists of the costs of operations and maintenance (O&M) of the vehicles and equipment and the costs for military and civilian manpower dedicated to the fuel delivery mission divided by the gallons of fuel delivered. For fuel delivery systems that are major systems in their own right, such as oilers or aerial refueling aircraft, actual O&S cost history is collected and made available to registered users of the Air Forces and Navy's Visibility and

Management of Operating and Support Cost data systems. For other classes of equipment, cost and manpower data is found in planning factors used to develop O&M budgets and tables of organization and equipment associated with fuel delivery units. If the planning scenarios/missions being used for this calculation requires another Services assets to delivering fuel in the battlespace, Services may need share data.

The cost of depreciation of the primary fuel delivery assets is also part of the second price element. Normally, depreciation is not used in DoD analyses, since most studies tend to deal with equipment recapitalization costs explicitly. However, in this case, depreciation provides a measure of the decline in capital value of the fuel delivery assets over time from use. The standard method is to use straight line depreciation over the anticipated service life of the primary fuel delivery asset. For example, for an ADP calculation for an aerial system that requires air-to-air refueling as part of its mission profile/duty cycle, this step would require inclusion of a depreciation value for the systems air refueling tanker.

An additional part of the cost of depreciation is the potential loss of delivery assets due to hostile attack or other attrition. Based on the scenario chosen, there is a definable probability that the associated logistics platforms will be interdicted and destroyed. If destroyed, the entire remaining value of the platform is immediately amortized and this cost is added to this price element. Depending on the quantity of fuel being carried by the delivery asset, an adjustment to the amount of fuel obtained from the point of sale will be required to account for this potential loss, if appropriate. Many cost and attrition factors related to fuel resupply convoys are available through existing combat models and historical databases.

Finally, miscellaneous infrastructure costs may be added if they significantly add to the cost of supporting the delivery assets and if the scenarios in the AoA involve energy infrastructure. These items may include the price of O&S and recapitalization for the facilities (such as fueling facilities and fuel storage sites) and related ground system equipment (such as pumps, fuel storage bladders, hose lines, and other refueling equipment to include maintenance and parts for refueling vehicles and other related ground refueling equipment). The costs to deploy the delivery assets may also be included, if the assets need to be transported to the theater of interest. This applies only to infrastructure that is operated by the military Services in the theaters of interest, and does not apply to infrastructure that is operated by DLA Energy and incorporated into the DLA Energy capitalized cost of fuel.

For DoD infrastructure, data sources and associated cost factors are centrally managed by the Office of the Deputy Under Secretary of Defense (Installations and Environment) and available to authorized users. Data on all DoD world-wide facilities is stored in the DUSD(I&E) Facilities Assessment Database. A four digit number known as the Facility Analysis Code (FAC) classifies each facility. For example, there is a unique code for each facility category such as marine fueling facility, POL pipeline, pump station, or fuel storage facility. For each four digit code, the DoD Facilities Pricing Guide provides cost factors used in DoD facilities cost models. Cost factors are expressed as annual costs

per unit of measure (e.g., square foot) and are provided for facilities sustainment, modernization, and operations.

Security

The third and final price element includes the costs of escort protection of the fuel supply chain in hostile environments. In the case of DoD force protection assets allocated to the fuel delivery forces, the O&S costs, direct fuel costs and the depreciation cost of those forces will also have to be estimated and included in the overall calculation. In essence, all of the costs considered in the second price element should also be considered for security assets. This includes the possibility that some security assets will be destroyed due to hostile activity while protecting the fuel supply chain. In some high-risk scenarios, force protection costs may be the largest factor in the FBCE estimate.

Fully Burdened Cost of Energy Computation

To arrive at the FBCE, the ADP is multiplied by the apportioned amount of fuel demanded by the system of interest. The FBCE is computed for each scenario being considered. Programs then have the option of reporting out the FBCE for each of the scenario they've assessed separately, or to provide their mean or weighted average, depending on anticipated usage of the system. To arrive at a single FBCE for the program, average these estimates based upon the relative amount of time that the system is expected to operate in each of the chosen scenarios.

Other Considerations

The FBCE, which is based on a simplified activity based costing framework, is meant to provide the acquisition process with a realistic, financial proxy for the fuel burden our forces will incur in the future battlespace. It is not meant to capture the operational impacts and capability gained or lost by changes in the logistical burden or in the unrefueled range of the system due to fuel consumption. The DoD force planning process and the analyses conducted to inform requirement development, the Joint Capabilities Integration Development System (JCIDS) process, are evolving to consider these variables. Because acquisition is governed by "cost, schedule, and performance", the requirements developer and approving authority should consider those fuel-related variables as part of the performance tradespace relative to the capability gap they are trying to fill.

The use of FBCE estimates do not normally identify near-term savings that can be identified in a budget. Choices made during an acquisition program to reduce the fuel demand will not begin to show an effect until after the system is fielded. Further, actual usage may vary considerably from the planning scenarios used in the AoA. This is often 10 to 20 years following an initial ICD for a major program, well beyond the FYDP. Readers interested in this subject should periodically check this section of the

Guidebook for future updates to this framework.

3.2. Affordability

Affordability Analysis is a Component leadership responsibility that should involve the Components programming, resource planning, requirements, intelligence, and acquisition communities. The Department has a long history of starting programs that proved to be unaffordable. The result of this practice has been costly program cancelations and dramatic reductions in inventory objectives. Thus, the purpose of Affordability Analysis is to avoid starting or continuing programs that cannot be produced and supported within reasonable expectations for future budgets. Affordability constraints for both procurement and sustainment are derived early in program planning processes. These constraints are used to ensure requirements prioritization and cost tradeoffs occur as early as possible in the programs life cycle. Implementation of this new affordability policy is in early stages, so revisions to this guidance are likely in the future as the specific products and processes are developed.

Program life-cycle affordability is a cornerstone of DoD acquisition planning as indicated in DoD Directive 5000.01, Affordability within the Future Years Defense Program (FYDP) is also part of the Milestone Decision Authority (MDA) certification and monitoring required by section 2366b of title 10, United States Code, for Major Defense Acquisition Programs (MDAPs) at and beyond Milestone B (MS B). However, the intent of Affordability policy is to require additional affordability analysis that addresses the total life cycle of the planned program beyond the FYDP. Assessing life-cycle affordability of new and upgraded systems is crucial for long-range investment planning beyond the FYDP, establishing fiscal feasibility of the program, informing Analyses of Alternatives (AoAs), guiding requirements and engineering tradeoffs, and setting realistic program baselines to control life-cycle costs and help instill a more cost-conscious culture in the Department. Affordability analysis and management necessitates effective and ongoing communication with the requirements community on the cost and risk implications of requirements.

Section 3.2.1 describes how affordability is considered during the identification of military capability needs, and at acquisition milestone reviews. Section 3.2.2 provides parameters and analytic approaches for preparing affordability analyses. Section 3.2.3 describes affordability implementation and enforcement and Section 3.2.4 explains the

Department's full-funding policy.

3.2.1. Affordability in Decision Support Systems

The Milestone Decision Authority (MDA) considers affordability at all major decision points of an acquisition program. Consideration and subsequent enforcement of affordability constraints help to ensure sufficient resources will be available to support the procurement and operation and support (O&S) of the system throughout its life cycle. The MDA also examines the realism of projected funding over the programs life cycle, given likely DoD Component resource constraints.

Affordability analysis and constraints are not intended to produce rigid, long-term plans. Rather, they are tools to promote responsible and sustainable investment decisions by examining the likely long-range implications of today's requirements choices and investment decisions based on reasonable projections of future force structure equipment needs-before substantial resources are committed to a program.

3.2.1.1. Affordability in JCIDS

Even before a program is approved for formal initiation into the acquisition process, affordability plays a key role in identifying capability needs as part of the Joint Capabilities Integration and Development System (JCIDS), which balances cost versus performance in establishing requirements for new acquisitions.

After the Materiel Development Decision (MDD), an Analysis of Alternatives (AoA) is initiated to examine potential materiel solutions to satisfy a capability need documented in an approved Initial Capabilities Document (ICD). Integral components of the AoA are the cost analyses of each material alternative under consideration as well as cost-effectiveness comparisons of the alternatives.

Moreover, all elements of life-cycle cost (or total ownership cost, if applicable) are documented as part of the Capability Development Document and the Capability Production Document (section 16 in both documents). To ensure the program is affordable, cost constraints are established to drive early consideration of potential tradeoffs.

3.2.1.2. Affordability Defined

Affordability is the ability to allocate resources out of a future total budget projection to individual activities. It is determined by Component leadership given priorities, values, and total resource limitations against all competing fiscal demands on the Component. Affordability goals set early cost objectives and highlight the potential need for tradeoffs within a program, and affordability caps set the level beyond which actions must be taken, such as reducing costs.

Affordability analysis and constraints are not synonymous with cost estimation and

approaches for reducing costs. Constraints are determined in a top-down manner by the resources a Component can allocate for a system given inventory objectives and all other fiscal demands on the Component. Constraints then provide a threshold for procurement and sustainment costs that cannot be exceeded by the Program Manager (PM) without advanced permission of the MDA and Component leadership. On the other hand, cost estimates are generated in a bottom-up manner and forecast whether the system can be acquired under those constraints and at what level of risk. Thus, constraints are not set based on cost estimates but rather on a different calculus of whether a Component can afford the estimated costs of a system. The difference between the affordability constraints and the cost estimates indicate the levels of risk at the current requirements and quantity levels, and whether actions must be taken to prevent exceeding the constraints.

Cost control and cost reduction approaches are central to maximizing the buying power of the Department and should be considered in all phases and aspects of program management as ways to meet or beat affordability constraints. Reducing the cost of program management, RDT&E, procurement, or sustainment of a product that meets validated requirements is always of importance, independent of achieving affordability constraints; however, if those constraints cannot be met-even with aggressive cost control and reduction approaches-then technical requirements, schedule, and planned quantities are revisited, with support from the Components Configuration Steering Board, with any requirements trades proposed to the validation authority. If constraints still cannot be met and the Component cannot afford to raise the constraint level by lowering constraints elsewhere in their analysis and obtaining MDA approval, then the program may be cancelled.

3.2.2. Affordability Analysis

3.2.2.1. Analysis Parameters

3.2.2. Affordability Analysis

Affordability analysis is the cornerstone process for the Component leadership to set priorities and determine what it can afford for each acquisition. Each DoD Component develops life-cycle affordability constraints for its ACAT I and IA acquisition programs for procurement unit cost and sustainment costs by conducting portfolio affordability analyses that contain a product life-cycle funding projection and supporting analysis. The basic procurement unit cost calculation is the annual estimated procurement budget divided by the number of items that should be procured each year to sustain the desired inventory.

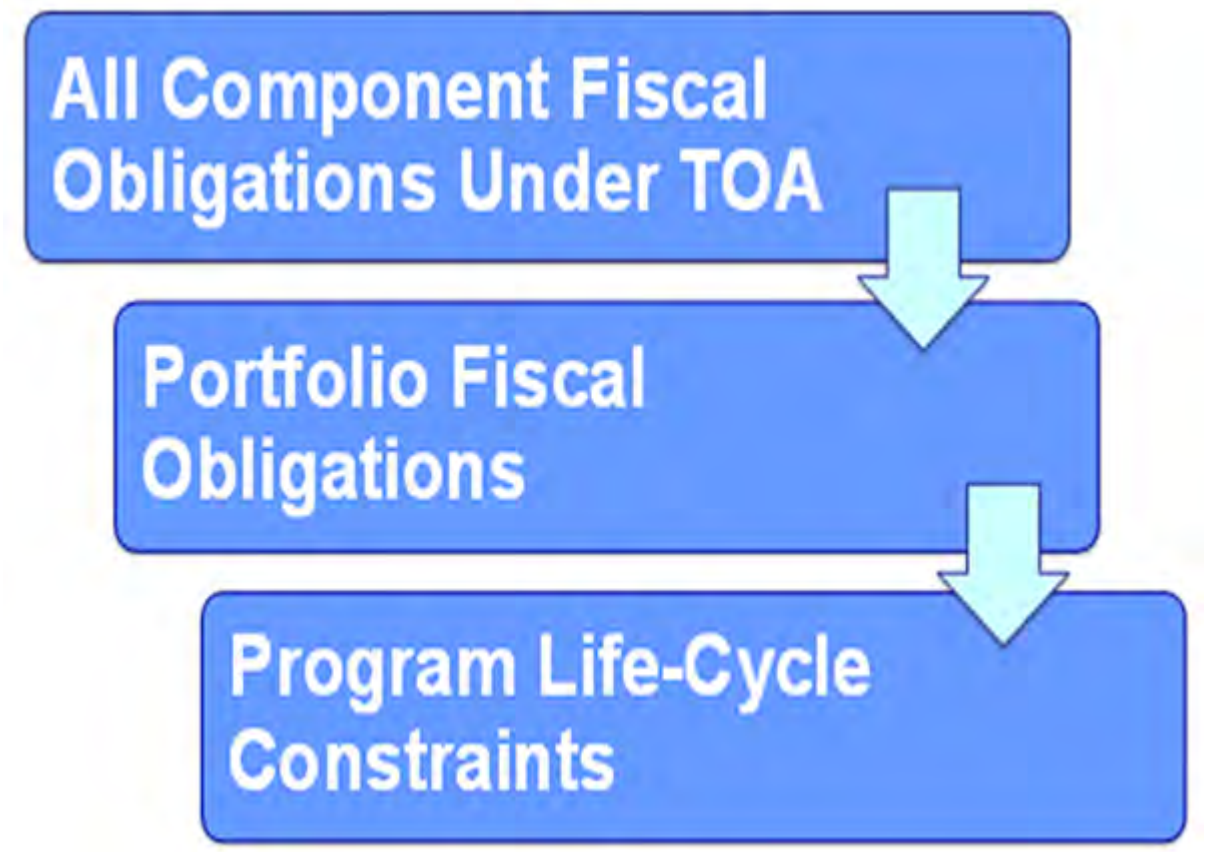
As a simple example, if $1 billion is projected to be available annually to sustain an inventory of 200,000 trucks, and the trucks have an expected service life of 20 years, then an average of 10,000 trucks must be procured each year, and the affordability constraint for procurement is $1 billion divided by 10,000, or $100,000 per truck.

Similar calculations are made to derive sustainment affordability constraints. Components standardize the portfolios they use for their analysis and can be based on mission areas or commodity types. These portfolios provide a collection of products that can be managed together for investment planning and oversight purposes. Components normally make trade-offs within portfolios, but if necessary, can and should make trade-offs across portfolios to provide adequate resources for high-priority programs.

3.2.2.1. Analysis Parameters

Component leadership-not the acquisition community or program management-conducts affordability analysis with support and inputs from their programming, resource planning, requirements, intelligence, and acquisition communities. Each Component determines the processes and analytic techniques they use for affordability analysis within the basic parameters described in the following paragraphs. As noted above, affordability analysis is a top-down process that starts with all fiscal demands on the Component. Figure 3.2.2.1.F1 summarizes the general approach from topline budget to portfolios to individual program constraints.

Figure 3.2.2.1.F1. Affordability Analysis Summary



A future total budget projection for each Component for affordability analysis provides

the first-order economic reality and for allocation of estimated future resources to each portfolio. This projection establishes a nominal rather than optimistic foundation for the future and covers all fiscal demands that compete for resources in the Component, including those outside acquisition and sustainment.

The affordability analysis examines all programs and portfolios together, extending over enough years to reveal the life-cycle cost and inventory implications of the longest program for the Component. The same analysis is used as individual programs come up for review. Nominally, affordability analysis covers at least 30 to 40 years into the future (especially for the Military Departments) but may be approximately 15 years for Components whose acquisitions all have planned life cycles of, and reach steady-state inventory in, 15 years or less (e.g., Components with only MAIS programs whose life cycles are estimated to be acquisition time plus 10 years after Full Deployment declaration).

The aggregation of portfolio cost estimates for each year, when combined with all other fiscal demands on the Component, may not exceed the Components reasonably anticipated future budget levels. Absent specific Component-level guidance by Director, Cost Assessment and Program Evaluation (DCAPE) or USD(AT&L), each Component projects its topline budget beyond the FYDP using the average of the last two years of the current FYDP and the OSD inflator provided by Under Secretary of Defense (Comptroller) (USD(C)), resulting in zero real growth.

3.2.2.2. Inputs and Structure

Portfolios. Components subdivide their accounts into portfolios to facilitate trade-off analysis; but when summed using the affordability constraints, the total cost for all portfolios and their elements cannot be above the Components future total budget projection. Components may use existing affordability portfolios, which are stable between affordability analysis updates. When the analysis is presented for a specific

programs review, the Component employs the relevant portfolio to facilitate understanding and discussion of life-cycle costs and inventories of related acquisition systems.

Other Portfolio Plans. The Components affordability analyses should be consistent with any relevant existing portfolio plans and strategies such as those required by statute, e.g., the 30-year plans required by section 231 of title 10, United States Code, for ships, and section 231a of title 10, United States Code, for aircraft.

3.2.2.3. Updates

Each Component maintains and updates its affordability analysis as needed at the Component or portfolio level to reflect significant changes such as large cost growths in portfolios and programs, changes in defense strategy, force structure changes, or major budgetary changes.

3.2.2.4. Presentation

Each Components affordability analysis is presented within the governance framework to the MDA in preparation for major acquisition decisions in a format that demonstrates the affordability of the program within the Component and portfolio context, to ensure that the resulting affordability constraints are understood and consistent with the future total budget projection.

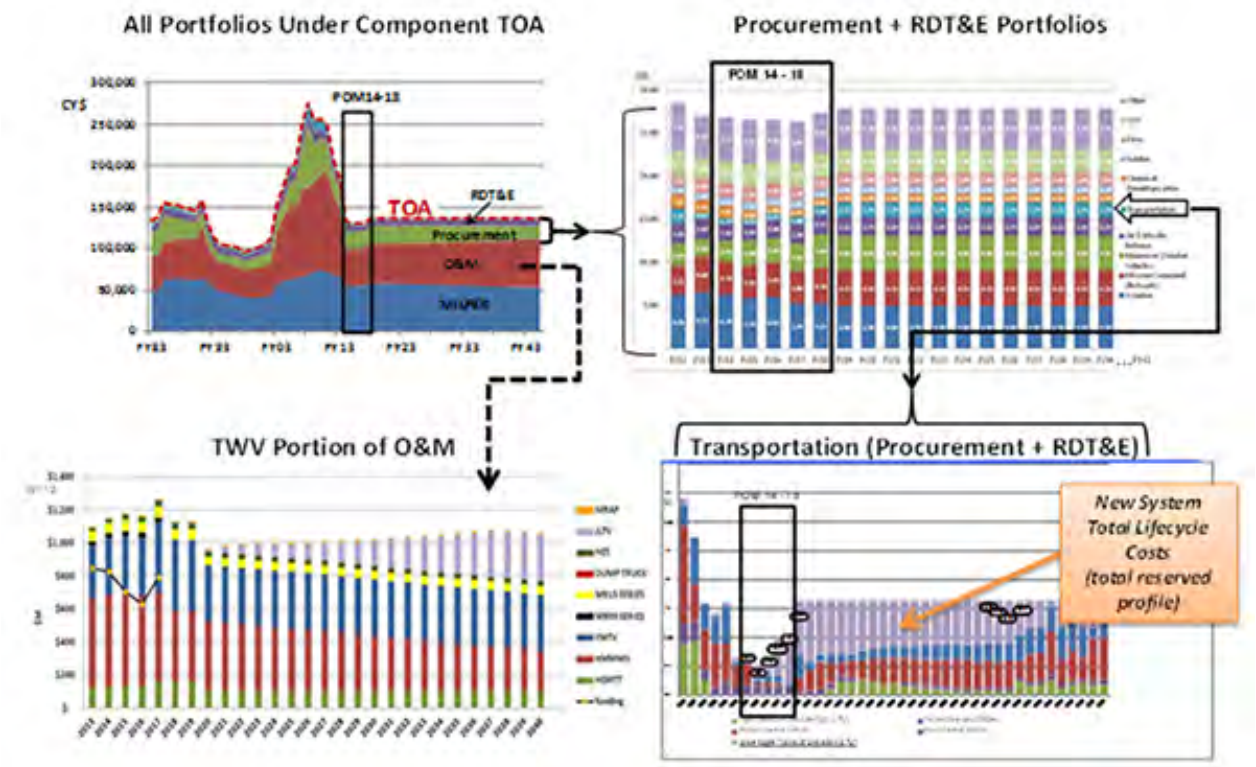
Transparency ensures that the risk, cost implications, and alternatives of system acquisitions and sustainment are sufficiently understood by the Component leadership and the programming, resource planning, requirements, intelligence, and acquisition communities.

3.2.2.5. Format

Each Component uses standardized templates provided by OUSD(AT&L) to present its affordability analysis. In general, standardized stacked area charts (or "sand charts") and spreadsheets listing the estimated budget by year for each element of the analysis, are adequate. The data should compare life-cycle estimates to the historical experience within the portfolio and the Component for sustainment and procurement costs.

At each major acquisition decision meeting, the Component provides stacked area charts ("sand charts") and underlying spreadsheet data showing the programs budget, what portfolio it fits within, and the top-level total of all portfolios and accounts totaling at or below the future total budget projection, equivalent to Total Obligation Authority (TOA), using the affordability constraints (refer to Figure 3.2.2.5.F1).

Figure 3.2.2.5.F1. Notional Example of Affordability Analysis Charts



An enlarged version of Figure 3.2.2.5.F1 is available for viewing by selecting/clicking on the image.

Notional examples used by the Army , Navy , and Air Force are provided for informational purposes.

3.2.2.6. Data Requirements

The affordability analysis must be consistent with the data in the Cost Analysis Requirements Description (CARD) for a program under review, including the requirements, quantity, and schedule used in the analysis. Affordability Analysis also provides data to support the procurement and sustainment constraints that are documented in the MDD, Milestone A, and Pre-B Acquisition Decision Memorandums (ADMs) and in the acquisition program baselines (APBs) normally set at Milestone B and beyond.

3.2.2.7. Timing

Affordability Analysis should be conducted as early as possible in a systems life cycle so that it can inform early requirements trades and the selection of alternatives to be considered during the AoA. Affordability constraints are not required before the MDD decision; however, conducting some analysis before that point is beneficial. The best

opportunity for ensuring that a program will be affordable is through requirements tailoring that occur before and during the AoA(s) and early development. Thus, the Components incorporate estimated funding streams for future programs within their affordability analyses at the earliest conceptual point and specify those estimates at MDD and beyond to inform system design concepts and alternative selection.

3.2.2.8. Incorporation in AoAs

Comprehensive and substantive examination of key requirements during AoAs is crucial for making programs more affordable. Thus, AoAs must seriously explore options below the affordability goal while making excursions above the goal to understand tradeoff options for Component leadership consideration.

3.2.3. Affordability Implementation and Enforcement

Affordability constraints are established to inform the requirements authority, PM, and AoA team of the cost limitations dictated by the Components affordability analysis.

3.2.3.1. Affordability Constraints Defined: Goals and Caps

Affordability goals are key objectives set to inform requirements and design tradeoffs during early research and development. Affordability caps are fixed requirements that are functionally equivalent to Key Performance Parameters (KPPs). Based on the Components affordability analysis and recommendations, the MDA sets and enforces affordability constraints as follows:

- **At MDD**: tentative affordability cost goals (e.g., total funding, annual funding profiles, unit procurement and/or sustainment costs, as appropriate) and inventory goals to help scope the AoA and provide targets around which to consider alternatives;

- **At Milestone A**: affordability goals for unit procurement and sustainment costs; and
- **At the Pre-B Decision Review, Milestone B, and Beyond**: binding affordability caps.

These constraints are documented in the ADMs for these decision points. At Milestone B, the affordability caps are documented in the programs APB. Any programs that skip earlier reviews, or have baselines set before Milestone B, receive goals or constraints commensurate with their position in the acquisition cycle and their levels of maturity.

3.2.3.2. Measuring Constraints

The type of measures used for MDA-approved affordability constraints on procurement and sustainment costs (e.g., Acquisition Program Unit Cost [APUC] or unit-recurring flyaway for procurement; and cost per operating hour and estimated reliability for sustainment) may be tailored to the type of acquisition and the specific circumstances of a given program. In addition to requirements tradeoffs approved by the requirements validation authority, prudent investments in RDT&E, innovative acquisition strategies, and incentives to reduce costs can be used to ensure that affordability constraints are achieved.

3.2.3.3. Monitoring and Reporting

The MDA enforces affordability constraints throughout the life cycle of the program. If a PM concludes that, despite efforts to control costs and reduce requirements an affordability constraint will be exceeded, then the PM notifies the Component Acquisition Executive and the MDA to request assistance and resolution. The PM also reports progress relative to affordability constraints at Defense Acquisition Executive Summary (DAES) reviews.

Inflators. When determining whether an affordability constraint has been exceeded in the life-cycle cost estimates, Components use the OSD inflator provided by USD(C) or, at the Components discretion, higher inflators reflecting historical experience.

3.2.3.4. Developing Proposed Constraints

As noted above, the affordability constraints are not based on cost estimates. Rather, the constraints are what the Component can afford to spend on the program under review relative to all other fiscal demands.

Once affordability is established, cost estimates can help inform the feasibility and risk of a set of proposed requirements given the affordable level of investment. Thus, at the point of establishing an APB, the affordability caps should be at least as high as the APB values (otherwise, the program will already require action to address cost and/or requirements). In practical terms, Components will likely want to propose caps above the APB values to allow for some flexibility in dealing with unforeseen issues. The

amount by which the proposed caps exceed the APB values is at the Components discretion as long as the life-cycle cost at those caps, along with all other Component fiscal demands, can be shown to fit within the Components future total budget projection.

The caps set the level at which the program may be de-scoped or cancelled, not what the cost estimates say a specified set of program requirements will cost.

3.2.3.5. Affordability for Lower ACAT Programs

Components are responsible for developing and issuing similar guidance to ensure life-cycle affordability for lower ACAT programs that have resource implications beyond the FYDP, and PMs should ensure they are familiar with that guidance.

3.2.4. Full Funding

It has been a long-standing DoD policy to seek full funding of acquisition programs, based on the most likely cost, in the budget year and out-year program years. DoD Directive 5000.01 affirms this full funding policy. Moreover, DoD Instruction 5000.02 requires full funding-defined as inclusion of the dollars and manpower needed for all current and future efforts to carry out the acquisition strategy in the budget and out-year program-as part of the entrance criteria for the transition into engineering and manufacturing development.

For MDAPs at MS B, the MDA must certify in writing to Congress that the program is fully funded through the period covered by the FYDP, relative to reasonable cost and schedule estimates that meet DCAPE concurrence. Other certification requirements are listed under section 2366b of title 10, United States Code. For all acquisition programs, the MDA normally assesses full funding at all major decision points. As part of this assessment, the MDA reviews the actual funding (in the most recent FYDP position) in comparison to the (time-phased) DoD Component Cost Estimate. In addition, the MDA considers the funding recommendations made by DCAPE (for Acquisition Category ID and IAM programs), or the DoD Component Cost Analysis team (for Acquisition Category IC and IAC programs). If the MDA concludes that the current funding does not support the acquisition program, then the ADMD may direct a funding adjustment and/or program restructure in the next FYDP update.

While full funding focuses on the FYDP, the long-range aspects of affordability analysis and constraints are meant to consider the implications beyond the FYDP of decisions made today.

3.3. Analysis of Alternatives

3.3.1. Introduction

The Analysis of Alternatives (AoA) is an important element of the defense acquisition process. An AoA is an analytical comparison of the operational effectiveness, suitability, and life-cycle cost (or total ownership cost, if applicable) of alternatives that satisfy established capability needs. Initially, after the Materiel Development Decision, the AoA is initiated to examine potential materiel solutions with the goal of identifying the most promising option, thereby guiding the Materiel Solution Analysis phase (see section 3.3.2). Subsequently, an update to the AoA is initiated at the start of the Technology Development Phase and is reviewed at Milestone B (which usually represents the first

major funding commitment to the acquisition program). The update to the AoA is used to refine the proposed materiel solution, as well as reaffirm the rationale, in terms of cost-effectiveness, for initiation of the program into the formal systems acquisition process. For Major Defense Acquisition Programs at Milestone A, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the Department has completed an AoA consistent with study guidance developed by the Director, Cost Assessment and Program Evaluation (DCAPE), in addition to meeting other certification criteria (10 U.S.C. 2366a). For Major Defense Acquisition Programs at Milestone B, the Milestone Decision Authority (MDA) must certify in writing to the Congress that the Department has completed an AoA with respect to the program in addition to meeting other certification criteria (10 U.S.C. 2366b). Pursuant to DoDI 5000.02, the AoA is updated as needed at Milestone C.

In practice, AoA issues vary somewhat between AoAs for weapon and other tactical systems and AoAs for major automated information systems. Sections 3.3.2 , 3.3.3 , and 3.3.4 provide discussion about AoAs that may be of general interest, although much of the discussion is focused on weapon systems. Section 3.3.5 discusses the AoA process for major automated information systems.

3.3.2. Role of the Analysis of Alternatives (AoA) as Part of the Materiel Solution Analysis

The analysis of alternatives process is expected to play a key role in support of the Materiel Solution Analysis Phase. After a program has an approved Materiel Development Decision, the analysis of alternatives process is expected to contribute to the selection of a preferred materiel solution that satisfies the capability need documented in the approved Initial Capabilities Document (ICD).

The Director, Cost Assessment and Program Evaluation (DCAPE), develops and approves study guidance for the AoA. The guidance is developed with the input of other DoD officials. Prior to the MDD review, DCAPE provides the AoA study guidance to the DoD Component designated by the MDA. Following receipt of the AoA study guidance, the DoD Component prepares an AoA study plan that describes the intended methodology for the management and execution of the AoA. The AoA study plan is coordinated with the MDA and approved by DCAPE prior to the MDD review. A suggested template for the AoA study plan is provided in section 3.3.3.

The study guidance shall require, at minimum, full consideration of possible trade-offs among cost, schedule, and performance objectives for each alternative considered. The study guidance shall also require an assessment of whether or not the joint military requirement can be met in a manner that is consistent with the cost and schedule objectives recommended by the JROC. The AoA study guidance and resulting AoA plan should build upon the prior analyses conducted as part of the Joint Capabilities Integration and Development System (JCIDS). The JCIDS process is briefly described in section 1.3, and is fully described in CJCS Instruction 3170.01. The JCIDS analysis process that leads to an approved Initial Capabilities Document (ICD) is built upon the

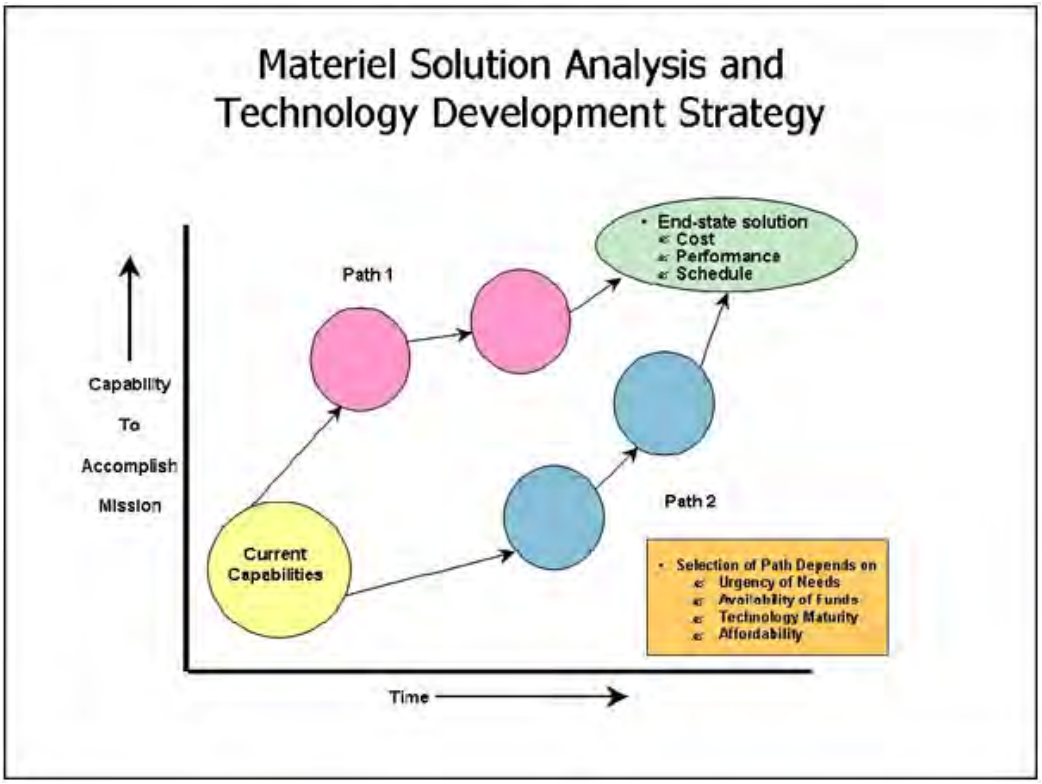
analysis known as the Capabilities-Based Assessment (CBA). The CBA provides recommendations (documented in the ICD) to pursue a materiel solution to an identified capability gap that meets an established capability need. The CBA does not provide specific recommendations as to a particular materiel solution, but rather provides a more general recommendation as to the type of materiel solution (such as Information Technology system, incremental improvement to an existing capability, or an entirely new "breakout" or other transformational capability). In this way, the ICD can be used to establish boundary conditions for the scope of alternatives to be considered in the subsequent AoA. The AoA study guidance should be crafted to provide a fair balance between focusing the AoA and ensuring that the AoA considers a robust set of novel and imaginative alternatives.

The final AoA supporting a Milestone A decision is provided to the DCAPE not later than 60 days prior to the milestone decision review meeting. The evaluation criteria to be addressed in this assessment are provided in DoD Instruction 5000.02, Enclosure 7, paragraph 5, and are discussed further in section 3.3.4.1.

3.3.2.1. Role of the Analysis of Alternatives (AoA) in Evolutionary Acquisition

The AoA is used to identify the most promising end-state materiel solution, but the AoA also can play a supporting role in crafting a cost-effective and balanced evolutionary acquisition strategy. The alternatives considered in the AoA may include alternative evolutionary paths, each path consisting of intermediate nodes leading to the proposed end-state solution. In this way, the Materiel Solution Analysis can help determine the best path to the end-state solution, based on a balanced assessment of technology maturity and risk, and cost, performance, and schedule considerations (as shown in Figure 3.3.2.1.F1). The rationale for the proposed evolutionary acquisition strategy would be documented as part of the Technology Development Strategy.

Figure 3.3.2.1.F1. Establishment of an Evolutionary Acquisition Strategy



3.3.3. Analysis of Alternatives (AoA) Study Plan

The first major step leading to a successful AoA is the creation and coordination of a well-considered analysis plan. The study plan should establish a roadmap of how the analysis will proceed, and who is responsible for doing what. At minimum, the study plan should facilitate full consideration of possible trade-offs among cost, schedule, and performance objectives for each alternative considered, as well as an assessment of whether or not the joint military requirement can be met in a manner that is consistent with the cost and schedule objectives recommended by the JROC.

A recommended outline for the AoA plan would resemble the following:

- Introduction
  - Background
  - Purpose
  - Scope
- Ground Rules
  - Scenarios
  - Threats
  - Environment
  - Constraints and Assumptions
  - Timeframe

    - Excursions
- Alternatives
    - Description of Alternatives
    - Nonviable Alternatives
    - Operations Concepts
    - Sustainment Concepts
- Determination of Effectiveness Measures
    - Mission Tasks
    - Measures of Effectiveness
    - Measures of Performance
- Effectiveness Analysis
    - Effectiveness Methodology
    - Models, Simulations, and Data
    - Effectiveness Sensitivity Analysis
- Cost Analysis
    - Life-Cycle Cost Methodology
    - Additional Total Ownership Cost Considerations (if applicable)
    - Fully Burdened Cost of Delivered Energy (if applicable)
    - Models and Data
    - Cost Sensitivity and/or Risk Analysis
- Cost-Effectiveness Comparisons
    - Cost-Effectiveness Methodology
    - Displays or Presentation Formats
    - Criteria for Screening Alternatives
- Organization and Management
    - Study Team/Organization
    - AoA Review Process
    - Schedule

Of course, every AoA is unique, and the above outline may need to be tailored or streamlined to support a given situation. Each point in the above outline is discussed further in the next several sections.

3.3.3.1. Analysis of Alternatives (AoA) Study Plan-Introduction

The introduction to the AoA plan describes the developments that led to the AoA, including prior relevant analyses (such as the Capabilities-Based Assessment. It should reference the applicable capability needs document(s) and other pertinent documents, and highlight the capability gaps being addressed through the applicable capability needs. The introduction should describe the applicable AoA study guidance and any other terms of reference. It also should provide a broad overview of the planned AoA that describes in general terms the level of detail of the study, and the scope (breadth and depth) of the analysis necessary to support the specific milestone decision.

3.3.3.2. Analysis of Alternatives (AoA) Study Plan-Ground Rules

The ground rules described in the analysis plan include the scenarios and threats, as well as the assumed physical environment and any constraints or additional assumptions. The scenarios are typically derived from defense planning scenarios and associated joint operational plans, augmented by more detailed intelligence products such as target information and enemy and friendly orders of battle. Environmental factors that impact operations (e.g., climate, weather, or terrain) are important as well. In addition, environment, safety, and occupational health factors associated with the use of chemical and/or biological weapons may need to be considered as excursions to the baseline scenario(s).

The study plan should describe what future timeframe, or timeframes, will be considered in the analysis. Often, the time period(s) selected will be determined by the time period(s) assumed in the DoD-approved planning scenario. However, there is some flexibility on this point, especially if something significant-such as the deployment of a new capability, or the retirement of a legacy system-is projected to occur one or two years after one of the time periods in the scenario. A common and desirable practice is to consider two time periods of interest, say "near-term" and "far-term," separated by a decade or so.

The AoA study plan should describe the planned analytic excursions to the baseline scenarios and other major ground rules. Such excursions are strongly encouraged in order to explore any impact of changing threat levels, warning times, involvement of allied forces, political constraints on basing or overflights, just to name a few issues. These excursions can be used to see if there any major issues that are critical to the relative cost-effectiveness of the alternatives considered in the AoA.

3.3.3.3. Analysis of Alternatives (AoA) Study Plan-Range of Alternatives

The analysis plan also should document the range of alternatives to be addressed in the analysis. In many cases, there will be a minimum set of alternatives required by the initial analysis guidance. Additional direction during subsequent AoA reviews may insert yet other alternatives. Practically, the range of alternatives should be kept manageable. Selecting too few or too many are both possibilities, but experience has shown that selecting too many, exceeding the available resources of the AoA study team, is the greater concern. The number of alternatives can be controlled by avoiding similar but slightly different alternatives and by early elimination of alternatives (due to factors such as unacceptable life-cycle cost or inability to meet Key Performance Parameters). In many studies, the first alternative (base case) is to retain one or more existing systems, representing a benchmark of current capabilities. An additional alternative based on major upgrades and/or service-life extensions to existing systems also may be considered.

For each alternative, evaluating its effectiveness and estimating its life-cycle cost (or total ownership cost, if applicable) requires a significant level of understanding of its

operations and support concepts. The operations concept describes the details of the peacetime, contingency, and wartime employment of the alternative within projected military units or organizations. It also may be necessary to describe the planned basing and deployment concepts (contingency and wartime) for each alternative. The sustainment concept for each alternative describes the plans and resources for system training, maintenance, and other logistics support.

It is important that the alternatives considered in the AoA should address alternative concepts for maintenance, training, supply chain management, and other major sustainment elements. In this way, the AoA can identify the preferred materiel solution not only in terms of traditional performance and design criteria (e.g., speed, range, lethality), but also in terms of support strategy and sustainment performance as well. In other words, the AoA should describe and include the results of the supportability analyses and trade-offs conducted to determine the most cost-effective support concept as part of the proposed system concept.

3.3.3.4. Analysis of Alternatives (AoA) Study Plan-Effectiveness Measures

The analysis plan should describe how the AoA will establish metrics associated with the military worth of each alternative. Military worth often is portrayed in AoAs as a hierarchy of mission tasks, measures of effectiveness, and measures of performance. Military worth is fundamentally the ability to perform mission tasks, which are derived from the identified capability needs. Mission tasks are usually expressed in terms of general tasks to be performed to correct the gaps in needed capabilities (e.g., hold targets at risk, or communicate in a jamming environment). Mission tasks should not be stated in solution-specific language. Measures of effectiveness are more refined and they provide the details that allow the proficiency of each alternative in performing the mission tasks to be quantified. Each mission task should have at least one measure of effectiveness supporting it, and each measure of effectiveness should support at least one mission task. A measure of performance typically is a quantitative measure of a system characteristic (e.g., range, weapon load-out, logistics footprint, etc.) chosen to enable calculation of one or more measures of effectiveness. Measures of performance are often linked to Key Performance Parameters or other parameters contained in the approved capability needs document(s). Also, measures of performance are usually the measures most directly related to test and evaluation criteria.

3.3.3.5. Analysis of Alternatives (AoA) Study Plan-Effectiveness Analysis

The analysis plan spells out the analytic approach to the effectiveness analysis, which is built upon the hierarchy of military worth, the assumed scenarios and threats, and the nature of the selected alternatives. The analytic approach describes the level of detail at various points of the effectiveness analysis. In many AoAs involving combat operations, the levels of effectiveness analysis can be characterized by the numbers and types of alternative and threat elements being modeled. A typical classification would consist of four levels: (1) system performance, based on analyses of individual components of each alternative or threat system, (2) engagement, based on analyses of the interaction

of a single alternative and a single threat system, and possibly the interactions of a few alternative systems with a few threat systems, (3) mission, based on assessments of how well alternative systems perform military missions in the context of many-on-many engagements, and (4) campaign, based on how well alternative systems contribute to the overall military campaign, often in a joint context. For AoAs involving combat support operations, the characterization would need to be modified to the nature of the support. Nevertheless, most AoAs involve analyses at different levels of detail, where the outputs of the more specialized analysis are used as inputs to more aggregate analyses. At each level, establishing the effectiveness methodology often involves the identification of suitable models (simulation or otherwise), other analytic techniques, and data. This identification primarily should be based on the earlier selection of measures of effectiveness. The modeling effort should be focused on the computation of the specific measures of effectiveness established for the purpose of the particular study. Models are seldom good or bad per se; rather, models are either suitable or not suitable for a particular purpose.

It also is important to address excursions and other sensitivity analyses in the overall effectiveness analysis. Typically, there are a few critical assumptions that often drive the results of the analysis, and it is important to understand and point out how variations in these assumptions affect the results. As one example, in many cases the assumed performance of a future system is based on engineering estimates that have not been tested or validated. In such cases, the effectiveness analysis should describe how sensitive the mission or campaign outcomes are to the assumed performance estimates.

3.3.3.6. Analysis of Alternatives (AoA) Study Plan-Cost Analysis

The AoA plan also describes the approach to the life-cycle cost (or total ownership cost (see section 3.1.5, if applicable) analysis. The cost analysis normally is performed in parallel with the operational effectiveness analysis. It is equal in importance as part of the overall AoA process. It estimates the total life-cycle cost (or total ownership cost) of each alternative, and its results are later combined with the operational effectiveness analysis to portray cost-effectiveness comparisons. What is important to emphasize is that the cost analysis will be a major effort that will demand the attention of experienced, professional cost analysts.

The principles of economic analysis apply to the cost analysis in an AoA. Although the cost estimates used in an AoA originally are estimated in constant dollars, they should be adjusted for discounting (time value of money), accounting for the distribution of the costs over the study time period of interest. In addition, the cost estimates should account for any residual values associated with capital assets that have remaining useful value at the end of the period of analysis. Further guidance on economic analysis is provided in DoD Instruction 7041.3, "Economic Analysis for Decisionmaking."

The cost analysis should also describe the planned approach for addressing the Fully Burdened Cost of Energy, for those AoAs where this issue is applicable. See section

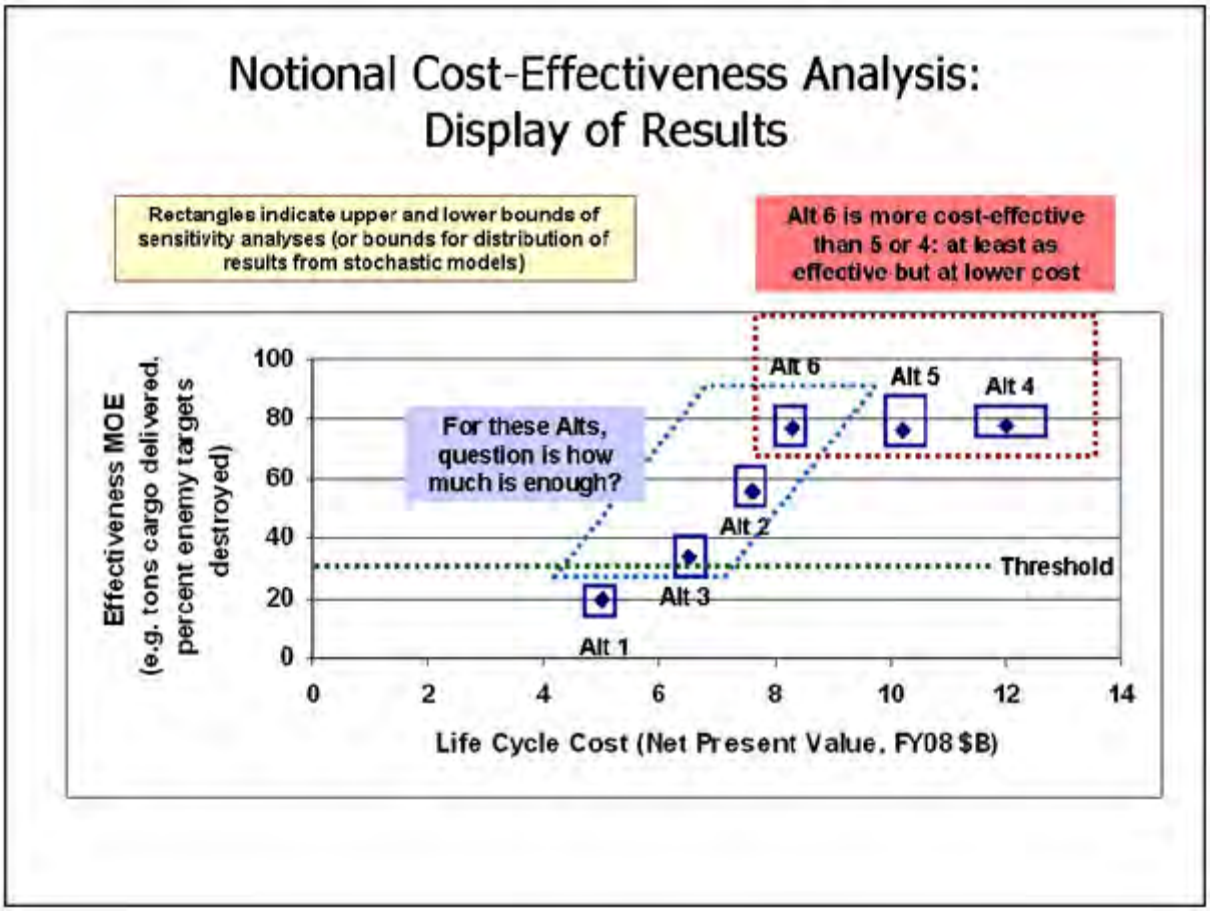
3.3.4.1 for further information on this topic.

Further information on the recommended analytic approach for cost estimates is provided in section 3.7.

3.3.3.7. Analysis of Alternatives (AoA) Study Plan-Cost-Effectiveness Comparisons

Typically, the next analytical section of the AoA plan deals with the planned approach for the cost-effectiveness comparisons of the study alternatives. In most AoAs, these comparisons involve alternatives that have both different effectiveness and cost, which leads to the question of how to judge when additional effectiveness is worth additional cost. Cost-effectiveness comparisons in theory would be best if the analysis structured the alternatives so that all the alternatives have equal effectiveness (the best alternative is the one with lowest cost) or equal cost (the best alternative is the one with greatest effectiveness). Either case would be preferred; however, in actual practice, in many cases the ideal of equal effectiveness or equal cost alternatives is difficult or impossible to achieve due to the complexity of AoA issues. A common method for dealing with such situations is to provide a scatter plot of effectiveness versus cost. Figure 3.3.3.7.F1 presents a notional example of such a plot.

Figure 3.3.3.7.F1. Sample Scatter Plot of Effectiveness versus Cost



Note that the notional sample display shown in Figure 3.3.3.7.F1 does not make use of ratios (of effectiveness to cost) for comparing alternatives. Usually, ratios are regarded as potentially misleading because they mask important information. The advantage to the approach in the figure above is that it reduces the original set of alternatives to a small set of viable alternatives for decision makers to consider.

3.3.3.8. Analysis of Alternatives (AoA) Study Plan-Organization and Management

Finally, the AoA plan should address the AoA study organization and management. Often, the AoA is conducted by a working group (study team) led by a study director and staffed appropriately with a diverse mix of military, civilian, and contractor personnel. Program offices or similar organizations may provide assistance or data to the AoA study team, but (per DoD Instruction 5000.02, Enclosure 7) the responsibility for the AoA may not be assigned to a program manager, and the study team members should not reside in a program office. In some cases, the AoA may be assigned to an in-house analytic organization, a federally funded research and development center, or some other similar organization.

The AoA study team is usually organized along functional lines into panels, with a chair for each panel. Typical functional areas for the panels could be threats and scenarios, technology and alternatives (responsible for defining the alternatives), operations and support concepts (for each alternative), effectiveness analysis, and cost analysis. In many cases, the effectiveness panel occupies the central position and integrates the work of the other panels. The study plan also should describe the planned oversight and review process for the AoA. It is important to obtain guidance and direction from senior reviewers with a variety of perspectives (operational, technical, and cost) throughout the entire AoA process.

The analysis plan is fundamentally important because it defines what will be accomplished, and how and when it will be accomplished. However, the plan should be treated as a living document, and updated as needed throughout the AoA to reflect new information and changing study direction. New directions are inevitably part of the AoA process, and so the analysis should be structured so as to be flexible. Frequently, AoAs turn out to be more difficult than originally envisioned, and the collaborative analytical process associated with AoAs is inherently slow. There are often delays in obtaining proper input data, and there may be disagreements between the study participants concerning ground rules or alternatives that lead to an increase in excursions or cases to be considered. Experience has shown that delays for analyses dealing with Special Access materials can be especially problematic, due to issues of clearances, access to data, storage, modeling, etc. It is often common for the study director to scale back the planned analysis (or at least consider doing so) to maintain the study schedule.

3.3.4. Analysis of Alternatives Final Results

3.3.4.1. Analysis of Alternatives (AoA) Final Results and Assessment

Normally, the final results of the AoA initially are presented as a series of briefings. For potential and designated major defense acquisition programs (Acquisition Category (ACAT) I) and major automated information systems (ACAT IA), the final AoA results are provided to the Office of the Director, Cost Assessment and Program Evaluation (CAPE), no later than 60 days prior to the milestone decision meeting (Defense Acquisition Board or Information Technology Acquisition Board review). Providing emerging results to CAPE prior to the final briefing is wise to ensure that there are no unexpected problems or issues. For other programs, the AoA results should be provided to the DoD Component entity equivalent to CAPE, if applicable. In any case, the AoA final results should follow all of the important aspects of the study plan, and support the AoA findings with the presentation. In particular, all of the stated AoA conclusions and findings should follow logically from the supporting analysis.

Having received the final AoA briefing(s), the CAPE evaluates the AoA and provides an independent assessment to the Head of the DoD Component (or the Principal Staff Assistant) and to the Milestone Decision Authority. DoD Instruction 5000.02, Enclosure 7, provides the evaluation criteria for this assessment. According to the Instruction, the CAPE, in collaboration with the OSD and Joint Staff, shall assess the extent to which

the AoA:

1. Illuminated capability advantages and disadvantages;
2. Considered joint operational plans;
3. Examined sufficient feasible alternatives;
4. Discussed key assumptions and variables and sensitivity to changes in these;
5. Calculated costs; and,
6. Assessed the following:

- Technology risk and maturity;
- Alternative ways to improve the energy efficiency of DoD tactical systems with end items that create a demand for energy, consistent with mission requirements and cost effectiveness; and
- Appropriate system training to ensure that effective and efficient training is provided with the system.

The recommended template for the AoA study plan provided in Section 3.3.3 provides considerable guidance for conducting an AoA that would be responsive to the first five assessment criteria.

For the issue of technology risk and maturity, Section 3.3.2.1 provides a suggested approach where the AoA can help craft a cost-effective evolutionary acquisition strategy that is based on a balanced assessment of technology maturity and risk, as well as cost, performance, and schedule considerations.

For the issue of energy efficiency (applicable to tactical systems with end items that create a demand for delivered fuel or other forms of energy), Section 3.1.6 describes the analytic construct known as the Fully Burdened Cost of Delivered Energy; the Department now intends for this construct to play a major role in applicable AoAs.

For the issue of system training, the AoA should consider alternatives that provide for the individual, collective, and joint training for system operators, maintainers, and support personnel. The training system includes simulators and other training equipment, as well as supporting material such as computer-based interactive courseware or interactive electronic technical manuals. Where possible, the alternatives should consider options to exploit the use of new learning techniques, simulation technology, embedded training (i.e., training capabilities built into, strapped onto, or plugged into operational systems) and/or distributed learning to promote the goals of enhancing user capabilities, maintaining skill proficiencies, and reducing individual and collective training costs. Further information on system training is provided in Section 6.3.3. In addition to addressing the assessment criteria explicitly identified in DoD Instruction 5000.02, Enclosure 7, the AoA should also address alternative concepts for maintenance, supply chain management, and other sustainment elements (see Chapter 5 of this Guidebook).

3.3.4.2. Analysis of Alternatives (AoA) Final Report

Usually, in addition to a final briefing, the AoA process and results are documented in a written final report. The report typically is not published formally by the time of the program milestone decision review, due to schedule constraints. However, the report nevertheless may be important to the historical record of the program, since the report serves as the principal supporting documentation for the AoA. The report also may serve as a reference source for analysts conducting future AoAs. The final report can follow the same format as the study plan, with the addition of these sections:

- Effectiveness Analysis
  - Effectiveness Results
- Cost Analysis
  - Life-Cycle Cost (or Total Ownership Cost, if applicable) Results
- Cost-Effectiveness Comparisons
  - Cost-Effectiveness Results
  - Assessment of Preferred Alternative(s)

By following the same format, much of the material from the (updated) study plan can be used in the final report.

3.3.5. Analysis of Alternatives (AoA) Considerations for Major Automated Information Systems (MAIS)

DoD Instruction 5000.02, Enclosure 4, Table 2-1 and Table 3, requires an AoA for MAIS programs at milestone decisions. Much of the discussion on AoAs provided in the earlier sections of the Guidebook is more applicable to weapon systems, and needs to be modified somewhat for MAIS programs. This section discusses AoA issues for MAIS programs. The AoA should include a discussion of whether the proposed program (1) supports a core/priority mission or function performed by the DoD Component, (2) needs to be undertaken because no alternative private sector or governmental source can better support the function, and (3) supports improved work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial off-the-shelf technology. The analysis should be tied to benchmarking and business process reengineering studies (such as analyses of simplified or streamlined work processes, or outsourcing of non-core functions).

For all MAIS program AoAs, one alternative should be the status quo alternative as used in the Economic Analysis, and one alternative should be associated with the proposed MAIS program. Other possible alternatives could be different system, network, and/or data architectures, or they might involve different options for the purchase and integration of commercial-off-the-shelf products, modifications, and upgrades of existing assets, or major in-house development.

Most likely, the effectiveness analysis in a MAIS program AoA will not involve scenario-based analysis as is common for the weapon system AoAs. The effectiveness analysis

for an MAIS program should be tied to the organizational missions, functions, and objectives that are directly supported by the implementation of the system being considered. The results of the AoA should provide insight into how well the various alternatives support the business outcomes that have been identified as the business goals or capabilities sought. In some cases, it may be possible to express the assessment of effectiveness across the alternatives in monetary terms, and so effectiveness could be assessed as benefits in the framework for the Economic Analysis. In other cases, the effectiveness might be related to measurable improvements to business capabilities or better or timelier management information (leading to improved decision-making, where it can be difficult or impossible to quantify the benefits). In these cases, a common approach is to portray effectiveness by the use of one or more surrogate metrics. Examples of such metrics might be report generation timeliness, customer satisfaction, or supplier responsiveness. In addition to management information, the effectiveness analysis also should consider information assurance and interoperability issues.

The cost analysis supporting the AoA should follow the framework of the Economic Analysis. The life-cycle cost estimates of the alternatives considered in the AoA should be consistent with and clearly linked to the alternatives addressed in the Economic Analysis. Both the effectiveness analysis and the cost analysis should address the risks and uncertainties for the alternatives, and present appropriate sensitivity analysis that describes how such uncertainties can influence the cost-effectiveness comparison of the alternatives.

The appropriate sponsor or domain owner should lead the development of the AoA for a MAIS program. Experience has shown that the MAIS programs for which the sponsor or domain owner engages with the Office of the Director, Cost Assessment and Program Evaluation (CAPE) early in the process are much more likely to be successful than those that select a preferred alternative before contacting CAPE or before completing the AoA.

The DoD Component performing the AoA should develop a study plan that addresses the AoA study guidance, as applicable. At a minimum, the study plan should address the following topics:

AoA Study Plan Outline

a. Introduction (Background, Purpose & Scope)
b. Ground Rules: Constraints and Assumptions
c. Description of Alternatives
d. Determination of Effectiveness Measures
    1. Measures of Effectiveness (MOEs) operationally relevant & measurable
    2. Measures of Performance technical characteristics required to satisfy MOEs and are measurable & employed as an operational test criteria
e. Effectiveness Analysis Methodology
f. Cost Analysis

g. Cost-Effectiveness Comparisons
h. Risk & Sensitivity Analysis

    1. Mission
    2. Technology
    3. Programmatic, to include funding

i. Study Organization and Management
j. Schedule, with associated deliverables

3.4. Cost Estimation for Major Defense Acquisition Programs

3.4.1. Independent Cost Estimates

The Director, Cost Assessment and Program Evaluation (DCAPE), conducts independent cost estimates (ICEs) for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) programs for which the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Milestone Decision Authority. An ICE is required for MDAPs prior to certification at

Milestone A, certification at Milestone B, before any decision to enter into low-rate initial production or full-rate production, and in advance of certification following critical cost growth. An ICE is required for MAIS programs that have experienced a critical change. An ICE may be conducted by DCAPE for MDAPs and MAIS programs for which USD(AT&L) is the MDA at any time considered appropriate by DCAPE or upon the request of the USD(AT&L).

For ACAT ID programs, DCAPE conducts the ICE (as described in Section 3.4.3), and for ACAT IC programs, the appropriate Service Cost Center or Defense Agency equivalent conducts the ICE. The Service Cost Centers are in the financial management organizations of their respective military departments, and are outside of their department's acquisition chain-of-command.

DCAPE and the Secretary of the Military Department concerned are required by Congress to report certain elements of program cost risk for MDAP and MAIS programs. For such programs, DCAPE and the Secretary of the Military Department concerned (or the head of the Defense Agency concerned) must state the confidence level used in establishing a cost estimate, the rationale for selecting the confidence level, and ensure that the confidence level provides a high degree of confidence that the program can be completed without the need for significant adjustment to program budgets.

The confidence level disclosure shall be included in the ADM approving the APB; in any other cost estimates for MDAPs or MAIS programs prepared in association with the estimates prepared in accordance with Section 3.4.1, above; and for MDAPs, in the next Selected Acquisition Report prepared in accordance with 10 U.S.C. 2432, or for MAIS programs, in the next quarterly report prepared in accordance with 10 U.S.C. 2445c.

3.4.2. DoD Component Cost Estimates

DCAPE reviews all cost estimates and cost analyses conducted in conjunction with MDAPs and MAIS programs. In order to accomplish this, 10 U.S.C. 2334(b) requires that DCAPE promptly receive the results of all cost estimates and analyses conducted by military departments and Defense Agencies (together, "DoD Component Cost Estimates").

Each DoD Component establishes a DoD Component-level cost position for all MDAPs and MAIS programs at milestone reviews. To support the Department's full funding policy for acquisition programs (see section 3.2.3), as well as statutory certifications and regulatory requirements, the DoD Component is expected to fully fund the program to this cost position in the current President's Budget Future Years Defense Program (FYDP), or commit to full funding of the cost position in the next President's Budget FYDP, with identification of specific offsets to address any funding shortfalls that may exist in the current FYDP. In addition, the appropriate Deputy Assistant Secretary of the Military Department for Cost and Economics (or defense agency equivalent) signs for

the DoD Component-level cost position, and the DoD Component Acquisition Executive and the Component Chief Financial Officer endorses and certifies that the FYDP fully funds the program consistent with the DoD Component-level cost position. This policy was promulgated in the OSD Memorandum, "Required Signed and Documented Component-level Cost Position for Milestone Reviews," dated March 12, 2009.

3.4.3. Office of Cost Assessment

3.4.3.1. Cost Assessment Reviews (Pre-Milestone Decisions and Full-Rate Production)

3.4.3.1.1. Cost Assessment Review Events-180 Days before Overarching Integrated Product Team (OIPT) Meeting

3.4.3.1.2. Cost Assessment Review Events-45 Days before Overarching Integrated Product Team (OIPT) Meeting

3.4.3.1.3. Cost Assessment Review Events-21 Days before Overarching Integrated Product Team (OIPT) Meeting

3.4.3.1.4. Cost Assessment Review Events-10 Days before Overarching Integrated Product Team (OIPT) Meeting

3.4.3.1.5. Cost Assessment Review Events-3 Days before Overarching Integrated Product Team (OIPT) Meeting

The Office of Cost Assessment (CA), within the Office of Cost Assessment and Program Evaluation (CAPE), receives the results of and reviews all cost estimates and cost analyses and associated studies conducted by the DoD Components for major defense acquisition programs (MDAPs) and major automated information system (MAIS) programs and has timely access to any records and data in the Department.

During the CA review process, CA staff may engage in discussion with the DoD Components regarding any discrepancies related to the cost estimates and comment on deficiencies regarding the methodology or execution of cost estimates. Furthermore, the Director, CAPE, is authorized to concur with the choice of a cost estimate used to support the acquisition program baseline (APB).

Although CA will provide periodic reviews, certain reviews are regular and required. For programs subject to CAPE review (normally Acquisition Category ID) that are approaching Milestone decisions or the Full-Rate Production Decision Review, CA staff conducts a comprehensive review, establishes a formal position on a program's life-cycle cost, and advises the Milestone Decision Authority accordingly. The CA review consists of preparation of an independent life-cycle cost estimate as well as an

assessment of the DoD Component Cost Estimate. This section provides a brief summary of the major events associated with the CA review and provides additional information on the procedures for each event. A more comprehensive description of the Cost Assessment review process is found in DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Section 2.

Table 3.4.3.1.T1 provides a brief summary of the major events and timelines associated with a Cost Assessment review leading to a Defense Acquisition Board milestone decision review:

Table 3.4.3.1.T1. Cost Assessment Timeline Associated with a DAB Milestone Decision Review

Event	Date
• Cost Assessment Review Kick-off Meeting o Draft Cost Analysis Requirements Description (CARD) Delivered by DoD Component	180 days before Overarching Integrated Product Team (OIPT) meeting
• Cost Assessment Briefs Preliminary Independent Life-Cycle Cost Estimate (LCCE) to Program Manager (PM) o Draft Documentation of DoD Component Cost Estimate Delivered by DoD Component o Final CARD Delivered by DoD Component	45 days before OIPT meeting
• Cost Assessment Review Meeting o PM Representative Briefs Program Defined in CARD, and Program Office Cost Estimate o DoD Component Representative Briefs Component Cost Position, if applicable o Cost Assessment Briefs Final Estimate of Independent LCCE to PM	21 days before OIPT meeting
• Final Documentation of DoD Component Cost Estimate Delivered by DoD Component	10 days before OIPT meeting
• OSD Cost Assessment Report Delivered to OIPT Members	3 days before OIPT meeting

3.4.3.1.1. Cost Assessment Review Events-180 Days before Overarching Integrated Product Team (OIPT) Meeting

The Cost Assessment (CA) review process begins roughly six months before the planned Defense Acquisition Board milestone review. At that time, the draft Cost Analysis Requirements Description (CARD) is provided to CA for review. The CARD is used to describe formally the acquisition program for purposes of preparing both the DoD Component Cost Estimate and the CA independent cost estimate. CA staff promptly evaluates the CARD for completeness and consistency with other program documents (such as capability needs documents, acquisition strategy, etc.). As part of this evaluation, CA staff may require access to privileged information such as contractor proposals that are proprietary or source selection sensitive. CA staff will follow all necessary procedures to ensure that the integrity of the privileged information is protected.

The expectation is that the CARD should be sufficiently comprehensive in program definition to support a life-cycle cost estimate. Normally, CA staff provides any necessary feedback to the DoD Component if any additional information or revisions are needed. If the CARD is found to be deficient to the point of unacceptability, the Deputy Director, CA, will advise the OIPT leader that the planned milestone review should be postponed.

At roughly the same time that the draft CARD is submitted, CA staff announces its upcoming review in a formal memo. The memo initiates a working-level kick-off meeting that is held with representatives from the program office cost estimating team, the CA independent cost estimate team, and other interested parties (typically DoD Component or OSD staff members). The purpose of the meeting is to discuss requirements and issues for the upcoming milestone review, the scope of the cost estimates, and ground rules and assumptions on which the estimates will be based. Much of the discussion will focus on material provided in the draft CARD. This ensures that both cost teams have a common understanding of the program to be costed. In addition, ground rules are established for CA interactions with the program office. CA staff also coordinates any travel or visit requirements with appropriate DoD Component points of contact.

3.4.3.1.2. Cost Assessment Review Events-45 Days before Overarching Integrated Product Team (OIPT) Meeting

Per DoD Instruction 5000.02, Enclosure 7, section 4, Cost Assessment (CA) staff will brief the preliminary independent Life-Cycle Cost Estimate (LCCE) to the program manager (PM) 45 days before the OIPT meeting. In a similar timeframe, the program office should provide draft documentation of its estimate to the CA staff, and if applicable, the DoD Component should provide draft documentation of the DoD Component Cost Position. The CA report eventually submitted to the OIPT and to the Defense Acquisition Board membership provides not only the CA independent cost estimate but also an evaluation of the DoD Component Cost Estimate. It is therefore important for the DoD Components to submit well-documented cost estimates that are

ready for review.

The specific standards for the cost documentation are described in DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Sections 1 and 2. In general, the documentation should be sufficiently complete and well organized that a cost professional could replicate the estimate, given the documentation. Along with the draft documentation of the program office cost estimate, the DoD Component provides an updated (and final) Cost Analysis Requirements Description to CA staff. At the same time that the documents are provided, CA staff will provide feedback and identify any emerging cost issues to the program manager and DoD Component staff, in part based on CA work to date on its independent cost estimate.

3.4.3.1.3. Cost Assessment Review Events-21 Days before Overarching Integrated Product Team (OIPT) Meeting

Per DoD Instruction 5000.02, Enclosure 7, section 4, CA staff will brief the results of the independent cost estimate to the program manager 21 days before the OIPT meeting. This is normally handled as part of the CA review meeting. At this time, the program office should provide their final estimate to the Cost Assessment staff, and the DoD Component should provide the final DoD Component Cost Position. Other invited OSD and Joint Staff representatives may attend these reviews/exchanges. A typical presentation format for the Cost Assessment review meeting would include:

- Program overview and status
- Program office acquisition cost estimate
    - Summary of results
    - Methodology for high-cost elements
- Rationale for DoD Component cost position, if applicable
- Comparison of (time-phased) program office cost estimate to current funding
- Operating and Support cost estimate

In addition, at the CA meeting, CA staff provides any further feedback to the program office and DoD Component staff. If appropriate, CA staff will provide a presentation of the major areas of difference between its independent cost estimate and the program office cost estimate and/or DoD Component cost position.

3.4.3.1.4. Cost Assessment Review Events-10 Days before Overarching Integrated Product Team (OIPT) Meeting

At least 10 days before the OIPT meeting, the DoD Component provides final documentation if its cost estimate (program office cost estimate, or DoD Component Cost Position where applicable).

3.4.3.1.5. Cost Assessment Review Events-3 Days before Overarching Integrated Product Team (OIPT) Meeting

Cost Assessment (CA) staff's final report is delivered to the OIPT leader at least three days before the OIPT meeting. Immediately thereafter, it is distributed to the OIPT members and is available to the DoD Component staff. The expectation is that any issues had already emerged in prior discussions and that the final CA report should not contain any surprises. The report normally is two to three pages and typically includes the following:

- Summary of DoD Component Cost Estimate
- Summary of Cost Assessment independent cost estimate
- Comparison or reconciliation of the two estimates
- Assessment of program risks
- Comparison of (time-phased) Cost Assessment cost estimate to current program funding
    - Recommendations concerning program funding

3.4.3.2. Cost Estimates for Milestone A Reviews

Per DoD Instruction 5000.02, Enclosure 2, section 5.c.(5), the DoD Component at Milestone A submits a cost estimate for the proposed materiel solution(s). Also, per 10 U.S.C. 2334, the Director of Cost Assessment and Program Evaluation (DCAPE) conducts an independent cost estimate in advance of Milestone A certification. In order to facilitate these estimates, the cost estimating procedures at Milestone A will track those at the other milestone decisions points. This includes the required preparation of a Cost Analysis Requirements Description (CARD), see below, although the early stage of the program development will necessitate less specificity in many of the required elements within the CARD.

The actual process and timing leading to the DoD Component estimate may vary among programs, and therefore, a tailored approach should be developed and proposed. Early in the Materiel Solution Analysis Phase, the Program Manager and DoD Component staff should work with the OSD Office of Cost Assessment (CA) and Acquisition Resources & Analysis staffs to develop a plan and schedule for delivery of the cost estimate to support the upcoming Milestone A review. The plan is subject to approval of the Milestone Decision Authority (MDA).

The DoD Component Cost Estimate, in addition to the DCAPE independent cost estimate, is used to support the MDA certification requirements for Milestone A (10 U.S.C. 2366a). The emphasis for the Milestone A cost estimate is to provide costing adequate to support the selection of the preferred materiel solution(s) identified by the Analysis of Alternatives, and to support a determination by the MDA that current funding for the Technology Development Phase (required technology development, competitive

prototyping, and possibly preliminary design of the end-item system) is adequate. The Milestone A cost estimate is a complete estimate of the system life-cycle cost. However, for the costs associated with the acquisition phases beyond Technology Development (i.e., Engineering and Manufacturing Development, Production and Deployment, and Operations and Support), the Milestone A cost estimate typically would not have the same level of rigor or fidelity as will later cost estimates (prepared for milestones B and beyond). Although the cost estimate addresses the complete life-cycle cost, since it must support the Analysis of Alternatives process, only the program development and procurement costs are subject to certification.

The DoD Component Cost Estimate submitted at Milestone A should be based on a sound description of the program and follow the general requirements of the CARD. Understandably, programs at Milestone A are less well-defined than programs at later milestone decision points. The Initial Capabilities Document, Technology Development Strategy, Systems Engineering Plan, Test and Evaluation Strategy, and Analysis of Alternatives, together with the CARD, should be used to provide a technical and programmatic description that should be the foundation for the cost estimate.

Note that if the certified cost estimate grows at least 25 percent during the Technology Development Phase, then the Program Manager must notify the MDA of the increase. The MDA in turn consults with the Joint Requirements Oversight Council to reassess program requirements and the military need(s) for the system. See DoD Instruction 5000.02, Enclosure 2, section 5.c.(3) for further guidance.

3.4.4. Cost Assessment Reporting Requirements

3.4.4.1. Cost Analysis Requirements Description (CARD)

A sound cost estimate is based on a well-defined program. For Acquisition Category (ACAT) I and ACAT IA programs, the CARD is used to formally describe the acquisition

program for purposes of preparing both the DoD Component Cost Estimate and the Cost Assessment independent cost estimate. DoD Instruction 5000.02 specifies that for major defense acquisition programs, the CARD will be provided in support of major milestone decision points (Milestone B, Milestone C, or the full-rate production decision review). In addition, for Major Automated Information Systems, the CARD is prepared whenever an Economic Analysis is required. For other acquisition programs, the preparation of a CARD, or an abbreviated CARD-like document with appropriate tailoring, is strongly encouraged to provide a written program description suitable to support a credible life-cycle cost estimate.

The CARD is prepared by the program office and approved by the DoD Component Program Executive Officer. For joint programs, the CARD includes the common program agreed to by all participating DoD Components as well as all unique program requirements of the participating DoD Components. DoD 5000.4-M, "DoD Cost Analysis Guidance and Procedures," Chapter 1, provides further guidelines for CARD content.

3.4.4.1.1. Cost Analysis Requirements Description (CARD) Outline

- System description and characteristics
    - System overview
    - System performance parameters and characteristics
    - Technical and physical description
    - Work breakdown structure
    - Summary of maturity levels of critical technologies
    - Software description and sizing information
    - Interfaces with other systems
    - Subsystem descriptions, as appropriate
- System suitability factors
    - Reliability/Maintainability/Availability
- Predecessor and/or Reference System
- PM's assessment of program risk and risk mitigation measures
- System operational concept
    - Organizational/unit structure
    - Basing and deployment description (peacetime, contingency, and wartime)
    - System sustainment concept
    - System logistics concept
        - Maintenance concept
        - Supply management concept
        - Transportation concept
    - Software maintenance concept
    - System training concept
- Time-phased system quantity requirements
- System manpower requirements
- System activity rates (operating tempo or similar information)
- Facilities requirements

- Summary of security or program protection features
- Summary of environment, safety, and occupational health considerations
- System milestone schedule
- Summary of acquisition plan or strategy
- Plans for system disposal
- Track to prior CARD
- Approved or proposed CSDR plan

3.4.4.1.2. Cost Analysis Requirements Description (CARD) Content

For each topic listed in the suggested outline, the CARD should provide information and data for the program to be costed. In addition, the CARD should include quantitative comparisons between the proposed system and a predecessor and/or reference system for the major topics, as much as possible. A reference system is a currently operational or pre-existing system with a mission similar to that of the proposed system. It is often the system being replaced or augmented by the new acquisition. For a program that is a major upgrade to an existing weapon platform, such as an avionics replacement for an operational aircraft, the new system would be the platform as equipped with the upgrade, and the reference system would be the platform as equipped prior to the upgrade. For Major Automated Information System programs, the CARD format described above may need to be tailored.

The level of detail provided in the CARD will depend on the maturity of the program. Programs at the Pre-Engineering and Manufacturing Development Review are less well-defined than programs at Milestone C or at full-rate production. In cases where there are gaps or uncertainties in the various program descriptions, these uncertainties should be acknowledged as such in the CARD. This applies to uncertainties in either general program concepts or specific program data. For uncertainties in program concepts, nominal assumptions should be specified for cost-estimating purposes. For example, if the future depot maintenance concept were not yet determined, it would be necessary for the CARD to provide nominal (but specific) assumptions about the maintenance concept. For uncertainties in numerical data, ranges that bound the likely values (such as low, most likely and high estimates) should be included. In general, values that are "to be determined" are not adequate for cost estimating. Dealing with program uncertainty in the CARD greatly facilitates subsequent sensitivity or quantitative risk analyses in the life-cycle cost estimate.

For programs employing an evolutionary acquisition strategy, the CARD should be structured to reflect the specifics of the approach. Although the circumstances may vary somewhat by program, normally the CARD should attempt to include as much of the program, including known future increments, as can be described at the time of the milestone decision review, and clearly document any exclusions for portions of the program that cannot be defined at the present time.

The last section of the CARD should contain a copy of the approved Cost and Software Data Reporting plan (see section 3.4.4.2), if available. If the plan has not yet been

approved, then the proposed plan should be included as part of the CARD.

3.4.4.1.3. Cost Analysis Requirements Description (CARD) and Other Program Documentation

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to cost in the appropriate section of the CARD and provide a reference to the source document. DoD Instruction 5000.02, Enclosure 7, paragraph 2, states that the program manager shall synchronize preparation of the CARD with other program documentation so that the final CARD is consistent with other final program documentation. The source documents should be readily available to the program office and independent cost estimating teams or can be provided as an appendix to the CARD. Many program offices provide controlled access to source documents through a web site (perhaps at a ".mil" web address or on the Secret Internet Protocol Router Network).

Common source documents for the CARD include:

- Technology Readiness Assessment (TRA);
- Capability Needs Documents (i.e., Initial Capabilities Document / Capability Development Document /Capability Production Document);
- Acquisition Strategy;
- Life-cycle Sustainment Plan (part of the Acquisition Strategy);
- Test and Evaluation Master Plan;
- Manpower Estimate; and
- Systems Engineering Plan.

The CARD should be consistent with any contractual solicitations, such as a Request for Proposal or any accompanying document (e.g., System Requirements Document).

3.4.4.1.4. Cost Analysis Requirements Description (CARD) at Milestone B

For programs at the Pre-Engineering and Manufacturing Development (EMD) Review, the program content described in the final CARD should reflect the program definition established during the Technology Development Phase. For all MDAPs, the Preliminary Design Review (PDR) may be conducted before the Pre-EMD Review and Milestone B approval, and the CARD should also incorporate the results from the PDR for such cases.

Another issue for the CARD at the Pre-EMD Review can occur when the Technology Development Phase maintains two or more competing contractor teams (that are producing prototypes of the system) up to and through the PDR. In this situation, there are two possible approaches for the preparation of the CARD. If the competing teams

are using similar technologies and designs, then a single generic CARD, based on a nominal Government design, may be used to prepare a single ICE for the nominal design. If the competing teams have significantly different technologies or designs, then it may be necessary to prepare offeror-specific CARDs, which in turn may be used to prepare multiple ICEs. For programs with competing prototype teams approaching a Pre-EMD Review, the DoD Component should discuss its proposed use of a single generic CARD, or use of multiple offeror-specific CARDs, with the Cost Assessment staff at the Kick-Off Review meeting (see section 3.4.3.1.1), if not earlier.

3.4.4.2. Cost and Software Data Reporting (CSDR)

The CSDR system is the primary means that DoD uses to collect and program managers use to report actual cost, software, and related business data on Acquisition Category (ACAT) I, ACAT IA, pre-MDAP, pre-MAIS, and sustainment defense contracts. The repository of collected data serves as the primary contract cost and software data repository for most DoD resource analysis efforts, including cost database

development, applied cost estimating, cost research, program reviews, analysis of alternatives, and life cycle cost estimates. The two principal components of CSDR are contractor cost data reporting (CCDR) and software resources data reporting (SRDR).

The Deputy Director, Cost Assessment establishes procedural guidance and reporting formats for the CSDR system and monitors implementation throughout the Department of Defense. DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual," establishes the policies and procedures for CSDR and provides report formats and definitions, specific report examples, and other related information. The CSDR Manual is available on the Defense Cost and Resource Center (DCARC) web site. Access to CSDR data is readily provided by DCARC to DoD government cost analysts and sponsored support contractors possessing Non-Disclosure Agreements who are registered users.

3.4.4.2.1. Contractor Cost Data Reporting (CCDR)

The CCDR system collects data on the development, production, and sustainment costs incurred by contractors in performing DoD ACAT I, ACAT IA, pre-MDAP, pre-MAIS, and sustainment program contracts. DoD Instruction 5000.02, Enclosure 4, Table 4, establishes the CCDR requirements for Acquisition Category I and IA contracts and sub-contracts, regardless of contract type. Detailed procedures and other implementation guidance are found in DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual."

CCDR focuses on the collection of actual total contract costs that are subdivided into standard categories for cost estimating purposes by Work Breakdown Structure (WBS), functional categories, and resource elements. CCDR reports provide a display of incurred costs to date and estimated incurred costs at completion by elements of the WBS, with nonrecurring costs and recurring costs separately identified. In some cases, CCDR reports can display incurred costs to date and estimated incurred costs at completion by functional category (manufacturing labor, engineering, etc.). Where appropriate, a functional category is broken out by direct labor hours, direct material, overhead, and other indirect.

3.4.4.2.1.1. Contractor Cost Data Reporting (CCDR) Requirements

CCDR reports are required on all major contracts and subcontracts, regardless of contract type, for Acquisition Category I and IA programs and pre-Major Defense Acquisition Program and pre-Major Automated Information System programs subsequent to Milestone A approval, valued at more than $50 million Then year dollars. CCDRs are not required for contracts priced below $20 million Then year dollars. The CCDR requirement on high-risk or high-technical-interest contracts priced between $20 and $50 million is left to the discretion of the DoD Program Manager (PM) based upon the advice of the Cost Working-level Integrated Product Team (CWIPT). These requirements must also be approved by the Deputy Director, Cost Assessment. CCDRs are not required for procurement of commercial systems provided the DoD PM requests

and obtains approval for a reporting waiver from the Deputy Director, Cost Assessment.

3.4.4.2.1.2. Contractor Cost Data Reporting (CCDR) Level of Reporting

CCDR shall normally be at level 3 (level 4 for space contracts) of the Contract Work Breakdown Structure (WBS) and determined separately for each prime contractor and subcontractor that meets the reporting thresholds. Reporting at levels 4 and below shall be required on prime contracts or subcontracts containing WBS elements that address high-risk, high-value, or high-technical-interest areas of a program. Such reporting applies only if the CWIPT proposes and the Deputy Director, Cost Assessment approves.

3.4.4.2.1.3. Contractor Cost Data Reporting (CCDR) Report Timing

Initial reports, if required, are due within 60 days following the completion of the integrated baseline review when a pre-award or post-award conference is held. If a conference is not held, the initial report, if required, is due within 180 days of contract award. For subsequent reporting on development contracts, reporting contractors typically shall submit CCDR reports after such major events as first flight or completion of prototype, before major milestones, and upon contract completion. Annual reporting is allowed if requested and approved by the Deputy Director, Cost Assessment. For production, reporting contractors normally shall submit CCDR reports upon the delivery of each annual lot for all weapon systems. Due to the extended construction process for ships, CCDR reports are also required for the total number of ships in each buy and for each individual ship within that buy at three intervals-initial report (total buy and individual ships), the mid-point of first ship construction (individual ships only) or other relevant timeframe as the CWIPT determines, and after final delivery (total buy and individual ships).

3.4.4.2.1.4. Contractor Cost Data Reporting (CCDR) Formats and Instructions

CCDR reports consist of the following forms:

- DD Form 1921, "Cost Data Summary Report"
- DD Form 1921-1, "Functional Cost-Hour Report"
- DD Form 1921-2, "Progress Curve Report"
- DD Form 1921-3, "Contractor Business Data Report"

The related instructions are included in the DIDs for these forms as follows:

- DD Form 1921: DID, DI-FNCL-81565
- DD Form 1921-1 DID, DI-FNCL-81566
- DD Form 1921-2 DID, DI-FNCL-81567
- DD Form 1921-3 DID, DI-FNCL-81765

The forms including the Microsoft Excel templates and the link to the official DIDs are

shown on the DCARC web site. The DCARC also provides software which will produce the forms from an excel flat file.

3.4.4.2.2. Software Resources Data Reporting (SRDR)

The SRDR system collects software metrics data to supplement the actual Contractor Cost Data Reporting (CCDR) data in order to provide a better understanding and improved estimating of software intensive programs. DoD Instruction 5000.02, Enclosure 4, Table 4, establishes SRDR requirements for Acquisition Category I and IA contracts and sub-contracts, regardless of contract type. Detailed procedures and other implementation guidance are found in DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual."

3.4.4.2.2.1. Software Resources Data Reporting (SRDR) General Requirements

SRDRs are required on all major contracts and subcontracts, regardless of contract type, for contractors developing/producing software elements within Acquisition Category I and IA programs and pre-Major Defense Acquisition Program and pre-Major Automated Information System programs subsequent to Milestone A approval for any software development element with a projected software effort greater than $20M Then year dollars. The SRDR requirement on high-risk or high-technical-interest contracts priced below $20 million is left to the discretion of the DoD Program Manager (PM) based upon the advice of the Cost Working-level Integrated Product Team (CWIPT). These requirements must also be approved by the Deputy Director, Cost Assessment.

3.4.4.2.2.2. Software Resources Data Reporting (SRDR) Level of Reporting

The program office, in coordination with the CWIPT, may choose to combine a set of smaller releases within a contract into a single release for reporting purposes. Separate software element developments within a single contract may be reported on separately or may be aggregated at the discretion of the DoD PM based upon the advice of the CWIPT.

3.4.4.2.2.3. Software Resources Data Reporting (SRDR) Report Timing

Within 60 days of contract award, the software developer shall submit an SRDR Initial Developer Report for the entire software product, customized as agreed to by the DoD PM in coordination with the CWIPT. The software developer also shall submit an SRDR Initial Developer Report for each deliverable software release or element within 60 days of the beginning of its development. In addition, the software developer shall submit an "as built" SRDR Final Developer Report, customized as agreed to by the CWIPT, within 60 days after delivery of each software release or element to the U.S. Government.

3.4.4.2.2.4. Software Resources Data Reporting (SRDR) Formats and Instructions

SRDR reports consist of the sample SRDR formats which are contained within the

report instructions as follows:

- SRDR Sample Format 1, "Software Resources Data Reporting: Initial Government Report"
- SRDR Sample Format 2, "Software Resources Data Report: Initial Developer Report and Data Dictionary"
- SRDR Sample Format 3, "Software Resources Data Report, Final Developer Report and Data Dictionary"

The instructions for the Initial Government Report can be found on the DCARC web site. The instructions for the other two reports are contained in DIDs DI-MGMT-81739 and DI-MGMT-81740, respectively. Links to the official DIDs and the Microsoft Excel templates are also found on the DCARC web site. To note, SRDR formats should be tailored based upon the way the software developer performs its activities and the related metrics it uses. The three sample SRDR formats are intended as the starting point for developing tailored reports that capture the developer's unique software process.

3.4.4.2.3. Data Collection and Availability

CSDR data is collected and stored in a central repository, the Defense Automated Cost Information Management System (DACIMS), maintained by the DCARC. DACIMS has more than thirty five years of contractor cost data. DACIMS access is easy and quick for all authorized DoD users. The DCARC web site and Chapter 5 of the CSDR Manual, DoD 5000.04-M-1, contain specific registration instructions.

DACIMS may be used to obtain cost data to estimate total program acquisition costs, including work by both contractors and the U.S. Government; total program contract costs, awarded and future, for a particular contractor; and individual contract costs.

Reporting Formats and Instructions. The CSDR system includes two formats and instructions that apply to both CCDRs and SRDRs, four unique CCDRs, and three unique SRDRs. The two CSDRs are shown in this section while the unique reports are covered in the separate CCDR and SRDR sections. The DD Form 2794, "Cost and Software Data Reporting Plan" (commonly referred to as the "CSDR Plan") describes the proposed collection of data by individual report, by work breakdown structure (WBS) and reporting frequency. The plan must be approved by the Deputy Director, Cost Assessment prior to issuance of a contract solicitation. The Deputy Director, Cost Assessment, may waive the information requirements prescribed in Table 4 in Enclosure 4 of DoDI 5000.02. The format for the Contract Work Breakdown Structure is contained within the Data Item Description (DID) (DI-MGMT-81334, current edition). The CSDR Plan format and instructions and the link to the official DID can be found at the DCARC web site.

Training. The DCARC provides periodic CSDR training at various sites throughout CONUS for both government and contractor personnel. DCARC strongly encourages

stakeholders to attend these training sessions and schedules classes to meet stakeholder requirements. The training schedule and various training materials can also be found at the DCARC web site.

3.4.4.3. Operating and Support (O&S) Cost Data

Historical O&S cost data for currently fielded systems are available from the Visibility and Management of Operating and Support Costs (VAMOSC) data system managed by each DoD military service. The data can be displayed in several different formats, including the Office of Cost Assessment standard cost element structure described previously. Data can be obtained for entire systems, or at lower levels of detail. VAMOSC provides not only cost data, but related non-cost data (such as operating tempo or maintenance man-hours) as well. This type of data is useful for analogy estimates (between proposed systems and appropriate predecessor or reference systems) and for "bottoms-up" engineering estimates (for fielded systems or components, possibly adjusted for projected reliability and maintainability growth). VAMOSC data should always be carefully examined before use in a cost estimate. The data should be displayed over a period of a few years (not just a single year), and stratified by different sources (such as major command or base). This should be done so that abnormal outliers in the data can be identified, investigated, and resolved as necessary.

3.4.4.4. Visibility and Management of Operating and Support Costs (VAMOSC)

To achieve visibility into the Operating and Support (O&S) costs of major fielded weapon systems, DoD requires that each military service will maintain an historical data collection system that collects O&S data in a standard presentation format. The Office of Cost Assessment provides policy guidance on this requirement, known as the VAMOSC program, and monitors its implementation by each of the military services. Each service has its own unique VAMOSC data system that tracks actual O&S cost experience for major weapon systems. The data can be displayed by time frame, at various levels of detail, and by functional elements of cost (such as depot maintenance, fuel, consumable items, and so forth). Each VAMOSC system provides not only cost data, but related non-cost data (such as system quantities, operating tempo, or maintenance man-hours) as well. VAMOSC data can be used to analyze trends in O&S cost experience for each major system, as well as to identify and assess major cost drivers. In addition, VAMOSC data are important as a data source for cost estimates of future systems, since cost estimates for future systems are often made by analogy to appropriate predecessor systems. DoD 5000.04-M, "DoD Cost Analysis Guidance and Procedures," Section 8, provides additional direction for VAMOSC.

3.5. Manpower Estimates

3.5. Manpower Estimates

For major defense acquisition programs, manpower estimates are required by

- (1) 10 U.S.C. 2434, which directs the Secretary of Defense to consider an estimate of the personnel required to operate, maintain, support, and provide system-related training in advance of approval of the development, or production and deployment; and
- (2) DoD Instruction 5000.02, Enclosure 4, Table 2-1, which directs development of a manpower estimate at Milestones B, C, and full-rate production.

Manpower estimates serve as the authoritative source for out-year projections of active-duty and reserve end-strength, civilian full-time equivalents, and contractor support work-years. As such, references to manpower in other program documentation should be consistent with the manpower estimate once it is finalized. In particular, the manpower estimates should be consistent with the manpower levels assumed in the final Affordability Analysis and the Cost Analysis Requirements Description (CARD).

Organizational responsibilities in preparing the manpower estimate vary by DoD Component. Normally, the manpower estimate is prepared by an analytic organization in the DoD Component manpower community, in consultation with the program manager. The manpower estimates are approved by the DoD Component manpower authority (for the military departments, normally the Assistant Secretary for Manpower and Reserve Affairs).

For Acquisition Category ID programs, a preliminary manpower estimate should be made available at least six months in advance of the Defense Acquisition Board (DAB) milestone review, and should be reflected in the draft CARD due at that time, in order to support the development of cost estimates and affordability analyses. The final manpower estimate should be fully staffed and submitted to the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) in sufficient time to support the Overarching Integrated Product Team (OIPT) review in preparation of the DAB meeting. Normally this would be four weeks prior to the OIPT review meeting. The USD(P&R) staff will review the final manpower estimate and provide comments to the OIPT.

The exact content of the manpower estimate is tailored to fit the particular program under review. A sample format for the manpower estimate is displayed in the Table 3.5.T1 below. In addition, the estimate should identify if there are any resource shortfalls (i.e., discrepancies between manpower requirements and authorizations) in any fiscal year addressed by the estimate. Where appropriate, the manpower estimate should compare manpower levels for the new system with those required for similar legacy systems, if any. The manpower estimate also should include a narrative that describes the scope of each functional area (operations, maintenance, support, and training), and the methods, factors, and assumptions used to estimate the manpower for each

functional area. See section 6.3.1.2 and section 6.3.1.3 for further information concerning manpower.

Table 3.5.T1. Sample Manpower Estimate Format MANPOWER ESTIMATE (Program Title) SERVICE

	FYxx [2]	FYxx+1	FYxx+2	FYxx+3	FYxx+4	... [3]
OPERATE: [4] Military Officers Enlisted Civilian Contractor Sub-Total						
MAINTAIN: [4] Military Officers Enlisted Civilian						
Contractor Sub-Total						
SUPPORT: [4] Military Officers Enlisted Civilian Contractor Sub-Total						
TRAIN: [4] Military Officers Enlisted Civilian Contractor Sub-Total						
TOTAL						

[1] Provide separate estimates for Active and Reserve Components for each Service.
[2] Report manpower by fiscal year (FY) starting with initial fielding and continuing through retirement and disposal of the system (to include environmental clean-up).
[3] Until fielding is completed.
[4] Provide estimates for manpower requirements and authorizations. Provide deltas between requirements and authorizations for each fiscal year.

3.6. Major Automated Information Systems Economic Analysis

3.6.1. Introduction

An automated information system (AIS) is a system of computer hardware, computer software, data and/or telecommunications that performs functions such as collecting, processing, storing, transmitting and displaying information; however, systems that are an integral part of a weapon or weapon system are excluded from this definition. AIS programs that meet the specified dollar thresholds in DoD Instruction 5000.02, Enclosure 3, Table 1, qualify as major automated information system (MAIS) programs. MAIS programs that are subject to review by OSD at the Defense Acquisition Board (DAB) are designated Acquisition Category (ACAT) IAM. Other MAIS programs, delegated to the head of the DoD Component or the appropriate DoD Component Acquisition Executive, are designated ACAT IAC. In some cases, an ACAT IA program also meets the definition of a Major Defense Acquisition Program (MDAP). In these cases, the Secretary of Defense may designate that the program be treated only as a MAIS program or only as a major defense acquisition program (MDAP). Generally, a program that requires the development of customized hardware shall be treated only as a MDAP, and a program that does not require the development of customized hardware shall be treated only as a MAIS program.

DoD Instruction 5000.02, Enclosure 4, Table 2-1, requires that an Economic Analysis be performed in support of the Milestone A, Milestone B, and full-rate production decision (or equivalent) reviews. The purpose of the Economic Analysis is to determine the best MAIS program acquisition alternative by assessing the net costs and benefits of the proposed MAIS program relative to the status quo. In general, the best alternative will be the one that meets validated capability needs at the lowest life-cycle cost (measured in net present value terms), and/or provides the most favorable return on investment.

Whenever an Economic Analysis is required, the DoD Component responsible for the program also may be required to provide a DoD Component Cost Analysis, which is an independent estimate of program life-cycle costs. Normally, the Economic Analysis is prepared by the MAIS program office, and the DoD Component Cost Analysis is prepared by an office or entity not associated with the program office or its immediate

chain of command. The need for a DoD Component Cost Analysis at Milestone A is evaluated for each program in tailoring the oversight process.

The Economic Analysis should be accomplished in accordance with DoD Instruction 7041.3, "Economic Analysis for Decision Making." Normally, the DoD Component submits a Final Cost/Benefit Position that resolves the differences between the Economic Analysis and the Component Cost Analysis. Also, the Component and the MDA should address any differences between the Final Cost/Benefit Position and the funding in the current Future Years Defense Program.

In addition to an Economic Analysis, independent cost estimates are occasionally required for MAIS programs. Per 10 U.S.C. 2445c, MAIS programs where the MDA is USD(AT&L) (ACAT IA) that experience critical program changes must undergo an independent cost estimate (ICE) prepared by the Director of Cost Assessment and Program Evaluation (DCAPE). ICEs will also be conducted for MAIS programs at any other time considered appropriate by DCAPE, or upon request by USD(AT&L) (see 10 U.S.C. 2334). Additionally, DCAPE develops an ICE for MAIS Defense Business Systems when the Deputy Chief Management Officer or DoD Chief Information Officer is the MDA and a critical change, as defined in 10 U.S.C. 2445c, has occurred.

3.6.2. Office of Cost Assessment and Program Evaluation Review Procedures

For Acquisition Category IAM programs, both the Economic Analysis and the DoD Component Cost Analysis are subject to independent review and assessment by the Director, Cost Assessment and Program Evaluation (DCAPE).

The purpose of the DCAPEs assessment is to provide the Milestone Decision Authority with an independent determination that (1) the estimates of life-cycle costs and benefits are reasonable, traceable, and reflect DoD policy and DCAPE guidance on the consideration of life-cycle costs, (2) the return on investment calculation is valid, and (3) the cost estimates are built on realistic program and schedule assumptions.

During the review process, DCAPE staff may engage in discussion with the DoD Components regarding any discrepancies related to MAIS cost estimates and comment on deficiencies regarding the methodology or execution of cost estimates. Furthermore, DCAPE staff are authorized to concur with the choice of a cost estimate used to support the acquisition program baseline (APB) as well as in the selection of a proper confidence interval for the MAIS program.

DCAPE and the Secretary of the Military Department concerned are required by Congress to report certain elements of program cost risk for MAIS programs. For such programs, DCAPE and the Secretary of the Military Department concerned (or the head of the Defense Agency concerned) must state the confidence level used in establishing a cost estimate, the rationale for selecting the confidence level, and ensure that the confidence level provides a high degree of confidence that the program can be

completed without the need for significant adjustment to program budgets.

The confidence level disclosure shall be included in the ADM approving the APB and in any other cost estimates for MAIS programs prepared in association with this section.

3.6.2.1. Kick-Off Meeting

The review process normally begins with a kick-off meeting held with DCAPE staff, representatives from the Major Automated Information System (MAIS) program office, the DoD Component Cost Analysis Team, and any DoD Component functional or headquarters sponsors. The purpose of the meeting is to reach a common understanding on the expectations for the upcoming activities and events leading to the Information Technology Acquisition Board milestone review. As a starting point, the DoD Component staff and/or sponsors' representatives should review the contents of the most recently approved capability needs documents, and explain any prior analysis (such as a Capabilities-Based Assessment) used to justify the need for a materiel solution (that will be met by the MAIS program).

At the kick-off meeting, the DoD Component staff and/or sponsors' representatives also should be prepared to explain the planned approach for the upcoming Economic Analysis. To facilitate this dialogue, the MAIS program office should prepare and provide a brief Economic Analysis development plan. The development plan should document the organizational responsibilities, analytic approach, ground rules and assumptions, and schedule for the economic analysis. The development plan should identify the specific alternatives that will be compared in the Economic Analysis. Normally, at least one alternative should be associated with the proposed MAIS program, and one alternative should be associated with the status quo (no modernization investment). It may well be the case that the status quo alternative represents an unacceptable mission posture-it may cost too much to sustain, be unable to meet critical capability needs, or be unsupportable due to technological obsolescence. Nevertheless, the status quo concept, applied over the same time frame (Life Cycle) as the proposed MAIS program, is used for comparative purposes in the Economic Analysis. The Economic Analysis development plan should document the DoD Component Cost Analysis approach and schedule as well.

As part of the Economic Analysis development plan, the program office should propose the cost element structure that will be used to organize and categorize cost estimates in the Economic Analysis. The cost element structure provides a hierarchal framework of defined cost elements that in total comprise the program life-cycle cost. The cost element structure should include phase-out costs associated with the status quo (legacy or predecessor) system. These costs would be incurred in managing, preserving, and maintaining the operations of the status quo system as it runs parallel to the phasing in of the new system. The status quo phase-out cost elements are not used in the estimate of the status quo alternative. A sample of a generic cost element structure is available from DCAPE staff. DCAPE can also provide advice on a consistent approach

to net present value and return on investment computations.

3.6.2.2. Use of the Cost Analysis Requirements Description (CARD) for Major Automated Information System (MAIS) Programs

As soon as possible after the kick-off meeting, the draft Cost Analysis Requirements Description (CARD) is provided to DCAPE staff for review. The CARD is used to define and describe the MAIS program for purposes of preparing both the Economic Analysis and the DoD Component Cost Analysis. For a MAIS program, the CARD typically would address the following elements:

- Program description;
- Program operational concept;
- Program data management requirements;
- Program quantity requirements;
- Program manpower requirements;
- Program fielding strategy;
- Program milestone schedule; and
- Program acquisition plan or strategy.

Procedures for the preparation of the CARD are described in DoD Instruction 5000.02, Enclosure 7, paragraph 2. Additional guidelines on CARD preparation are found in DoD 5000.4 M, "DoD Cost Analysis Guidance and Procedures," Section 1. However, these guidelines are for the most part oriented toward weapon systems and may need to be tailored somewhat for automated information systems. The system description in the CARD should address both hardware and software elements. The CARD should describe each major hardware item (computers, servers, etc.), noting those items that are to be developed, and those items that are off-the-shelf. The CARD also should describe each software configuration item (including applications as well as support software) and identify those items that are to be developed. For software items to be developed, the CARD should provide (1) some type of sizing information (such as counts of source lines of code, function points, or Reports, Interfaces, Conversions and Enhancements (RICE)-Forms and Workflows (FW) (RICE-(FW) objects) suitable for cost estimating, and (2) information about the programming language and environment. In addition, the CARD should describe any special (physical, information, or operations) system security requirements, if applicable.

Clearly, much of the information needed for the CARD is often available in other program documents. The CARD should stand-alone as a readable document, but can make liberal use of appropriate references to the source documents to minimize redundancy and effort. In such cases, the CARD should briefly summarize the information pertinent to the Economic Analysis in the appropriate section of the CARD, and provide a reference to the source document.

3.6.2.3. Office of Cost Assessment and Program Evaluations CARD Review and Assessment

To facilitate the DCAPE review and assessment, the DoD Component's Economic Analysis and Cost Analysis teams should provide written documentation early enough to permit a timely report to the Overarching Integrated Product Team (OIPT) and Information Technology Acquisition Board. The timeline for document submission is the same as the timeline set forth in Section 3.4.3.1 for major defense acquisition programs. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

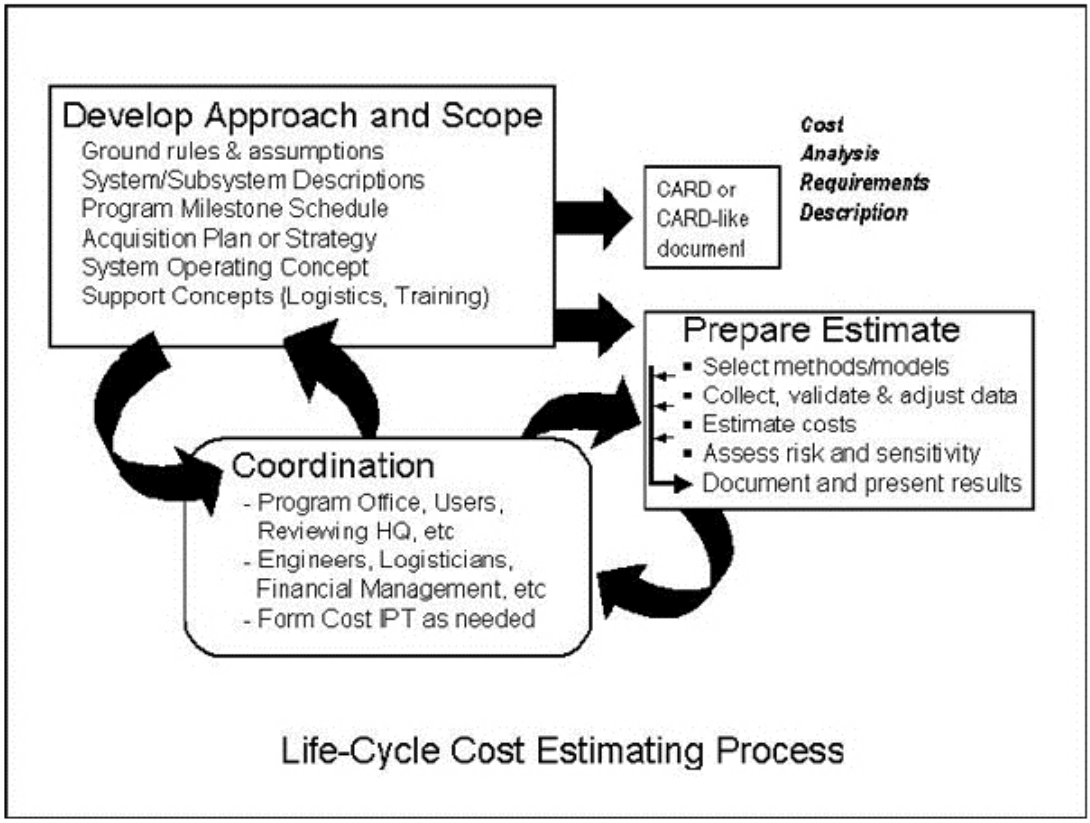
After review of the documentation, DCAPE staff provides feedback to the program office and DoD Component staff. Subsequently, DCAPE staff prepares a written report containing the findings of their independent assessment to the Milestone Decision Authority. Depending on the circumstances, the report may contain recommended cost and benefits positions, and it may raise funding or schedule issues. The expectation is that any issues raised have already emerged in prior discussions and that the final DCAPE report should not contain any surprises.

3.7. Principles for Life-Cycle Cost Estimates

Section 3.4.3 of this Guidebook primarily focused on procedures associated with life-cycle cost estimates which are subject to review by the Office of Cost Assessment for major defense acquisition programs. The estimate is prepared in support of major milestone or other program reviews held by the Defense Acquisition Board. This section is intended to be more generally applicable and somewhat more analytic in nature. It describes a recommended analytic approach for planning, conducting, and documenting a life-cycle cost estimate for a defense acquisition program (whether or not the estimate is subject to Office of Cost Assessment review). Much of the discussion in this section was written with the less experienced cost analyst in mind.

The recommended analytic approach for preparing a life-cycle cost estimate is shown in Figure 3.7.F1:

Figure 3.7.F1. A Recommended Analytic Approach for Life-Cycle Cost Estimates



The next few sections describe this process.

3.7.1. Develop Approach and Scope

The first step in preparing a credible cost estimate is to begin with the development of a sound analytic approach. During this planning phase, critical ground rules and assumptions are established, the scope of the estimate is determined, and the program to be costed is carefully defined and documented. The program definition includes not only a technical and physical description of the system (and perhaps major subsystems), but also a description of the system's program schedule, acquisition strategy, and operating and support concepts. In some cases, it is necessary to state explicitly the costs to be included, and the costs to be excluded. For example, when systems have complex interfaces with other systems or programs (that are outside the scope of the system being costed), the interfaces should be carefully defined.

For programs that will be reviewed by the Office of Cost Assessment, the program office is required to define its program in a comprehensive formal written document known as a Cost Analysis Requirements Description (CARD). The format for this document is briefly summarized in section 3.4.4.1 of this Guidebook, and is completely described in DoD 5000.4 M, "DoD Cost Analysis Guidance and Procedures," Section 1. Much of the

necessary information to prepare a written program description can be extracted and synthesized from common program source documents and contract specifications. The written program description should stand-alone as a readable document, but can make liberal use of suitable references to the source documents to minimize redundancy and effort.

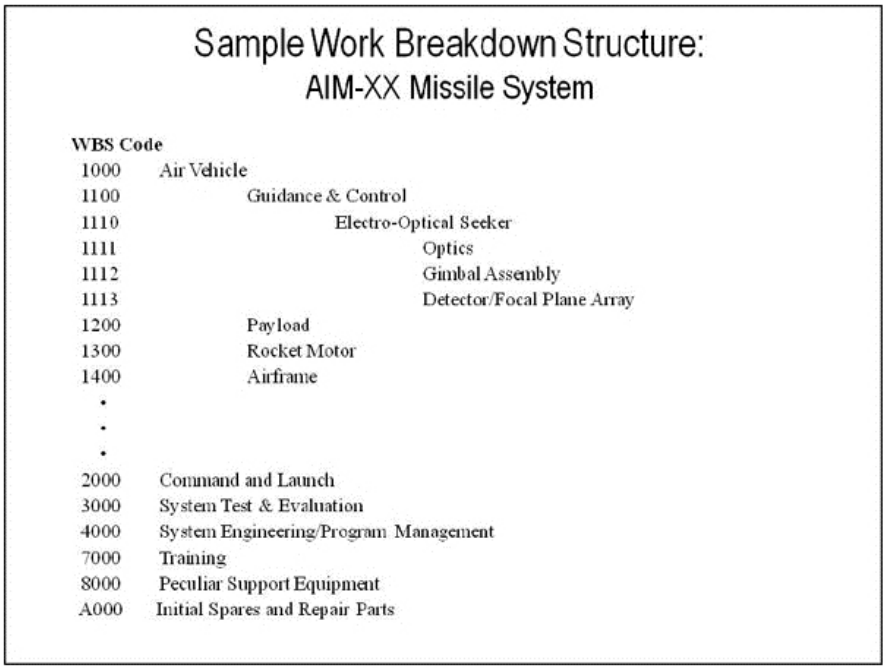
It is important that the analytic approach to the cost estimate be documented and reviewed by all potentially interested parties, before the actual work on preparing the cost estimate begins. This helps ensure that there are no false starts or misunderstandings later in the process.

3.7.1.1. Work Breakdown Structure (WBS)

Part of the system definition typically includes the program work breakdown structure. The program WBS is a hierarchy of product-oriented elements (hardware, deliverable software, data, and services) that collectively comprise the system to be developed or produced. The program WBS relates the elements of work to each other and to the end product. The program WBS is extended to a contract WBS that defines the logical relationship between the elements of the program and corresponding elements of the contract work statement. The WBS provides the framework for program and technical planning, cost estimating, resource allocation, performance measurement, technical assessment, and status reporting. In particular, the contract WBS provides the reporting structure used in contract management reports or reports in the Contractor Cost Data Reporting system. Further information about the WBS can be found in MIL-STD-881C, Work Breakdown Structures for Defense Materiel Items, which is available at the Defense Cost and Resource Center web site.

A sample of the WBS for an air-to-air tactical missile is provided in Figure 3.7.1.1.F1

Figure 3.7.1.1.F1. Sample Work Breakdown Structure



3.7.1.2. Cost Estimating Functional Categories

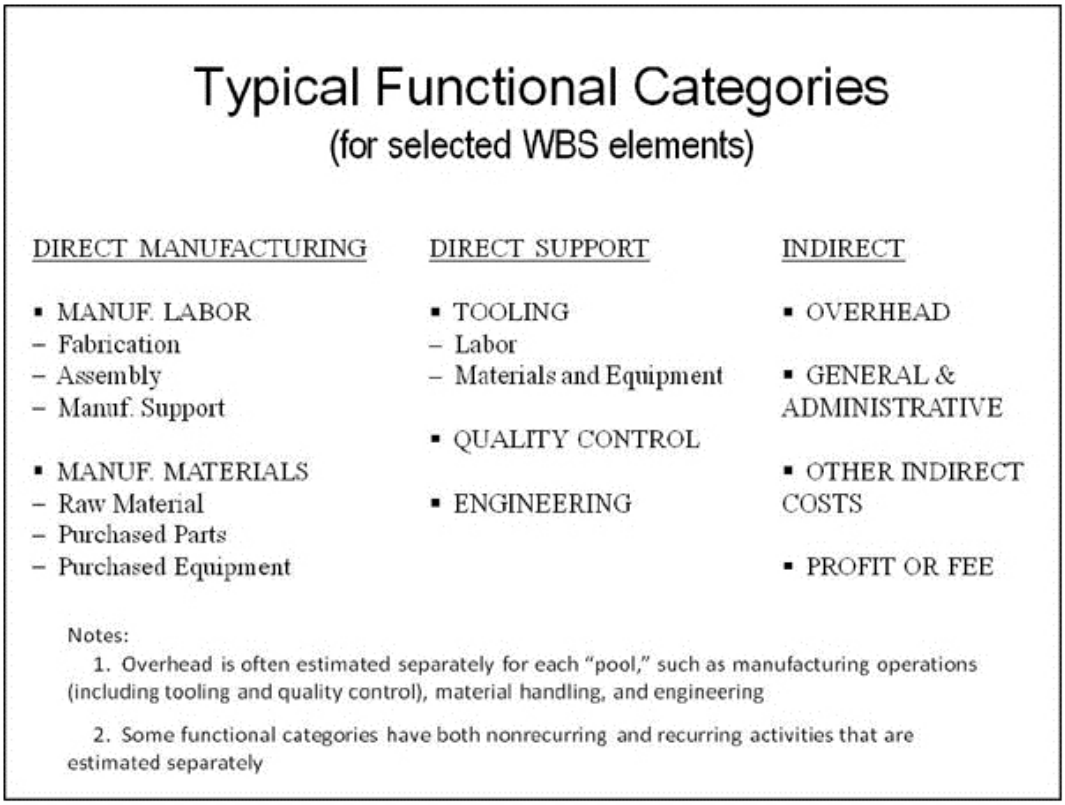
In most cost estimates, selected WBS elements (usually high cost) often are further broken down into functional categories. A typical structure for the functional categories is provided in Figure 3.7.1.2.F1. In the tactical missile example discussed in the last section, most likely the cost estimate for the Airframe WBS element would be broken down by functional category, whereas the cost estimate for the Initial Spares and Repair Parts WBS element most likely would be estimated at the level of total cost, and not by functional category.

Standard terms and definitions for the various functional categories were developed to support the Cost and Software Data Reporting system (see section 3.4.4.2). The terms and definitions used in Figure 3.7.1.2.F1 can be found in the following:

- DoD 5000.04-M-1, "Cost and Software Data Reporting (CSDR) Manual"
- Data Item Description DI-FNCL-81565B, "Cost Data Summary Report (DD Form 1921)"
- Data Item Description DI-FNCL-81566B, "Functional Cost-Hour Report (DD Form 1921-1)"

All of these are available at the Defense Cost and Resource Center web site.

Figure 3.7.1.2.F1. Functional Categories for Cost Estimating



3.7.1.3. Operating and Support (O&S) Cost Element Structure

Another step in developing the analytic approach to the cost estimate is establishing the cost element structure that will be used as the format for the O&S cost estimate. The cost element structure describes and defines the specific elements to be included in the O&S cost estimate in a disciplined hierarchy. Using a formal cost element structure (prepared and coordinated in advance of the actual estimating) identifies all of the costs to be considered, and organizes the estimate results. The cost element structure is used to organize an O&S cost estimate similar to the way that a work breakdown structure is used to organize a development or procurement cost estimate. The intent is to capture all costs of operating, maintaining, and supporting a fielded system (and its associated manpower and facilities). A notional portrayal of these costs, organized into a cost element structure format, is provided in Figure 3.7.1.3.F1. Note that the use of a cost element structure provides considerably more detail than simply using budget appropriation categories (operations and maintenance, military personnel).

Figure 3.7.1.3.F1. O&S Costs Organized by a Cost Element Structure

A standard cost element structure used by the Office of Cost Assessment was introduced in section 3.1.3.3. Details can be found in the OSD CAPE O&S Cost-Estimating Guide. Although each DoD Component (military department or defense agency) may have its own preferred cost element structure, it is expected that each DoD Component will have a cross walk or mapping so that any presentation to the Office of Cost Assessment can be made using the standard structure.

3.7.2. Prepare the Estimate

This section describes the typical steps in preparing a life-cycle cost estimate. The discussion summarizes the steps entailed in selecting estimating techniques or models, collecting data, estimating costs, and conducting sensitivity or risk analysis.

In addition, the importance of good documentation of the estimate is explained.

3.7.2.1. Select Methods and/or Models

A number of techniques may be employed to estimate the costs of a weapon system.

The suitability of a specific approach will depend to a large degree on the maturity of the program and the level of detail of the available data. Most cost estimates are accomplished using a combination of the following estimating techniques:

- **Parametric.** The parametric technique uses regression or other statistical methods to develop Cost Estimating Relationships (CERs). A CER is an equation used to estimate a given cost element using an established relationship with one or more independent variables. The relationship may be mathematically simple or it may involve a complex equation (often derived from regression analysis of historical systems or subsystems). CERs should be current, applicable to the system or subsystem in question, and appropriate for the range of data being considered.

- **Analogy.** An analogy is a technique used to estimate a cost based on historical data for an analogous system or subsystem. In this technique, a currently fielded system, similar in design and operation to the proposed system, is used as a basis for the analogy. The cost of the proposed system is then estimated by adjusting the historical cost of the current system to account for differences (between the proposed and current systems). Such adjustments can be made through the use of factors (sometimes called scaling parameters) that represent differences in size, performance, technology, and/or complexity. Adjustment factors based on quantitative data are usually preferable to adjustment factors based on judgments from subject-matter experts.

- **Engineering Estimate.** With this technique, the system being costed is broken down into lower-level components (such as parts or assemblies), each of which is costed separately for direct labor, direct material, and other costs. Engineering estimates for direct labor hours may be based on analyses of engineering drawings and contractor or industry-wide standards. Engineering estimates for direct material may be based on discrete raw material and purchase part requirements. The remaining elements of cost (such as quality control or various overhead charges) may be factored from the direct labor and material costs. The various discrete cost estimates are aggregated by simple algebraic equations (hence the common name "bottoms-up" estimate). The use of engineering estimates requires extensive knowledge of a system's (and its components') characteristics, and lots of detailed data.

- **Actual Costs.** With this technique, actual cost experience or trends (from prototypes, engineering development models, and/or early production items) are used to project estimates of future costs for the same system. These projections may be made at various levels of detail, depending on the availability of data. Cost estimates that support a full-rate production milestone decision should be based on actual cost data to the greatest extent possible. A common mistake is to use contract prices as a substitute for actual cost experience. Contract prices should not be used to project future costs (even when firm-fixed price) unless it is known that the contract prices are associated with profitable ventures, and that it

is reasonable to assume that similar price experience will be obtained for subsequent contracts.

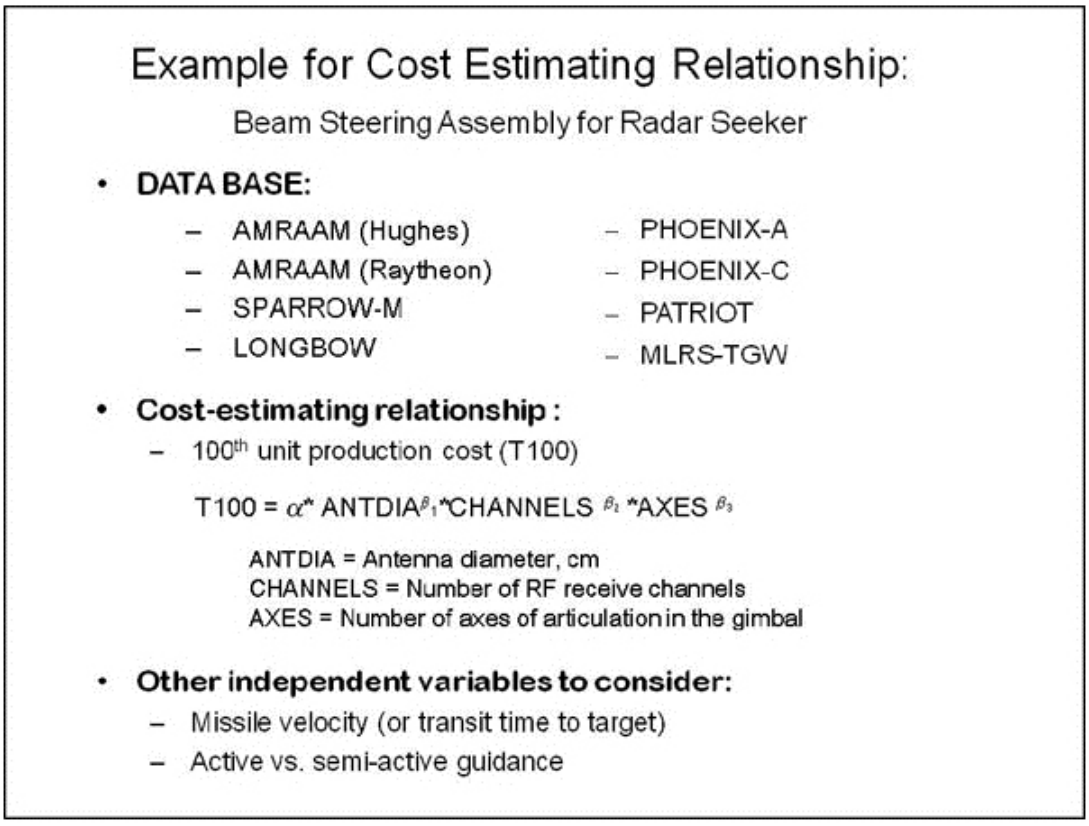
In many instances, it is a common practice to employ more than one cost estimating method, so that a second method can serve as a cross-check to the preferred method. Analogy estimates are often used as cross-checks, even for estimates of mature systems based on actual costs.

The next two sections provide two illustrative examples of common cost estimating techniques.

3.7.2.1.1. Example #1-Cost Estimating Relationship

An exemplar cost estimating relationship is provided in Figure 3.7.2.1.1.F1. The relationship is used to estimate production costs for a component of a tactical missile, using various technical characteristics as independent variables. Developing a good relationship requires not only sound statistical practice, but also considerable experience and insight on the part of the cost analyst. It also requires detailed and well-understood data.

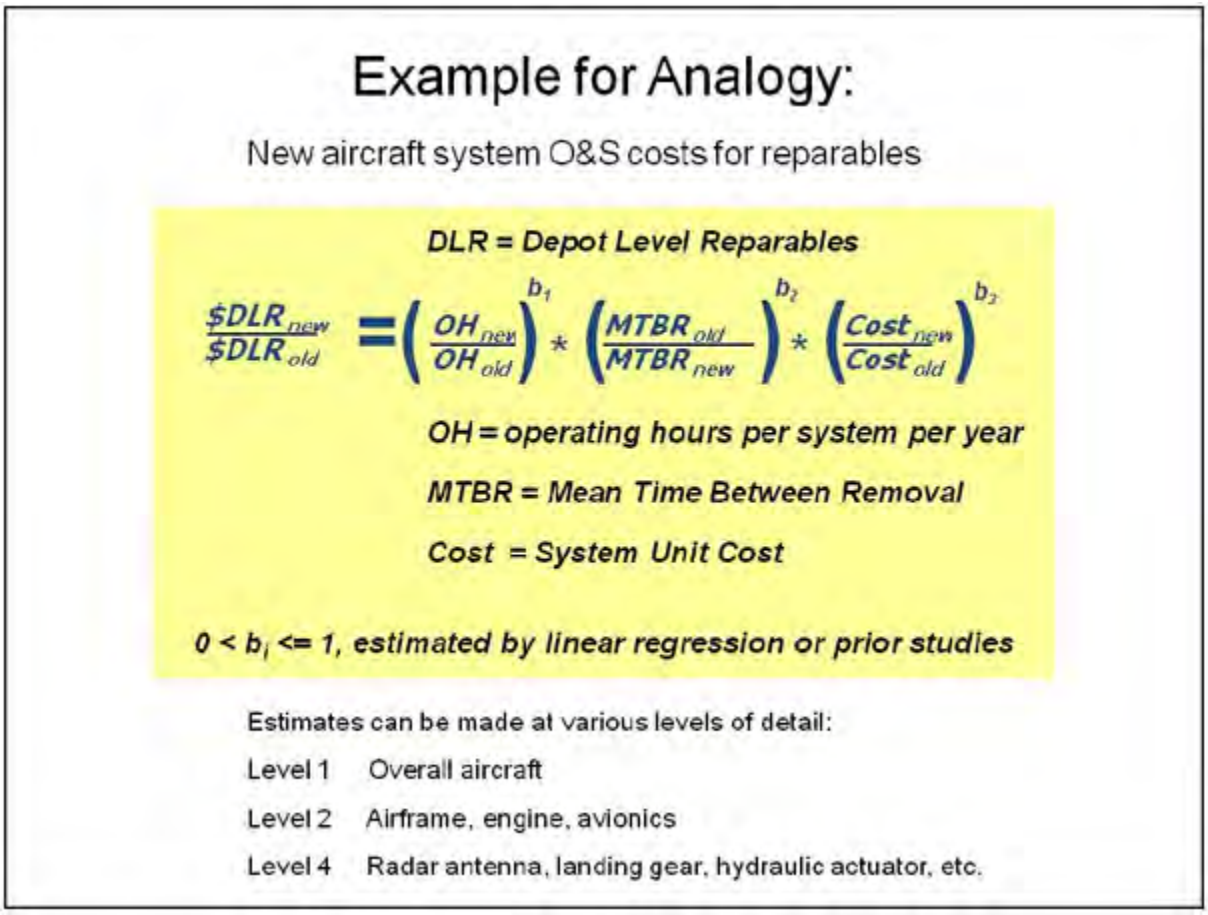
Figure 3.7.2.1.1.F1. Illustrative Cost Estimating Relationship



3.7.2.1.2. Example #2-Analogy

An exemplar cost estimate by analogy is provided in Figure 3.7.2.1.2.F1. In this case, an estimate for one of the Operating and Support (O&S) cost elements (depot level reparables) for a future aircraft system is made by direct analogy to a predecessor aircraft system with a similar mission. Note that the analogy uses scaling parameters for operating (i.e., flying) hours, reliability, and system unit cost. In many analogy estimates, unit cost is often used as a proxy for complexity.

Figure 3.7.2.1.2.F1. Illustrative Cost Estimate by Analogy



3.7.2.2. Collect, Validate, and Adjust Data

There are many possible sources of data that can be used in cost estimates. Regardless of the source, the validation of the data (relative to the purpose of its intended use) always remains the responsibility of the cost analyst. In some cases, the data will need to be adjusted or normalized. For example, in analogy estimates, the reference system cost should be adjusted to account for any differences in system characteristics (technical, physical, complexity, or hardware cost) or operating

environment between the reference system and the proposed system being costed.

3.7.2.2.1. Acquisition Cost Data

Actual cost experience on past and current acquisition programs often forms the basis of estimates of future systems. The Cost and Software Data Reporting (CSDR) system is the primary means within the Department of Defense to systematically collect data on the development and production costs and other resource usage incurred by contractors in performing DoD acquisition program contracts associated with major defense acquisition programs. DoD Instruction 5000.02 makes CSDR reporting mandatory for all major contracts and subcontracts, regardless of contract type valued at more than $50 million (then-year dollars). Program managers use the CSDR system to report data on contractor development, production, and sustainment costs and resource usage incurred in performing DoD programs. Further, the Defense Federal Acquisition Regulation Supplement (DFARS) establishes requirements for CSDR Reporting to be included in the proposals and contract performance for major acquisition programs (MDAPs) and Major Automated Information Systems (MAIS). Additional information on cost data reporting is found in section 3.4.4.2. of this Guidebook.

3.7.2.3. Estimate Costs

With the completion of the steps described earlier in this chapter, the actual computations of the cost estimate can begin. It is important to assess critically the outputs from the estimating methods and models, drawing conclusions about reasonableness and validity. Peer review is often helpful at this point. For complex cost estimates, with many elements provided from different sources, considerable effort and care are needed to deconflict and synthesize the various elements.

3.7.2.4. Assess Risk and Sensitivity

For any system, estimates of future life-cycle costs are subject to varying degrees of uncertainty. The overall uncertainty is not only due to uncertainty in cost estimating methods, but also due to uncertainties in program or system definition or in technical performance. Although these uncertainties cannot be eliminated, it is useful to identify associated risk issues and to attempt to quantify the degree of uncertainty as much as possible. This bounding of the cost estimate may be attempted through sensitivity analyses or through a formal quantitative risk analysis.

Sensitivity analysis attempts to demonstrate how cost estimates would change if one or more assumptions change. Typically, for the high-cost elements, the analyst identifies the relevant cost-drivers, and then examines how costs vary with changes in the cost-driver values. For example, a sensitivity analysis might examine how maintenance manning varies with different assumptions about system reliability and maintainability values, or how system manufacturing labor and material costs vary with system weight growth. In good sensitivity analyses, the cost-drivers are not changed by arbitrary

plus/minus percentages, but rather by a careful assessment of the underlying risks. Sensitivity analysis is useful for identifying critical estimating assumptions, but has limited utility in providing a comprehensive sense of overall uncertainty.

In contrast, quantitative risk analysis can provide a broad overall assessment of variability in the cost estimate. In risk analysis, selected factors (technical, programmatic and cost) are described by probability distributions. Where estimates are based on cost models derived from historical data, the effects of cost estimation error may be included in the range of considerations included in the cost risk assessment. Risk analysis assesses the aggregate variability in the overall estimate due to the variability in each input probability distribution, typically through Monte-Carlo simulations. It is then possible to derive an estimated empirical probability distribution for the overall life-cycle cost estimate. This allows the analyst to describe the nature and degree of variability in the estimate.

Sensitivity and risk analyses also have uses beyond addressing the uncertainty in cost estimates. They also can be used to help better understand what can go wrong with a program, and focus appropriate management attention to risk areas that are concerns. The history of DoD weapon system acquisition would indicate that cost growth and schedule delays can occur as a direct result of one or more of the following concerns:

- Immaturity of critical technologies at the start of development
- Inadequate understanding of design challenges at the start of development (often due to the absence of prototyping)
- Requirements uncertainty, instability, or creep
- Failure to acknowledge (or deal with) funding shortfalls
- Funding instability in the programming, budgeting or appropriations process
- Failure to detect (or deal with) unrealistic contractor cost proposals in competitive source selections (from either the prime or major subcontractors)
- Excessive concurrency between development and procurement schedules
- Inadequate understanding of software development size and integration challenges
- Failure to achieve design stability by the time of the critical design review
- Failure to achieve stable manufacturing processes by the time of early production

3.7.2.5. Document and Present Results

A complete cost estimate should be formally documented. The documentation serves as an audit trail of source data, methods, and results. The documentation should be easy to read, complete and well organized-to allow any reviewer to understand the estimate fully. The documentation also serves as a valuable reference for future cost analysts, as the program moves from one acquisition milestone to the next.

The documentation should address all aspects of the cost estimate: all ground rules and assumptions; the description of the system and its operating and support concepts; the selection of cost estimating methods; data sources; the actual estimate computations;

and the results of any sensitivity or risk analyses. The documentation for the ground rules and assumptions, and the system description, should be written as an updated (final) version of the Cost Analysis Requirements Description (CARD) or CARD-like document described earlier. The documentation for the portion of the cost estimate dealing with data, methods, and results often is published separately from the CARD or CARD-like document, but if that is the case, the two documents should be completely consistent.

3.7.3. Coordination

Managing the preparation of a life-cycle cost estimate requires continual coordination among all of the stakeholders. Normally, cost estimates are sponsored by a system program office and are prepared by a multi-disciplinary team with functional skills in financial management, logistics, engineering, and other talents. The team also should include participants or reviewers from major affected organizations, such as the system's operating command, product support center, maintenance depot, training center or command, and so forth. Typically, the analytic approach to the cost estimate is documented in a written study plan that includes a master schedule (of specific tasks, responsible parties, and due dates). For sufficiently complex efforts, the estimating team may be organized as a formal Integrated Product Team. Throughout the preparation of the estimate, coordination with all interested parties remains important. Frequent in-progress reviews or meetings are usually a good practice.

For independent cost estimates, the team may be smaller and less formal, but the basic principle-complete and continual coordination of the cost estimate with all interested parties-still applies.

3.7.4. Further Information and Training

3.7.4. Further Information and Training

The Acquisition Community Connection website has additional information on cost analysis.

In addition, the Defense Acquisition University offers the following courses in residence:

- BCF 106 -- Fundamentals of Cost Analysis
- BCF 107 -- Applied Cost Analysis
- BCF 204 -- Intermediate Cost Analysis
- BCF 206 -- Cost/Risk Analysis
- BCF 208 -- Software Cost Estimating
- BCF 215 -- Operating and Support Cost Analysis

As well as the following courses as on-line continuous learning modules:

- CLB 007 - - Cost Analysis

- CLM016 - - Cost Estimating
- CLB024 - - Cost Risk Analysis Introduction

In addition, each year the Cost Assessment Office sponsors a Department of Defense Cost Analysis Symposium. This symposium includes presentations from government and support contractor cost analysts concerning best practices and state-of-the-art in cost estimating. The Symposium also features senior distinguished speakers and panelists from government, industry, and academia. Further information may be found at the DoD Cost Analysis Symposium web site.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 4 -- Systems Engineering

4.0. Overview

4.0. Overview

4.0.1. Purpose

DAG Chapter 4 provides overarching guidance on the systems engineering (SE) discipline, its activities and processes, and its practice in defense acquisition programs. The Program Manager and the Systems Engineer should use DAG Chapter 4 to effectively plan and execute program activities across the system life cycle.

4.0.2. Contents

Section 4.1 Introduction defines Systems Engineering and why it is important.

Section 4.2 Systems Engineering Activities in the Life Cycle provides a by-phase description of key activities and the SE technical reviews and audits.

Section 4.3 Systems Engineering Processes provides a description of each process and contains the design considerations including specialty engineering.

4.1. Introduction

4.1. Introduction

Systems engineering (SE) establishes the technical framework for delivering materiel capabilities to the warfighter. SE provides the foundation upon which everything else is built and supports program success.

SE ensures the effective development and delivery of capability through the implementation of a balanced approach with respect to cost, schedule, performance, and risk using integrated, disciplined, and consistent SE activities and processes regardless of when a program enters the acquisition life cycle. SE also enables the development of engineered resilient systems that are trusted, assured, and easily modified (agile).

SE planning, as documented in the Systems Engineering Plan (SEP), identifies the most effective and efficient path to deliver a capability, from identifying user needs and concepts through delivery and sustainment. SE event-driven technical reviews and audits assess program maturity and determine the status of the technical risks associated with cost, schedule, and performance goals.

"Positive acquisition outcomes require the use of a knowledge-based approach to product development that demonstrates high levels of knowledge before significant commitments are made. In essence, knowledge supplants risk over time." (Source: GAO Report 12-400SP)

Additional SE benefits are it:

- Supports development of realistic and achievable program performance, schedule, and cost goals as documented in the Joint Capabilities Integration and Development System (JCIDS) documents, Acquisition Program Baseline (APB), Technology Development Strategy (TDS), and Acquisition Strategy (AS).
- Provides the end-to-end, integrated perspective of the technical activities and processes across the system life cycle, including how the system fits into a larger system of systems (SoS) construct.
- Emphasizes the use of integrated, consistent, and repeatable processes to reduce risk while maturing and managing the system baseline. The final product baseline forms the basis for production, sustainment, future changes, and upgrades.
- Provides insight into system life-cycle resource requirements and impacts on human health and the environment.

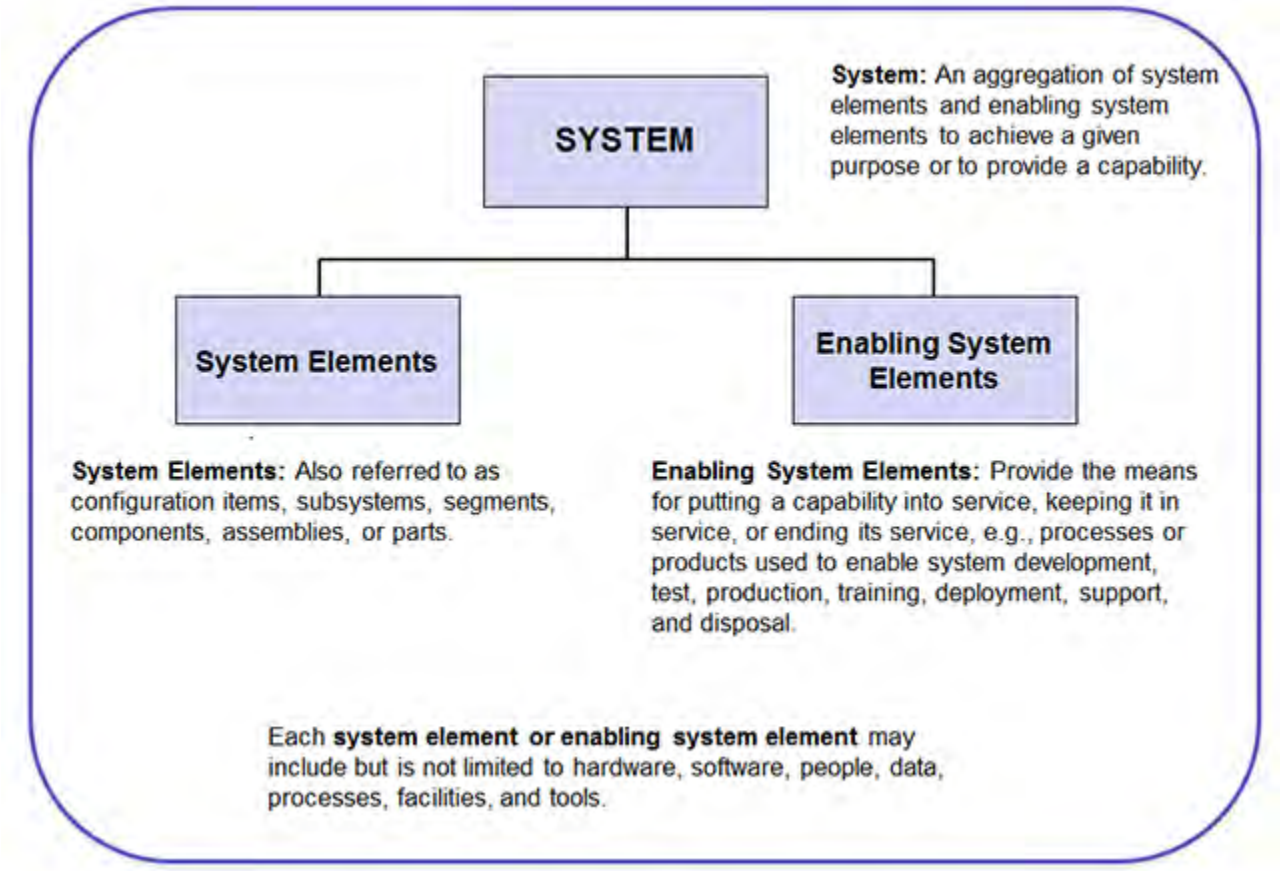
This chapter uses the following terms:

- The "Systems Engineer" refers to the Program Lead Systems Engineer, the Chief Engineer or Lead Engineer with SE responsibility, and the SE staff responsible for SE processes and who plan, conduct, and/or manage SE activities in the program.
- The "end user" includes the warfighter and other operational users, including support personnel, maintainers, and trainers who use or support the system.
- The "developer" refers to the system prime contractor (including associated subcontractors) or the Government agency responsible for designing and building the system.

Definition of Systems Engineering

Systems engineering (SE) is a methodical and disciplined approach for the specification, design, development, realization, technical management, operations, and retirement of a system. As illustrated in Figure 4.1.F1., a system is an aggregation of system elements and enabling system elements to achieve a given purpose or provide a needed capability. The enabling system elements provide the means for delivering a capability into service, keeping it in service, or ending its service and may include those processes or products necessary for developing, producing, testing, deploying, and sustaining the system.

Figure 4.1.F1. The System



SE applies critical thinking to the acquisition of a capability. It is a holistic, integrative discipline, whereby the contributions across engineering disciplines such as structural engineers, electrical engineers, mechanical designers, software engineers, human factors engineers, and reliability engineers are evaluated and balanced to produce a coherent capability - the system.

The Systems Engineer balances the conflicting design constraints of cost, schedule,

and performance while maintaining an acceptable level of risk. SE solves systems acquisition problems using a multi-disciplined approach. The Systems Engineer should possess the skills, instincts, and critical thinking ability to identify and focus efforts on the activities needed to enhance the overall system effectiveness, suitability, survivability and sustainability.

SE activities begin before a program is officially established and are applied throughout the acquisition life cycle. Any effective SE approach should support and be integrated with sound program management. Prior to program initiation, the Program Manager, or Service lead if no Program Manager has been assigned, should perform development planning to lay the technical foundation for successful acquisition. Development planning encompasses the engineering analyses and technical planning activities that provide the foundation for informed investment decisions on which path a materiel development decision takes. Development planning effectively addresses the capability gap(s), desired operational attributes, and associated dependencies of the desired capability. In addition, development planning ensures that there exists a range of technically feasible solutions generated from across the entire solution space and that consideration has been given to near-term opportunities to provide a more rapid interim response to the capability need. Development planning is initiated prior to the Materiel Development Decision review, continues throughout the Materiel Solution Analysis phase, and transitions the knowledge (documents, tools, and related data) to the designated program.

Affordability

The Systems Engineer contributes to defining, establishing, and achieving affordability targets throughout the life cycle of the system. Affordability targets are based on what the Department can afford to spend for the capability, including program acquisition and sustainment costs. Affordability targets are used as design constraints in the development, procurement, and sustainment of an affordable system. See DAG section 4.3.18.2. Affordability - Systems Engineering Trade-Off Analyses, for more information on how affordability drives design decisions.

The Program Manager controls requirements growth and should use affordability goals early to guide design trades and program decisions. The Systems Engineer assists in managing affordability by working closely with the program cost estimator/analyst team when developing common cost and technical models and aligning baselines. See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates for more information on affordability.

Throughout the acquisition life cycle, the Program Manager and Systems Engineer should monitor the system affordability, seek out cost saving opportunities, and identify any associated cost, schedule, and performance risks. The Program Manager's emphasis prior to Milestone B should be on defining and achieving affordability targets and desired capabilities. During the Technology Development (TD) phase, the Program Manager and Systems Engineer work to reduce technical risk and develop a sufficient

understanding of the materiel solution development to validate design approaches and cost estimates, to refine requirements and to ensure affordability is designed in to the desired capability. After Milestone B, the emphasis shifts to defining and achieving should cost estimates.

Should cost management is a deliberate strategy to drive cost efficiencies and productivity growth into programs. The will cost estimate is the likely life-cycle cost of the system based on historical data and represents the program's independent cost estimate, i.e., as generated by the Cost Assessment and Program Evaluation (CAPE) office or Service equivalent. As the program identifies inefficiencies, the should cost estimate is developed based on specific actions and opportunities to mitigate, eliminate, or reduce those inefficiencies that allow the program to come in below the expected will cost estimates. The Program Manager, with support from the Systems Engineer, develops program office cost estimates reflecting should cost opportunities and plans. The Program Manager uses the should cost estimate as a tool to:

- Influence design trades and choices when analyzing and setting contract/production execution targets
- Manage all costs throughout the product's life cycle
- Manage the product's final unit and sustainment cost
- Provide incentives for both of the parties (Government and industry) to execute efficiently: Government managers, who seek more value for the warfighter and taxpayer; and industry managers, who develop, build and sustain the systems and provide needed services

Should cost focuses on controlling the cost of both current and planned work. To have an impact, these activities should inform contract negotiations leading up to Engineering and Manufacturing Development (EMD) and Production and Deployment (P&D) phases. Should cost management does not mean trading away the long-term value of sound design practices and disciplined SE activities for short-term gain; it does mean eliminating non-value-added activities and reports that are not required and that are deemed unessential. For guidance on implementing should cost management, see the Better Buying Power website.

Program Managers address affordability requirements and begin to apply should cost management early in the acquisition life cycle. This includes applying SE to define an affordable system design while also working to eliminate inefficiencies and duplication where applicable and to drive productivity improvements into their programs.

Systems Engineering Processes

The practice of systems engineering (SE) is composed of 16 processes: eight technical processes and eight technical management processes as listed in Figure 4.1.F2. and described in DAG section 4.3. Systems Engineering Processes. These 16 processes provide a structured approach to increasing the technical maturity of a system and increasing the likelihood that the capability being developed balances mission

performance with cost, schedule, risk, and design constraints.

The eight technical management processes are implemented across the acquisition life cycle and provide insight and control to assist the Program Manager and Systems Engineer to meet performance, schedule, and cost goals. The eight technical processes closely align with the acquisition life-cycle phases and include the top-down design processes and bottom-up realization processes that support transformation of operational needs into operational capabilities.

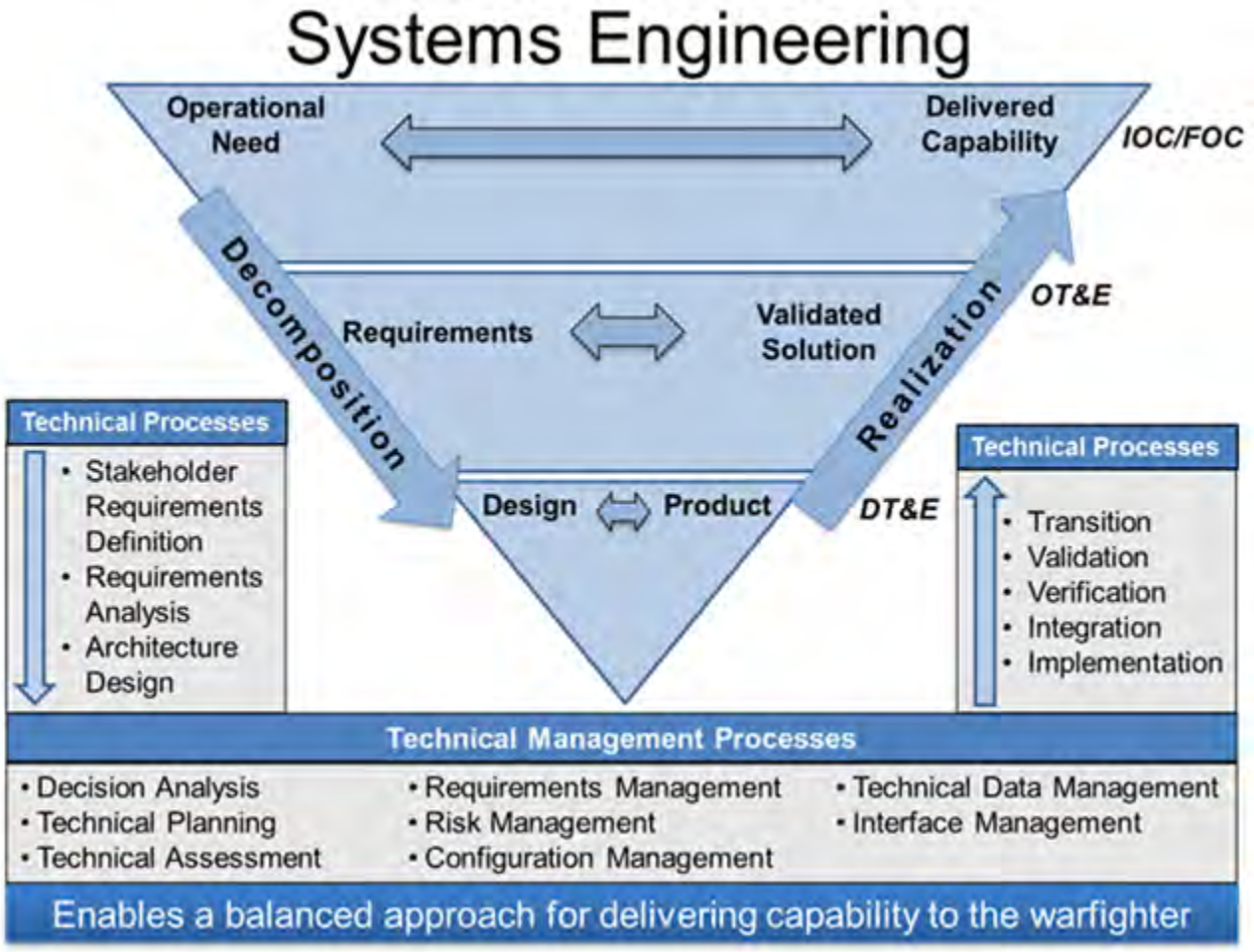
The ultimate purpose of the SE processes is to provide a framework that allows the SE team to efficiently and effectively deliver a capability to satisfy a validated operational need. To fulfill that purpose, a program implements the SE technical processes in an integrated and overlapping manner to support the iterative maturation of the system solution. The level of SE required supporting these processes declines as a program progresses into the later phases of the acquisition life cycle. Implementation of the SE processes begins with the identification of a validated operational need as shown in the top left corner of the V-diagram (see Figure 4.1.F2). The technical processes enable the SE team to ensure that the delivered capability accurately reflects the operational needs of the stakeholders. The key activities that are accomplished by the execution of the technical processes are described below:

- During the Stakeholder Requirements Definition process, the operational requirements and inputs from relevant stakeholders are translated into a set of top level technical requirements. These requirements are decomposed and elaborated during the Requirements Analysis process to produce a complete set of system functional and performance requirements. (**Note:** Figure 4.1.F2 is provided as a framework to illustrate where requirements are addressed within the SE Process flow. See DAG section 4.3.11. Requirements Analysis Process for more information on operational and system requirements.)
- During the Architecture Design process, the Systems Engineer, often through system modeling, trade-offs, and decision analyses, captures the functional requirements and interdependencies in the system architecture. Trade-offs and analyses are also used to mature and realize the design of the system and system elements during the Implementation process, generating the product baseline.
- During the Integration process, the program assembles the system elements together to provide the system for testing in the Verification process (developmental tests verifying the functional requirements) and Validation process (operational tests validating the system meets the operational need), resulting in a validated solution.
- During the Transition process, the program formally delivers the system capability to the end users, including all enabling system elements to support operational use and sustainment activities.

The technical management processes, listed at the bottom of Figure 4.1.F2, provide a

consistent approach to managing the program's technical activities and controlling information and events that are critical to the success of the program. Taken together, these 16 processes are a systematic approach focused on providing operational capability to the warfighter while reducing technical and programmatic risk.

Figure 4.1.F2. Systems Engineering Processes



All organizations performing SE should scale their application and use of the processes in DAG section 4.3. Systems Engineering Processes to reflect the unique needs of the program and the type of product or system being developed. This scaling should reflect the system's maturity and complexity, size and scope, life-cycle phase, and other relevant considerations. For example, lower-risk, less-complex programs may scale the processes to ensure key activities are effective but not overly cumbersome (e.g., simpler and less-expensive tools, less-frequent reporting, and activities adjusted to fit smaller organizations with fewer personnel).

4.1.1. Systems Engineering Policy and Guidance

4.1.1. Systems Engineering Policy and Guidance

Policy and guidance related to systems engineering (SE) are intended to minimize the burden and cost on programs while maintaining technical integrity through the planning and execution of SE activities across the acquisition life cycle. Program Managers and Systems Engineers should know and understand the statutory and regulatory SE mandates. Table 4.1.1.T1 identifies top-level SE-related policy and guidance.

Table 4.1.1.T1. Systems Engineering-Related Policy and Guidance

SE Policy and Guidance
DoDD 5000.01, The Defense Acquisition System
DoDI 5000.02, Operation of the Defense Acquisition System
DoDI 5134.16, Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))
PDUSD(AT&L) Memorandum, "Improving Milestone Process Effectiveness"
PDUSD(AT&L) Memorandum, "Expected Business Practice: Post-Critical Design Review Reports and Assessments"
PDUSD(AT&L) Memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan"
PDUSD(AT&L) Memorandum, "Document Streamlining - Program Protection Plan (PPP)"
PDUSD(AT&L) Memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)"
USD(AT&L) Memorandum, "Implementation of Will-Cost and Should-Cost Management"
USD(AT&L) Memorandum, "Better Buying Power: Mandate for Restoring Affordability and Productivity in Defense Spending"
Additional SE-related guidance is provided on the Deputy Assistant Secretary of Defense for Systems Engineering (DASD (SE)) website

SE-related policy, guidance, specifications, and standards are intended to successfully guide the technical planning and execution of a program across the acquisition life cycle. Understanding the use and value of SE specifications and standards is fundamental to establishing, executing, and maintaining disciplined SE processes. The ASSIST document database is the official source for current DoD specifications and standards.

Compliance with mandated DoD SE policy is required for program approval and completion of successful milestone decisions. DoD policy and guidance provide a framework for structuring the program and help define the areas available for tailoring to effectively and efficiently deliver capability to the warfighter.

Within this policy and guidance framework, tailoring the acquisition effort to meet program cost, schedule, and performance goals is not only desired but mandated in accordance with DoDD 5000.01. In July 2012, USD(AT&L) emphasized there is no one-size-fits-all optimal program structure. Every program has its own optimal structure, and

that structure is dependent on many variables that contribute to program success or failure. Areas that should be considered for tailoring include:

- The documentation of program information
- The execution of the acquisition phases
- The timing and scope of decision review
- The decision levels chosen to fit the particular conditions of the program in accordance with applicable laws and regulations
- The time-sensitivity of the capability need

The requirements of DoD SE policy that are identified for tailoring by the Program Manager are submitted to the Milestone Decision Authority (MDA) for approval.

The structuring of every program should start with a deep understanding of the nature of the capability intended to be acquired and the effort needed to realize that capability. Critical thinking during early program formulation is important to clearly identify the internal and external stakeholders, system interdependencies, technological opportunities, contractual and budgetary constraints, and policy mandates. The optimal program structure includes the set of technical activities, events, and management mechanisms that best address the unique circumstances and risks of the program.

All program strategy and planning documents depend on SE activities to define and balance requirements against cost, schedule, and risks; identify potential solutions; assess the maturity and feasibility of available technologies; develop a realistic schedule; and allow for multiple other considerations affecting the final cost and delivery of capability to the warfighter. Therefore, the Program Manager should build a program office structure that ensures the Systems Engineer is an integrated part of the program planning and execution activities.

The Systems Engineer leads or is a key enabler in the planning and execution of the program's technical approach. To aid this planning, the Systems Engineer should proactively seek experience from similar past and current programs and map this learning as applicable into the SE planning of the program (see also DAG section 4.3.19.4. Lessons Learned, Best Practices, Case Studies).

4.1.2. Systems Engineering Plan

4.1.2. Systems Engineering Plan

The purpose of the Systems Engineering Plan (SEP) is to help Program Managers develop, communicate, and manage the overall systems engineering (SE) approach that guides all technical activities of the program. The SEP documents key technical risks, processes, resources, metrics, SE products, and completed and scheduled SE activities. The SEP is a living document that should be updated as needed to reflect the program’s evolving SE approach and/or plans and current status. The PDUSD(AT&L) memorandum, "Program Strategies and Systems Engineering Plan" requires programs

to use the SEP Outline to guide SEP preparation. The SEP Outline identifies the minimum expected content to be addressed in the SEP. The SEP should be consistent with and complementary to the Acquisition Program Baseline (APB), Technology Development Strategy (TDS), Acquisition Strategy (AS), Test and Evaluation Strategy (TES), Test and Evaluation Master Plan (TEMP), Program Protection Plan (PPP), Life-Cycle Sustainment Plan (LCSP), and other program plans as appropriate. The SEP should be written in a common language to clearly communicate what the program plans to do in each phase of the acquisition life cycle and should be written to avoid redundancy and maintain consistency with other planning documents.

For Major Defense Acquisition Programs (MDAPs), the Program Manager should formally charter a SE Working-Level Integrated Product Team (WIPT), led by the Systems Engineer, to assist in developing and monitoring SE activities as documented in the program SEP. DoDI 5000.02, Public Law 111-23 (Weapon Systems Acquisition Reform Act), and DoDI 5134.16 require a formal SEP to be approved by the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) for all Acquisition Category level 1 (ACAT I) and potential ACAT I programs prior to Milestones A, B, and C and program restructures. The PDUSD(AT&L) memo on "Improving Milestone Process Effectiveness" requires that a draft formal SEP be available for the pre-Engineering and Manufacturing Development (pre-EMD) review. For all lower ACAT programs, the Component Acquisition Executive or delegated authority approves the SEP. As a best practice, SEP updates should be approved by the Program Executive Office (PEO) prior to each technical review and when the program changes in a way that has an impact on the technical strategy. The Program Manager may approve other periodic updates to the SEP.

The SEP describes the integration of SE activities with other program management and control efforts, including the Integrated Master Plan (IMP), Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), Risk Management Plan (RMP), Technical Performance Measures (TPMs), and other documentation fundamental to successful program execution. The SEP also describes the program's technical requirements, engineering resources and management, and technical activities and products as well as the planning, timing, conduct, and success criteria of event-driven SE technical reviews throughout the acquisition life cycle. As a best practice, the Government SEP should accompany the Request for Proposal (RFP) as guidance to the offerors. The developer's Systems Engineering Management Plan (SEMP), which is the contractor-developed plan for the conduct, management, and control of the integrated engineering effort, should be consistent with the Government SEP to ensure that Government and contractor technical plans are aligned. The SEMP should define the contractor technical planning and how it is accomplished from the contractor perspective, and articulates details of their processes, tools, and organization.

As the program's blueprint for the conduct, management, and control of all technical activities, the SEP captures decisions made during the technical planning process and communicates objectives and guidance to program personnel and other stakeholders. The SEP should define the "who, what, when, why, and how" of the SE approach, for

example:

- The program organization with roles and responsibilities, authority, accountability, and staffing resources. This includes the coordination of the program's integrated product teams (IPTs) and their products, resources, staffing, management metrics, and integration mechanisms.
- The key activities, resources, tools, and events that support execution of the SE technical processes and technical management processes (see DAG section 4.3. Systems Engineering Processes) to deliver a balanced solution to meet the warfighter's needs. It should identify unique processes, tools, and/or tailoring of organizational and Government standards, how these processes and tools are integrated, and how products are developed and managed.
- The event-driven technical review approach based on successful completion of key activities as opposed to calendar-based deadlines. The SEP should identify the timing of SE events in relation to other program events and key knowledge points, and it should describe how technical activities are integrated in the program's overall plan and schedule. The SEP should include the assumptions made in developing the schedule and the process for conducting schedule risk assessments and updates.
- The approach for how requirements and technical performance trade-offs are balanced within the larger program scope to deliver operationally effective, suitable, and affordable systems. Key design considerations and criteria (see DAG section 4.3.18. Design Considerations) should be listed in the mandatory table as applicable, with the associated plans embedded in the SEP or hot linked so that responsible staff can monitor system compliance.
- The SE tools and other enablers integrated and used to support SE processes, technical design initiatives, and activities.

4.1.3. Systems Level Considerations

4.1.3. Systems Level Considerations

A system should not be acquired in isolation from other systems with which it associates in the operational environment. The Program Manager and Systems Engineer should understand how their system fills the needs for which it was designed and the enterprise context within which it operates. This includes understanding the diverse or dissimilar mix of other systems (hardware, software, and human) with which the system needs to exchange information. To that end, the Program Manager and Systems Engineer should define intersystem interfaces using a systems engineering (SE) document, i.e., the interface control document(s). In addition to interface control documents, the Program Manager and Systems Engineer, should also actively pursue Memoranda of Agreement or Memoranda of Understanding (MOA/MOU) with companion programs regarding interfaces, data exchanges, and advance notices of changes interdependencies and schedule (timing) that may affect either program. These agreements are a professional courtesy and a means of mitigating the inherent risk in planning to deliver a capability to an anticipated future technical baseline when there is

uncertainty that the other programs are able to maintain schedule and have adequate resources to deploy the capabilities as planned.

SE is increasingly recognized as key to addressing the evolution of complex systems of systems. SE principles and tools can be used to apply systems thinking and engineering to the enterprise levels. An enterprise in this usage is understood to be the organization or cross-organizational entity supporting a defined business scope and mission, and includes the interdependent resources (people, organizations, and technology) to coordinate functions and share information in support of a common mission or set of related missions, (reference "Federal Enterprise Architecture Framework (FEAF)," September 1999).

This application of SE to address enterprises as complex systems builds on traditional SE activities and expands them to address enterprise challenges. The Systems Engineer can also assist with enterprise strategic planning and enterprise investment analysis. These two additional roles for Systems Engineers at the enterprise level are "shared with the organization's senior line management, and tend to be more entrepreneurial, business-driven, and economic in nature in comparison to the more technical nature of classical systems engineering," (reference Charlock, P.G., and R.E. Fenton, "System-of-Systems (SoS) Enterprise Systems for Information-Intensive Organizations," Systems Engineering, Vol. 4, No. 4 (2001), pages 242-261).

Each DoD Service and Agency, and the Department itself, are examples of enterprises as systems. Such organizations have the challenge of integrating and evolving multiple portfolios of systems often with conflicting sets of objectives, constraints, stakeholders, and demands for resources.

The Systems Engineer should be cognizant of the enterprise context and constraints for the system in development and should factor these enterprise considerations into acquisition technical decisions from the outset. Mission areas, for example, can be viewed as cross-organizational enterprises and also provide critical context for system acquisition. Controlled interfaces with enabling systems in the SoS architecture drive system design. In some cases, enterprise considerations have been articulated as standards and certification requirements. In other cases, system decisions need to be made in the context of the larger Service portfolio of systems and mission area needs.

Most DoD capabilities today are provided by an aggregation of systems often referred to as systems of systems (SoS). A SoS is described as a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. For complex SoS, the interdependencies that exist or are developed between and/or among the individual systems being integrated are significantly important and need to be tracked. Each SoS may consist of varying technologies that matured decades apart, designed for different purposes but now used to meet new objectives that may not have been defined at the time the systems were fielded.

Both individual systems and SoS conform to the accepted definition of a system in that each consists of parts, relationships, and a whole that is greater than the sum of its parts; however, not all systems are SoS. There are distinct differences between systems and SoS that should be taken into account in the application of SE to SoS (see Table 4.1.3.T1, adapted from DoD Systems Engineering Guide for Systems of Systems, page 11).

Table 4.1.3.T1. Comparing Systems and Systems of Systems

	System	System of Systems (SoS)
Management & Oversight		
Stakeholder Involvement	Clearer set of stakeholders	Two levels of stakeholders with mixed, possibly competing interests. The two levels of stakeholders represent: 1. the independent and useful systems 2. the aggregation of the independent and useful systems
Governance	Aligned PM and funding. Higher levels of governance such as PEO and AT&L (internal and external governance)	Added levels of complexity due to management and funding for both SoS and systems; No single manager controls all constituent systems in the SoS
Operational Environment		
Operational Focus	Designed and developed to meet operational objectives	Called upon to provide integrated capabilities using systems whose objectives have not been directly derived from current SoS system's objectives
Implementation		
Acquisition	Aligned to established acquisition process	Multiple system life cycles across acquisition programs, involving legacy systems, systems under development, new developments, and technology insertion; Stated capability objectives but may not have formal requirements
Test & Evaluation	Test and evaluation of the system is possible	Testing more challenging due to system's asynchronous life cycles and given the complexity of all the moving parts
Engineering & Design Considerations		
Boundaries & Interfaces	Focuses on boundaries and interfaces	Focus on identifying systems contributing to SoS objectives and enabling flow of data, control, and functionality across and/or between the SoS while balancing needs of systems. The boundaries and interfaces between systems become very important, since they serve as a conduit for data transfer
Performance & Behavior	Ability of the system to meet performance objectives	Performance across the SoS that satisfies SoS user capability needs while balancing needs of the systems

Application of Systems Engineering to Systems of Systems

Systems of systems (SoS) systems engineering (SE) deals with planning, analyzing, organizing, and integrating the capabilities of new and existing systems into a SoS capability greater than the sum of the capabilities of its constituent parts. Consistent with the DoD transformation vision and enabling net-centric operations, SoS may deliver capabilities by combining multiple collaborative and independent-yet-interacting systems. The mix of systems may include existing, partially developed, and yet-to-be-designed independent systems.

The DoD Guide to Systems Engineering for Systems of Systems addresses the application of SE to SoS. The guide defines four types of SoS (see Table 4.1.3.T2). When a SoS is recognized as a "directed," "acknowledged," or "collaborative" SoS, SE is applied across the constituent systems and is tailored to the characteristics and context of the SoS. Due to increased efforts to network systems to facilitate information sharing across the battlespace, most DoD systems also may be viewed as components of a "virtual" SoS. For virtual SoS, DoD net-centric policies and strategies, such as, Department of Defense Net-Centric Services Strategy provide SE guidance regarding SoS contexts where there is an absence of explicit shared objectives or central management.

Table 4.1.3.T2. Four Types of Systems of Systems

Type	Definition
Directed	Directed SoS are those in which the SoS is engineered and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the centrally managed purpose.
Acknowledged	Acknowledged SoS have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, development, and sustainment approaches. Changes in the systems are based on cooperative agreements between the SoS and the system.
Collaborative	In collaborative SoS, the component systems interact more or less voluntarily to fulfill agreed-upon central purposes.
Virtual	Virtual SoS lacks a central management authority and a centrally agreed-upon purpose for the system of systems. Large-scale behavior emerges-and may be desirable-but this type of SoS relies upon relatively invisible, self-organizing mechanisms to maintain it.

4.1.3.1. Software

4.1.3.1. Software

Software is a key enabler for almost every system, making possible the achievement and sustainment of advanced warfighting capabilities. Development and sustainment of software is frequently the major portion of the total system life-cycle cost, and factors such as safety, security, reliability, interoperability, and insertion of new technology are considered at every decision point in the acquisition life cycle.

Software engineering requires unique technical management and contracting expertise to address architectures, requirements mapping, integration, technical data rights, assurance, and suitability for intended use. The more critical or complex the software acquisition effort, the more important it is to seek developers with demonstrated experience and knowledge (for more information on the uses of external resources see DAG section 4.1.4. Engineering Resources). The Program Manager should understand software development principles and best practices. To support program protection, program planning, contracting, configuration management, integration, test, and sustainment, the Program Manager should also have a working knowledge of software terms, tools, development models, risks, and challenges. These elements are major cost drivers for software in complex systems. Because key system capabilities are now more frequently implemented in software, techniques that estimate and assess function size, cost, performance, and risk are required for program planning, contract development, and progress assessment. Systems engineering (SE) principles and practices help anticipate, plan for, and mitigate challenges and risks in software development and system integration.

Establish the software acquisition strategy as early as possible to address function and component allocation to software and determine what is to be developed, what is provided as Government off-the-shelf (GOTS) software, commercial-off-the-shelf (COTS) software, or open source software (OSS), and what is a mix or hybrid. The strategy also incorporates plans for associated data and intellectual property rights for GOTS, COTS, and OSS.

Software-intensive acquisitions typically involve modeling and simulation (M&S) in engineering support roles specific to each phase of acquisition. Example uses of M&S in software acquisition are to:

- Study development cost by function,
- Study feasibility of the prospective system in the intended operational environment,
- Conduct engineering trade-offs and analyses of alternatives,
- Study and refine viability of planned software and computers to meet KPPs,
- Simulate undeveloped equipment during software testing, and
- Emulate the interoperability environment of the system during integration.

M&S activities are most valuable earlier in program planning as decision support tools and may be used iteratively to assess evolving functional architectures. The cost of M&S is allocated during initial program planning. Cost basis is the rationale supporting the balance between M&S cost and degree of needed risk reduction. M&S used by a Program Manager to make decisions should be verified and validated to the intended use in a time frame before assessment is needed. Data used by M&S to support assessments should have a known pedigree and should be adequate to the level of assessment. See DAG section 4.3.19.1. Modeling and Simulation for more information.

An incremental software development approach enables the developers to deliver capability in a series of manageable releases or builds to gain user acceptance and feedback for the next increment and reduce the overall level of risk. Frequent requirements and design-validation activities involving the end users and developers can assist the program to define viable increments of capabilities that have operational value for early fielding before the whole system capability is delivered. This incremental approach may not be viable when the end system is not usable until the entire set of essential capabilities is integrated and tested. For example, weapon systems are dependent upon software for real-time controls that can affect life and safety. As such, these weapon systems are required to be qualified and certified for security, safety, and interoperability before being released for operational use. In addition, safety and security assurance certifications and approvals require a predetermined objective level of rigor in verification, validation, and accreditation (VV&A) of these software releases. This VV&A is based on risk, not on the complexity, number of software lines of code (SLOC), or size of each software release. The Joint Software Systems Safety Handbook provides guidance for implementing safety-critical software designs with the reasonable assurance that the software executes within the system context and is at an acceptable level of safety risk.

Iterative development approaches should be planned well in advance and should consider impacts to other system elements of the functional architecture or other interconnecting systems. The program should focus on the allocation of functional architecture elements to the physical architecture and identifying the interdependencies and associated technical risks as part of determining the content for each iteration or build. Incremental or iterative development should be employed to carefully define the final end state of the supporting physical hardware elements when functionality or capability is to be added over time. Memory, processor overhead, and input/output capacity should be designed to support growth in capability. Implementing an open systems architecture (OSA) as part of the software design and development increases design flexibility, supports incremental deliveries, allows for opportunities to use COTS and OSS, facilitates future upgrades and modifications, and supports technology insertion (see DAG sections 4.3.18.4. Commercial-Off-the-Shelf and 4.3.18.15. Open Systems Architecture).

Software SE uses architectural modeling to develop and refine software requirements and to partition a system's software into components and subcomponents. Software architectural decisions are driven by principles including co-location of external

interfaces in one component to reduce risk of vulnerability, aggregating functions having higher mutual interaction, determining components that have well-defined interfaces to other components as candidates for technology insertion or OSS in support of OSA, and allocation of functionality to maximize use of COTS given acceptable risk.

When employing COTS software, criteria for selecting among competitive alternatives may not include details of commercial design or performance but should require ample evidence that the software is adequate for its intended use. Code-scanning tools should be used to help ensure that COTS software does not pose a security or software assurance risk. (See DAG Chapter 7 Acquiring Information Technology, Including National Security Systems and NIST-SP-800 series publications for additional information.) In addition, mitigation of security and information assurance risks associated with COTS software go beyond code-scanning techniques for their solution. Those risk mitigation efforts should be expanded to make use of activities identified in DAG section 4.3.18.24. System Security Engineering, as well as the activities discussed in DAG Chapter 13 Program Protection.

In programs for which software capability is procured as a service, the service-level agreement(s) (SLA) should reflect operational or field performance including all path constraints, such as satellite time delays, low data rate access, and intermittent service, as part of the operational environmental constraints and potential security requirements. These SLA provisions are important because service providers may not be willing to disclose details of their operations and staffing (such as overseas data centers or help desks).

It is not uncommon for weapon system acquisitions to contain a mix of Government-off-the-shelf (GOTS) software with complete technical data and software rights, other software items with restricted Government purpose rights, and software with virtually no rights other than the commercial license to use or access the software (see FAR Subpart 27.4). The Systems Engineer and Program Manager should be aware of the implications of these differences regarding acquisition and sustainment costs, performance, and the consequences on change control and sustainment of deployed systems. For deployed systems, the Systems Engineer should understand the system concept of operations (CONOPS), any maintenance plans, the targeted audience that is expected to use the software application, and level of training of the potential users. This understanding is necessary in order to effectively balance the cost, scheduling and potential risks in maintenance, training, and documentation.

As a best practice, the Systems Engineer for a software-intensive system, defined as "a system in which software represents the largest segment in one or more of the following criteria: system development cost, system development risk, system functionality, or development time" (DAU Glossary of Acronyms and Terms), should be well versed in the technical and management activities of computer programming, software project planning, and software configuration management, including defining computer software configuration items. The SE approach should include software engineers early in the acquisition life cycle to ensure software considerations are included in defining and

allocating software-related requirements and generating cost and schedule estimates, especially for software-intensive systems. Software engineers are also needed to evaluate the developer's software architecture, functional baseline, allocated baseline, and product baseline, documents, plans, and estimates, including M&S capabilities and facilities. Program-independent software engineers should support validation activities.

SE processes should be adapted to address considerations of hardware, software, and human systems integration. For example, risk management activities for hardware, software, and human systems integration should be combined so that risk mitigation plans can address all hardware, software, and human systems integration aspects of individual risks.

For software-related acquisitions the Systems Engineering Plan (SEP) should consider the following, as a minimum, for software SE planning:

- Software-unique risks
- Inclusion of software in technical reviews, with the addition of the Software Specification Review (SSR) as a precursor to the Preliminary Design Review (PDR) for software-intensive systems
- Software organization, integrated product teams, and relationships to interdependent organizations
- Software technical performance, process, progress, and quality metrics (see DAG section 4.3.4. Technical Assessment Process)
- Software safety, security, protection, and similar requirements, including processes, architecture, and interfacing systems
- Configuration management, verification, and validation of software integration labs/facilities used as tools for software development
- Open systems architecture, associated data rights, and sustainment considerations
- Automated test plans, development tools, and pedigreed data to support modeling of requirements, design, and environmental interfaces
- Software problem reporting and assessment, code development, build generation, and regression testing
- Software independent verification and validation (IV&V) to be accomplished, especially as it relates to contractor proprietary software
- Versioning, data control, and testing, especially for GOTS
- Verification of documentation, configuration management, test relevancy, and other considerations for legacy versus new software

Each of the Services provides additional guidance to assist the Program Manager, Systems Engineer, and Software Engineers on software-intensive systems:

- The Department of the Navy published a Guidebook for Acquisition of Naval Software-Intensive Systems.
- The Department of the Air Force has published the Weapon Systems Software Management Guidebook.

- The Department of the Army provides software metrics recommendations within DA-PAM-70-3, Army Acquisition Procedures and DA-PAM-73-1, Test and Evaluation in Support of Systems Acquisition.

Software Integrated within the Acquisition Life Cycle

Software considerations occur and vary throughout the acquisition life cycle, with specific activities associated with each acquisition phase described in Table 4.1.3.1.T1.

Table 4.1.3.1.T1. Acquisition Phase-Specific Software Considerations

Phase	Software Considerations
Materiel Solution Analysis	Some system requirements map directly to software requirements, while others can be implemented in hardware or firmware, providing opportunities for trade-offs and studies that optimize design and reduce vulnerabilities and risks. The ability to analyze and model options, and articulate the pros and cons of each, can have long-range impacts on the delivered system, suitability for intended use, and ultimate life-cycle cost.
Technology Development	Competitive prototyping of software-intensive systems helps to identify and mitigate technical risks. System prototypes may be physical or math models and simulations that emulate expected performance. High-risk concepts may require scaled models to reduce uncertainty too difficult to resolve purely by mathematical emulation. On occasion, competitive full-scale prototypes are needed to resolve cost/benefit alternatives between competing software-intensive system designs. Software programs typically conduct a Software Specification Review (SSR) to assess the software requirements and interface specifications for computer software configuration items, in support of the Preliminary Design Review (PDR). The software trouble reporting system is in operation and may be used to track any remediation in design and software code and unit testing.
Engineering and Manufacturing Development	To demonstrate that the detailed software design is complete at Critical Design Review (CDR), software documentation should represent the design, performance, and test requirements, along with the development and software/systems integration facilities to be employed in coding and integrating the deliverable software. Software and systems used for computer software configuration item development such as simulations and emulations, should be validated, verified, and ready to begin coding upon completion of the CDR, starting the implementation and synthesis of the software products. Software trouble reporting is used extensively to track problems and problem criticality levels. Problem report metadata should be selected so that the reports are relevant in development, test, and in operation to tracking and assessments. Typically, software functions vary in mission criticality so that problems reported in those functions are more critical to the system. There is legacy problem report tracking information that can be used to generally profile and predict which types of software functions may accrue what levels of problem reports. Program progress decisions can be made based on assessments of patterns of problem reports among software components of the system.
Production and Deployment	Software may be refined as needed in response to operational test and evaluation activities and in support of the Full-Rate Production and/or Full Deployment Decision and Initial Operational Capability.

Phase	Software Considerations
Operations and Support	The In-Service Review (ISR) assesses user acceptance and potential upgrades on delivered software systems. A block change or follow-on incremental development may be defined that delivers maintenance, safety, or urgent builds and upgrades to the field in a controlled manner. Procedures for updating and maintaining software on fielded systems can require operators to download new builds or to install them from physical media, and may require more training. Procedures should be in place to support effective configuration management and control. There are inherent risks involved in modifying software on fielded systems upon which warfighters depend while engaged in frontline activities. Another aspect of the hardware-software interaction is that maliciously altered devices or inserted software can infect the supply chain, creating unexpected changes to systems. Vigilance is needed as part of supply chain risk management (see DAG Chapter 5 Life-Cycle Logistics and Chapter 13 Program Protection). Upon completion of development, the problem report tracking system can be used with other factors as legacy information to inform system and component upgrades. During Operations and Support phase, software problem reporting is continued.

Factors for Managing Software-Intensive Systems

Programs consider several factors when managing software-intensive systems, including the following:

Software Development Plan (SDP): The SDP as a best practice provides details below the level of the Systems Engineering Plan (SEP) and the contractor's Systems Engineering Management Plan (SEMP) for managing software development and integration. The SDP Data Item Description (DID) DI-IPSC-81427A is a tailorable template and a useful starting point in defining a software development plan. The SDP provides the Systems Engineer with insight into, and a tool for monitoring, the processes being followed by the developer for each activity, the project schedules, the developer's software organization, and resource allocations.

Post-Deployment Software Support (PDSS): The management of the software development process and the implementation of a process that ensures software supportability are among two of the most difficult challenges facing the Program Manager in management of software-intensive systems. The Program Manager should effectively address the issues of software supportability, the software test environment, and other equipment, material, and documentation, including data rights that are required to provide PDSS for those end users identified in the SDP or in other documents similar to the Computer Resources Life Cycle Management Plan. (For more information on PDSS see MIL-HDBK-347.) Successful PDSS planning should assist the Program Manager in controlling software life-cycle costs.

Data Protection and Software Assurance: These factors are defined as the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software code,

throughout the acquisition life cycle. The Program Manager is responsible for protecting system data and software, whether the data are stored and managed by the program office or by the developer (see DAG Chapter 13 Program Protection).

Software Data Management and Technical Data Rights: Rights associated with commercial products can be highly restrictive and are defined in licenses that may restrict the number of copies made and ability to alter the product. Often there is no assurance of suitability for intended purposes and no recourse to the vendor. Open source, sometimes referred to as "freeware," may not be free and may also have restrictions or carry embedded modules that are more restrictive than the overall package. The Program Manager, Systems Engineer, software engineer, and contracting officer should be familiar with the restrictions placed on each software item used in the contract or deliverable to the Government. The Program Office should determine the necessary intellectual property rights to computer software and should ensure that the intellectual property right should be determined in advance of the RFP and contract award and that they are acquired as needed, including:

- All requirements tools and data sets;
- All test software and supporting information necessary to build and execute the tests;
- All other software test tools such as interface simulators and test data analyzers whether custom-developed or not; and
- All information for defects remaining in the software upon delivery to the Government.

Software Reuse: The reuse of any system, hardware, firmware, or software should be addressed in multiple plans and processes throughout the acquisition life cycle, including the SEP, SDP, firmware development plan, configuration management plan, test plans (Test and Evaluation Master Plan, Software Test Plan, Independent Verification and Validation Plan), and quality assurance plans (system and software). (**Note:** Software reuse has traditionally been overestimated in the beginning of programs, and software reuse has often proven to be more costly than new software development. Software reuse plans should be monitored as a potential risk.) For more discussion of the reuse of software, see DAG section 4.3.18.15. Open Systems Architecture.

Software Acquisition and Sustainment Costs: Related costs should be accurately estimated in advance and then tracked to monitor execution within program cost constraints using relevant metrics (size, complexity, productivity factors, quality, development organization’s past performance/productivity, etc.).

Government and Industry Teaming: Teaming is needed in order for the Government to successfully acquire software-reliant systems with industry as a partner. As a result of the teaming agreement, the Government may be able to use the experience and expertise of its industry partner. Extensive teaming with industry makes it incumbent on the Government to ensure that it maintains current and applicable software engineering

expertise.

Software Safety: Software safety is applicable to most DoD systems as a factor of the ubiquitous nature of software-driven functions, network connectivity, and systems of systems (SoS). Specific mandatory certifications such as "air worthiness certification" require attention early in the development cycle to ensure adequate documentation and testing are planned and executed to meet certification criteria. Systems Engineers are encouraged to check with certification authorities frequently because rules can change during development.

4.1.4. Engineering Resources

4.1.4. Engineering Resources

Organizing and staffing the systems engineering (SE) organization and providing supporting resources and tools are critical tasks that merit attention from both the Program Manager and Systems Engineer because these tasks influence the effective implementation and control of the SE approach. The Program Manager is responsible for developing a tailored strategy that enables a cost-effective program to deliver a required capability within the needed delivery time. However, any program tailoring should be based on SE assessments of maturity and risk in order to determine the appropriate entry point into the acquisition life cycle and to identify opportunities to streamline the acquisition strategy. Therefore, the Program Manager should create a program office structure ensuring the Systems Engineer is an integrated part of the program planning and execution activities.

Building an integrated SE team with the expertise and knowledge to implement and execute an effective program is a key to success. The structure and size of the SE organization should reflect both the risk and complexity of the system under development and its life-cycle phase. The Systems Engineering Plan (SEP) describes the SE organizations of both the Government program office and, when available, the developer organization.

Roles and Responsibilities

To provide the required capabilities in the most efficient and effective manner, the Program Manager should ensure completion of the following activities that affect the technical approach:

- Ensuring proper level of governance is applied
- Ensuring processes are followed and reporting is in compliance with plans
- Interfacing with the end users and developers to determine changes in operational requirements or concepts of operations that may affect the development of the desired capability
- Ensuring coordinated development and updating of acquisition strategy documents (e.g., Technology Development Strategy (TDS) and Acquisition

Strategy (AS)), program plans (e.g., SEP, Program Protection Plan (PPP), Test and Evaluation Master Plan (TEMP), and Life-Cycle Sustainment Plan (LCSP)), and cost and budget documents
- Establishing program office organization (roles, responsibilities, authorities accountabilities) and staffing the program office and Government technical team with qualified (trained and experienced) Systems Engineers and other relevant technical professionals
- Integrating all aspects of the program office, including business processes relating to program management, SE, test, and program control
- Ensuring all necessary memoranda of understanding and agreement (MOU/MOAs) are in place and sufficiently detailed
- Resourcing the managers of all functional areas such as administration, engineering, logistics, test, etc.
- Managing program risks by developing, resourcing, and implementing realistic mitigation strategies
- Approving the configuration management plan and ensuring adequate resources are allocated for implementing configuration management throughout the life cycle
- Reviewing/approving Engineering Change Proposal (ECP) requests and determining the path forward required by any baseline changes
- Ensuring contracting activities are coordinated with the program systems engineering team

The Systems Engineer is responsible for planning and overseeing all technical activity within the program office and for managing effective SE processes. The Systems Engineer should ensure the Program Manager has sufficient and clear information for scheduling and resource-allocation decisions. In addition, the Systems Engineer implements and controls the technical effort by:

- Implementing and maintaining disciplined SE processes
- Understanding the nature of the system under development, the needs of the end user, and the operating environment as described in the concept of operations
- Conducting activities in support of contract award and execution
- Ensuring that no constructive changes and unauthorized commitments are made with the contractor or developer
- Understanding how the system fits into a larger system of systems (SoS) context
- Providing recommendations on the contract strategy
- Assisting in generating affordability targets and should-cost goals by analyzing and verifying technical assumptions used in the cost analyses and related cost and budget documents
- Assessing process improvement activities in support of should-cost goals
- Developing and maintaining the SEP in coordination with key stakeholders and other functional experts who participate in the program development activities
- Tracking and managing the execution of the contract's SE-related tasks and activities in each acquisition phase as detailed in the SEP

- Working closely with developer's SE teams to ensure integrated and effective processes
- Planning and executing the formal technical reviews and audits
- Tracking and reporting baseline changes and recommending a path forward, as a part of configuration management
- Supporting the Program Manager in configuration management activities
- Identifying and mitigating the program's technical risks which include
    - Integration risks
    - Engineering risks
    - Critical technology risks assessed in the Technology Readiness Assessment (TRA)
- Measuring and tracking program maturity using technical performance measures, requirements stability, and integrated schedules
- Updating the PPP
- Staffing the engineering team with qualified and appropriate engineers
- Supporting updates to the TEMP and LCSP
- Supporting test and evaluation activities as documented in the TEMP (see Chief Developmental Tester responsibilities in DAG Chapter 9 Test and Evaluation)
- Reviewing requirements traceability matrix and cross reference matrix (verification)
- Managing root cause and corrective action (RCCA) efforts along with supporting the risk boards
- Ensuring selection of qualified vendors for parts, materiel, and processes (for hardware and software)
- Reviewing deliverables on the contract to ensure compliance and utility, and to ensure appropriate format and content

One of the key responsibilities of the Systems Engineer is to provide insight/oversight of the technical activities of the capability acquisition. To ensure the success of integrated processes the Systems Engineer should maintain continuous engagement with the developer's Systems Engineer responsible to build, deploy, and sustain the system or capability being acquired. This continuous engagement is necessary to ensure a common understanding of program goals, objectives, and activities. The program office and developer SE team should further maintain frequent, effective communication, in accordance with the contract, as they manage and execute program activities and trade-off decisions.

The Program Manager and Systems Engineer focus on the transformation of required operational and sustainment needs into a system design capability. As the design solution evolves through the application of the eight technical processes, the verification component or test organization provides confidence that the design solution that evolved from the requirements analysis, functional allocation, and design synthesis properly addresses the desired capabilities. The Test Engineer, working in tandem with the Systems Engineer, accomplishes the verification loop of the SE process. Together the Systems Engineer and Test Engineer generate and analyze data from the integrated tests. The developer uses the test results to improve system performance,

the SE team uses the test results for risk assessments, and the acquisition community and operational evaluators use the test results for operational assessments of the evolving system. This test and evaluation strategy should be consistent with and complementary to the SEP. The Program Manager and the Systems Engineer work closely with the Test Engineer to facilitate coordinated verification and validation activities.

Stakeholders

The Program Manager has the critical role of approving a systems engineering (SE) approach that includes all stakeholders. The Systems Engineer coordinates with all participants to translate the operational needs and capabilities into technically feasible, affordable, testable, measurable, sustainable, achievable (within scheduled need dates), and operationally effective and suitable system requirements. The Systems Engineer is responsible for planning and overseeing all technical activity within the program office and for managing stakeholder expectations. Early and frequent involvement with stakeholders by both the Program Manager and the Systems Engineer facilitates the successful execution of SE activities throughout the acquisition life cycle.

Most program personnel are involved in one or more of the 16 SE processes. Personnel from non-SE organizations or from outside the program office (e.g., end users, requirements sponsors, maintainers, testers, planners) should be integrated within the program's technical management activities so they have the ability to actively participate throughout the life cycle in support of SE-related activities.

The following is a partial list of the stakeholders that contribute to and benefit from SE activities and processes:

- Warfighters and other end users
- Milestone Decision Authority (MDA)
- Resource sponsors
- Budget authority
- Developers
- Enabled or enabling systems in the system of systems (SoS)
- Security Manager or System Security Engineer
- Chief Developmental Tester
- Operational test organization
- Certification and accreditation authorities
- Logisticians (materiel readiness and sustainment)
- Trainers
- Budget and cost analysts
- Contracting officers and associated staff
- Environment, safety, and occupational health (ESOH) staff
- Contractors who build, test, deploy, and/or support the capability under development

- Companion programs

Integrated Product Teams

An effective SE organization is typically structured as one or more IPTs (refer to the DoD IPPD Handbook for specific examples of functionally integrated IPTs). The IPTs include technical experts from relevant technical fields and carry out their activities as an integrated effort with a focus on delivering the required capability(ies). In developing the program office and SE organizational structure, the Program Manager and Systems Engineer should know and understand both the design and functions of the developer's technical organization along with the developer's business model (in-house vs. outsourced). This understanding is critical to ensure effective coordination and oversight of developer activities and can affect how meetings are set up and conducted, how configuration management is executed, etc. In some cases, the Program Manager and Systems Engineer may organize multiple IPTs to align with the major products in the program's Work Breakdown Structure. In smaller programs, the SE organization may be organized as a single IPT.

IPTs provide both the Government and developer stakeholders with the opportunity to maintain continuous engagement. This continuous engagement is necessary to ensure a common understanding of program goals, objectives, and activities. These Government/developer IPTs should further maintain effective communication as they manage and execute those activities and trade-off decisions. The program's SE processes should include all stakeholders in order to ensure the success of program efforts throughout the acquisition life cycle.

For Major Defense Acquisition Programs, the Program Manager ensures that the program office is structured to interface with the SE Working-Level Integrated Product Team (SE WIPT) (a multidisciplinary team responsible for the planning and execution of SE) to address DoD leadership concerns and interests. The SE WIPT is chartered by the Program Manager and is usually chaired by the Systems Engineer. The SE WIPT includes representatives from OUSD(AT&L) and the component acquisition executive's organization, both Government and developer IPT leads from the program, the Program Executive Office Systems Engineer, the SoS Systems Engineer, and the developer Systems Engineer. A generic SE WIPT charter is available on the ODASD(SE) Policy and Guidance website under "Guidance and Tools."

4.1.5. Certifications

4.1.5. Certifications

Certifications provide a formal acknowledgment by an approval authority that a system or program meets specific requirements. Certifications, in many cases, are based on statute or regulations and drive systems engineering (SE) planning (i.e., a program may not be able to test or field the capability without certain certifications). Used throughout the acquisition life cycle, certifications reduce program risk and increase understanding

of the system. Certain specific certifications are required before additional design, integration, network access, or testing can take place. For example, airworthiness certifications need to be in place before an aircraft can begin flight testing. Often programs insufficiently plan for the number of required certifications. Insufficient planning for certifications can have a negative impact on program costs and schedule.

Obtaining the various certifications can be a lengthy process. As a result, the Program Manager should ensure that the time necessary to obtain any required certification is factored into technical planning. By planning for the activities required to achieve the necessary certifications, the Program Manager and Systems Engineer can ensure that development of the system continues uninterrupted while the program meets all system certification requirements. Early planning allows the Systems Engineer and technical team to begin interacting with certification authorities, which sets the foundation for communication throughout the development of the system.

The SEP Outline requires programs to provide a certification matrix that identifies applicable technical certifications and when they are required during the acquisition life cycle. Programs should include certification activities and events in the Integrated Master Schedule (IMS) and the Integrated Master Plan (IMP).

A non-exhaustive list of certifications is available on the DASD(SE) website. Furthermore, Program Managers and Systems Engineers should consult both Joint and Service-specific domain experts to determine other certifications that may be required.

4.1.6. Systems Engineering Role in Contracting

4.1.6. Systems Engineering Role in Contracting

The Systems Engineer should actively participate in developing program contract tasks to ensure that the appropriate technical activities are contained and properly scoped in the final contract. Proper scoping of the technical tasks in the Statement of Work (SOW), Statement of Objectives (SOO), or Performance Work Statement (PWS) is necessary to ensure that the final system meets end user's needs. Often contracting activities may appear to be primarily programmatic in nature (e.g., acquisition strategy development, writing requests for proposal, performing market research, developing the Contract Data Requirements List (CDRL)) but, in fact, they reflect technical planning and should be influenced by the desired technical content. For example, technical understanding of data rights can be a key element in planning for modularity and open systems design, or the decision to choose an incremental acquisition strategy depends on generic functionality groupings that may not be appropriate for every system.

The Systems Engineer should contribute to the development of contract incentives and/or incentive approaches that promote an understanding of the technical risks inherent in the selected development approach. Incentives such as award fee may be tied to program performance and progress that may be evaluated during technical reviews, or more frequently the incentive is tied to the completion of a technical review.

If that is the case, the developer may have a strong incentive to call the review complete as soon as possible. The Systems Engineer and Program Manager exercise best judgment in an objective and informed manner to ensure the reviews are not prematurely declared completed in order for the developer to qualify for the contract incentive. Another area to which incentives are tied is the Earned Value Management System (EVMS). The Program Manager should ensure that the EVMS tied to any incentive measures the quality and technical maturity of technical work products instead of just the quantity of work. If contracts include earned value (EV) incentives, the criteria should be stated clearly and should be based on technical performance. EV incentives should be linked quantitatively with:

- Technical performance measurement (TPM)
- Progress against requirements
- Development maturity
- Exit criteria of life-cycle phases
- Significant work packages and work products

Additional information about EVMS can be found in DAG Chapter 11 Program Management Activities. The Program Manager should make it a priority to engage with industry to clarify Government expectations and ensure a common understanding of the capability desired, need dates, risks, complexity, and scope. Access to current market information is critical for the program office as it defines requirements for acquisition programs. It is equally important for the contracting officers as they develop acquisition strategies, seek opportunities for small businesses, and negotiate contract terms. The best source of this information is usually found within industry partners. OMB memo, "Myth-Busting: Addressing Misconceptions to Improve Communication with Industry during the Acquisition Process" addresses productive interactions between federal agencies and industry partners. These interactions are strongly encouraged to ensure that the Government clearly understands the marketplace and can award a contract or order for an effective solution at a reasonable price. Early, frequent engagement with industry is especially important for complex, high-risk procurements, including (but not limited to) those for large information technology (IT) projects. Program Managers should develop ways to remove unnecessary barriers to reasonable communication and develop vendor communications plans, consistent with existing law and regulation, which promote responsible exchanges.

The program office uses a Request for Information (RFI) to communicate expectations and plans, including the expected business rhythm for contract execution. This communication ensures the offerors have an opportunity to provide a tight linkage across the Integrated Master Plan (IMP), Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), risk management, and cost in their proposals. Early industry engagement opportunities include pre-solicitation notices, industry days, and other market research venues.

Before releasing the RFP, the program office needs to allow enough time to develop and mature the performance and functional specifications that need to be included in

the RFP. The RFP and supporting technical documentation clearly define the Government's expectations in terms of the performance and functional specifications, program planning, program process, risks, and assumptions. The RFP also should direct potential offerors to integrate their approach to reflect the Government's expectations.

It is the responsibility of the Systems Engineer to ensure that technical documents accurately and clearly communicate the Government's requirements including mandatory design, build, test, certification, approval, and acceptance criteria. This ensures the developer is made aware of all required processes and objective quality evidence (OQE) to be produced, to include processes leading to certification, approval, and acceptance using predetermined OQE. In addition, the Program Manager should consider providing all offerors with the IMP and top-level schedule (with internal and external dependencies), expected business rhythm, current risk assessments, and the Systems Engineering Plan (SEP) as part of the RFP.

Although there are many opportunities for contract-related interactions between the Government and potential offerors prior to contract award, the RFP remains the primary tool for shaping the contract, the program, and ultimately the system. See the "Guide for Integrating Systems Engineering into DoD Acquisition Contracts, Version 1.0, 2006" for additional guidance on the content and format of RFPs.

Within the RFP development team, the Systems Engineer should be responsible for the technical aspects of the RFP and should perform the following actions:

- Reference current required operational documentation and system performance specifications
- Identify SE process requirements (for example, requirements management, configuration management, and risk management; see DAG section 4.3. Systems Engineering Processes)
- Identify any design considerations including production; reliability and maintainability(R&M); environment, safety, and occupational health (ESOH); human systems integration (HSI); and security
- Identify for delivery Government-required technical data rights produced by the developer
- List and describe technical assessment evidence and events, including technical reviews, audits, and certifications and associated entrance/exit criteria
- Specify data protection, SoS, and system testing and verification requirements
- Coordinate with Chief Developmental Tester in regard to the test and evaluation requirements
- Provide a requirements verification traceability database (requirements and test method)
- Specify meetings and technical documentation between the program office and the developer
- Conduct a review of the deliverables (what data, level of detail, data rights, and when needed) and buy only what is needed in concert with should cost goals

- Lead or support the technical evaluation during source selection, to include providing inputs to the development of source selection criteria
- Perform schedule risk assessments as part of the source selection evaluation process
- Support the Independent Management Review (Peer Review) of the RFP before release
- Identify external or SoS interfaces and ensure the technical interface requirement and task scope are unambiguous to the offerors

Table 4.1.6.T1 contains the typical technical contents of the RFP and the associated Systems Engineer's responsibilities, and should not be considered an exhaustive or mandatory list.

Table 4.1.6.T1. Typical Technical Contents of a Request for Proposal (RFP)

	Typical Technical Contents	SE Responsibilities
Section C Description of Work to Be Performed	• Statement of Work (SOW) • System Performance Specification • Operational Documents (CONOPS, SoS, Requirements, etc.) • Engineering processes	• Provide program technical requirements and technical aspects in the SOW • Generate the system performance specification • Identify application of SE processes • Identify appropriate technical specifications and standards
Section H Special Contract Requirements	• Key personnel • Government-furnished equipment or information (GFE or GFI) • Obsolescence management • Warranties • Options for delivery of software • Award fees	• Include a clear statement of any special contract requirements that are not included in other sections of the uniform contract format
Section J Attachments	• Systems Engineering Plan (SEP) • Program Work Breakdown Structure (WBS) • Integrated Master Plan (IMP) • Top-level program schedule • Contract Data Requirements List (CDRL) • Contract security classification specification • Data rights attachment	• Support development of WBS, IMP, top-level program schedule, CDRL, and Contract Security Specification • Ensure that sufficient time is allotted to develop high-quality specifications and plans prior to releasing the RFP

	Typical Technical Contents	SE Responsibilities
Section K Representations, Certifications, and Other Statements	• Data rights	• Identify provisions that require representations, certifications, or the submission of other information by offerors • Consider including a provision requiring offerors to identify any technical data or computer software the offeror proposes to deliver to the Government after award with less than unlimited rights
Section L Instructions on Content and Structure of RFP Response	• Systems engineering solution • Systems engineering management processes • Technical baseline management • Technical reviews and audits • Risk management processes and known key risk areas • Mandatory (i.e., statute- and regulation-driven) and advised design considerations • Technical organization • Technical data required for a Streamlined Life Cycle Assessment (LCA)	• Adequately define the offeror's design • Provide technical background and context for the offeror's solution • Describe the offeror's SE technical and management processes • Provide consistency across the SOW and system specifications • Demonstrate alignment with Government processes

	Typical Technical Contents	SE Responsibilities
Section M Source Selection Evaluation Factors	• Technical: technical solution, supporting data, performance specification • Management: SOW, Contractor Systems Engineering Management Plan (SEMP), IMS, risks plans • Environmental objectives (when appropriate) • Quality or product assurance • Past performance • Price or cost to the Government • Extent offeror's rights in the data rights attachment meet Government's needs	• Define technical evaluation factors and provide SE specific evaluation criteria used to assess proposals • Participate on or lead the technical evaluation team • Provide technical personnel to participate on each evaluation factor team (e.g., management, past performance, cost) • Provide consistency across the SOW and system specifications • Evaluate RFP responses against technical requirements, threshold requirements, management (e.g., SEMP, WBS, and program schedule), and consistency across the proposal (e.g., link between WBS, program schedule, risks, and cost) • Identify and assess the technical risks for each proposal, including schedule risks and related risk mitigation plans

4.2. Systems Engineering Activities in the Life Cycle

4.2. Systems Engineering Activities in the Life Cycle

This section is split into two major areas.

- DAG sections 4.2.1 - 4.2.7 provide introductory material and describe the Systems Engineer's role in each phase of the weapon system acquisition life cycle. The notional technical reviews and audits in each phase are identified, but the details are left for the second major area of 4.2.
- DAG section 4.2.8 provides an overview of technical reviews and audits, followed by DAG sections 4.2.9 - 4.2.17 which address each specific technical review and audit. This arrangement accommodates the planning and conducting of the technical reviews and audits in accordance with a program's specific needs. Some large and complex programs may require each technical review and audit; others may combine technical reviews and audits or get permission to tailor them out.

4.2.1. Life-Cycle Expectations

4.2.1. Life-Cycle Expectations

Systems engineering (SE) provides the technical foundation for all acquisition activities regardless of acquisition category (ACAT) or acquisition model (e.g., weapon system or information system). The SE framework described in this chapter spans the entire acquisition life cycle and is based on DoDD 5000.01 and DoDI 5000.02. Framework content should be tailored and structured to fit the technology maturity, risks, interdependencies, related characteristics, and context for the program or the system of interest. The succeeding sections identify the SE activities, processes, inputs, outputs, and expectations during each acquisition phase and for each technical review and audit.

Acquisition milestones and SE technical reviews and audits serve as key points throughout the life cycle to evaluate significant achievements and assess technical maturity and risk. Table 4.2.1.T1 identifies the objectives of each SE assessment and the technical maturity point marked by each review. The Materiel Development Decision (MDD) review is the formal entry point into the acquisition process and is mandatory for all programs in accordance with DoDI 5000.02. Depending on the maturity of the preferred materiel solution, the Milestone Decision Authority (MDA) designates the initial review milestone. This would normally be the MDD, but it can be A, B, or C. In any case the decision is documented in the Acquisition Decision Memorandum (ADM) published immediately after an MDD event. Since the review milestone is chosen consistent with the maturity of the preferred materiel solution, entry at any milestone requires evidence of the associated solution maturity as summarized in Table 4.2.1.T1 Technical Maturity Points.

Department experience (e.g., GAO Report 12-400SP) has found that successful programs use knowledge-based product development practices which include steps to gather knowledge to confirm the program's technologies are mature, their designs are stable, and their production processes are in control. Successful product developers ensure a high level of knowledge is achieved at key junctures in development. Table 4.2.1.T1 summarizes the concept of technical maturity points.

Table 4.2.1.T1. Technical Maturity Points

TECHNICAL MATURITY POINTS			
DoD Acquisition Milestone/Decision Point & Technical Review/Audit	**Objective**	**Technical Maturity Point**	**Additional Information**

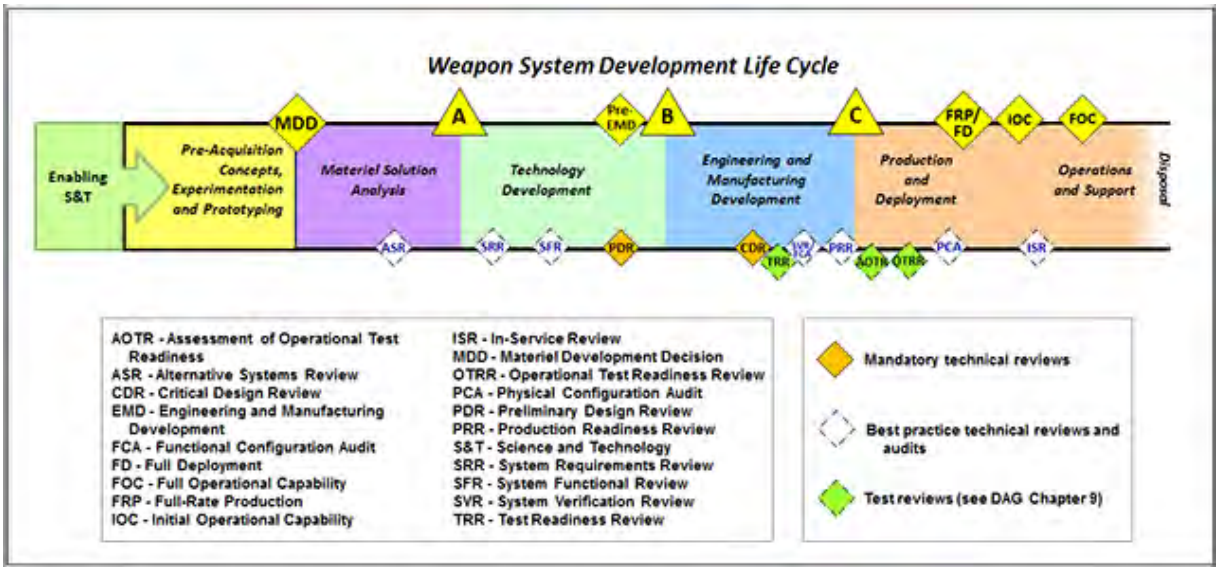
TECHNICAL MATURITY POINTS			
DoD Acquisition Milestone/Decision Point & Technical Review/Audit	**Objective**	**Technical Maturity Point**	**Additional Information**
Materiel Development Decision (MDD)	Decision to assess potential materiel solutions and appropriate phase for entry into acquisition life cycle.	Capability gap met by acquiring a materiel solution.	Technically feasible solutions have the potential to effectively address a validated capability need. Technical risks understood.
Alternative Systems Review (ASR)	Recommendation that the preferred materiel solution can affordably meet user needs with acceptable risk.	System parameters defined; balanced with cost, schedule, and risk.	Initial system performance established and plan for further analyses supports Milestone A criteria.
Milestone A	Decision to invest in technology maturation and preliminary design.	Affordable solution found for identified need with acceptable technology risk, scope, and complexity.	Affordability targets identified and technology development plans, time, funding, and other resources match customer needs. Prototyping and end-item development strategy for Technology Development (TD) phase focused on key technical risk areas.
System Requirements Review (SRR)	Recommendation to proceed into development with acceptable risk.	Level of understanding of top-level system requirements is adequate to support further requirements analysis and design activities.	Government and contractor mutually understand system requirements including (1) the preferred materiel solution (including its support concept) from the Materiel Solution Analysis (MSA) phase, (2) available technologies resulting from the prototyping efforts, and (3) maturity of interdependent systems.
System Functional Review (SFR)	Recommendation that functional baseline fully satisfies performance requirements and to begin preliminary design with acceptable risk.	Functional baseline established and under formal configuration control. System's functions decomposed and defined to lower levels in order to start preliminary design.	Functional requirements and verification methods support achievement of performance requirements. Acceptable technical risk of achieving allocated baseline.

TECHNICAL MATURITY POINTS			
DoD Acquisition Milestone/Decision Point & Technical Review/Audit	**Objective**	**Technical Maturity Point**	**Additional Information**
Preliminary Design Review (PDR)	Recommendation that allocated baseline fully satisfies user requirements and developer ready to begin detailed design with acceptable risk.	Allocated baseline established such that design provides sufficient confidence to support 2366b certification.	Preliminary design and basic system architecture support capability need and affordability target achievement.
Pre-Engineering and Manufacturing Development (EMD) Review	Determination that program plans are affordable and executable and that the program is ready to proceed to EMD phase source selection.	Systems engineering trades completed and have informed program requirements. Competitive prototyping and the development of the preliminary design have influenced risk management plans and should cost initiatives.	The Request for Proposal (RFP) reflects the program's plans articulated in the draft Acquisition Strategy and other draft, key planning documents such as the Systems Engineering Plan (SEP), Program Protection Plan (PPP), Test and Evaluation Master Plan (TEMP), and Life-Cycle Sustainment Plan (LCSP).
Milestone B	Decision to invest in product development, integration, and verification as well as manufacturing process development.	Critical technologies assessed able to meet required performance and are ready for further development. Resources and requirements match.	Maturity, integration, and producibility of the preliminary design (including critical technologies) and availability of key resources (time, funding, other) match customer needs. Should cost goals defined.
Critical Design Review (CDR)	Recommendation to start fabricating, integrating, and testing test articles with acceptable risk.	Product design is stable. Initial product baseline established.	Design is stable and performs as expected. Initial product baseline established by the system detailed design documentation confirms affordability/should-cost goals. Government control of Class I changes as appropriate.
System Verification Review (SVR)	Recommendation that the system as tested has been verified (i.e., product baseline is compliant with the functional baseline) and is ready for validation (operational assessment) with acceptable risk.	System design verified to conform to functional baseline.	Actual system (which represents the production configuration) has been verified through required analysis, demonstration, examination, and/or testing. Synonymous with system-level Functional Configuration Audit (FCA).

TECHNICAL MATURITY POINTS			
DoD Acquisition Milestone/Decision Point & Technical Review/Audit	**Objective**	**Technical Maturity Point**	**Additional Information**
Production Readiness Review (PRR)	Recommendation that production processes are mature enough to begin limited production with acceptable risk.	Design and manufacturing are ready to begin production.	Production engineering problems resolved and ready to enter production phase.
Milestone C	Decision to produce production-representative units for operational test and evaluation (OT&E).	Manufacturing processes are mature enough to support Low-Rate Initial Production (LRIP) and generate production-representative articles for OT&E.	Production readiness meets cost, schedule, and quality targets. Begin initial deployment as appropriate.
Physical Configuration Audit (PCA)	Recommendation to start full-rate production and/or full deployment with acceptable risk.	Final product baseline established. Verifies the design and manufacturing documentation matches the item to be fielded, following update of the product baseline to account for resolved OT&E issues.	Confirmation that the system to be fielded matches the product baseline. Product configuration finalized and system meets user's needs. Conducted after OT&E issues are resolved.
Full-Rate Production Decision Review (FRP DR) or Full Deployment Decision Review (FDDR)	Decision to begin full-rate production and/or decision to begin full deployment.	Manufacturing processes are mature and support full-rate production and/or capability demonstrated in operational environment supporting full deployment (i.e., system validated through OT&E).	Delivers fully funded quantity of systems and supporting materiel and services for the program or increment to the users.

Figure 4.2.1.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the system life cycle.

Figure 4.2.1.F1. Weapon System Development Life Cycle



The Systems Engineer leads the development and implementation of a technical program strategy. SE processes help deliver capabilities that meet warfighter needs within cost and schedule by balancing end-user needs, design considerations, resource constraints, and risk. The Systems Engineer uses technical reviews and audits to assess whether preplanned technical maturity points are reached during the acquisition life cycle as the system and system elements mature. This knowledge forms the basis for the Systems Engineer's recommendations to the Program Manager on how to technically proceed with the program.

4.2.1.1. Systems Engineering in Other Acquisition Models

4.2.1.1. Systems Engineering in Other Acquisition Models

The acquisition model captured in this version of the DAG Chapter 4 is based on the weapon system model described in DoDI 5000.02 dated December 8, 2008. Other models are being used in the Defense Department which are variations of this model. The anticipated update to DoDI 5000.02 is expected to address these other models. When it is issued, DAG Chapter 4 will be updated accordingly.

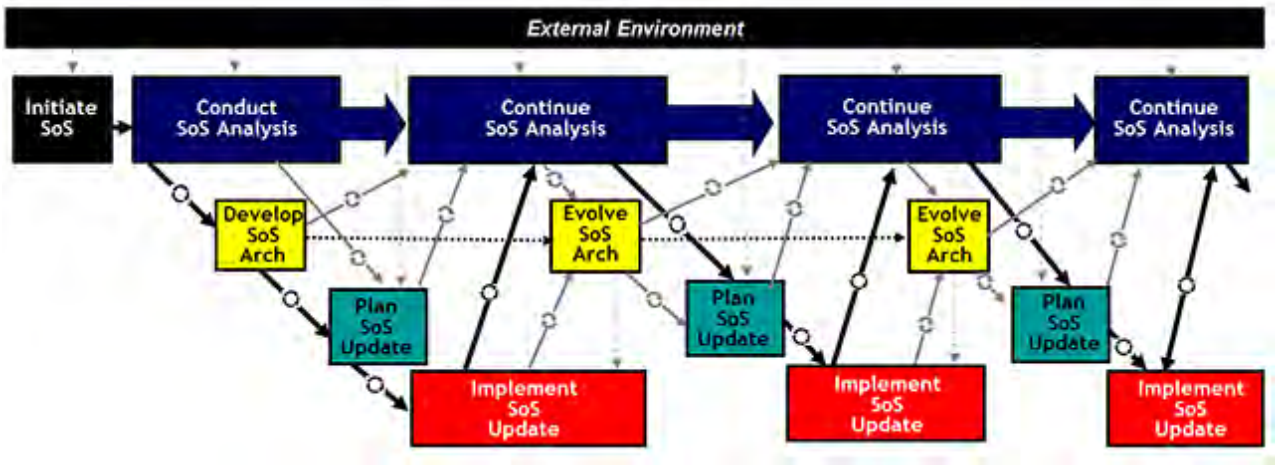
4.2.1.2. Systems of Systems

4.2.1.2. Systems of Systems

Whether or not a system is formally acknowledged as a system of systems (SoS), nearly all of our DoD systems function as part of an SoS to deliver a necessary capability to the warfighter (see Systems Engineering Guide for Systems of Systems on the DASD(SE) website). SoS systems engineering (SE) is an ongoing iterative process

as shown in the SoS SE Implementers' View in Figure 4.2.1.2.F1. The backbone of SoS SE implementation is continuous analysis that considers changes from the broader environment as well as feedback from the ongoing engineering process. The results of that analysis provide the basis for developing and evolving the SoS architecture, identifying or negotiating changes to the constituent systems that impact the SoS, and working with the constituent systems to implement and integrate those changes. This view of SoS SE implementation provides structure to the evolution of the SoS through changes in constituent systems that are typically on different life-cycle timelines, adapting as systems come in and move out, and as concept of operations (CONOPS) adapt and change. Hence the need for continually updating the SoS analysis and adapting the architecture and updating systems on an ongoing basis.

Figure 4.2.1.2.F1. SoS SE Implementers' View



Therefore, SoS SE planning and implementation should consider and leverage the development plans of the individual systems in order to balance SoS needs with individual system needs. Finally, SoS SE should address the end-to-end behavior of the ensemble of systems, addressing the key issues that affect this end-to-end behavior with particular emphasis on integration and interoperability. Effective application of SoS SE addresses organizational as well as technical issues in making SE trades and decisions. The Systems Engineer has different roles and authorities at the system versus the SoS level. The SoS-level Systems Engineer can provide the technical foundation for effective user capabilities by conducting balanced technical management of the SoS, using an SoS architecture based on open systems and loose coupling, and focusing on the design strategy and trades (both at establishment and through evolution). They should collaborate with multiple Systems Engineers across multiple systems. Each Systems Engineer has the authority for their system implementation. These waves of implementations and upgrades taken as a whole provide the SoS capability.

Consideration of SoS in SE for Individual Systems

Most acquisition programs address the development or major upgrade of individual systems (in contrast to SoS). Understanding the SoS context(s) of the system (including use in multiple operational environments) is critical to developing requirements for the system so when delivered it operates effectively in user operational environments. From the Joint Capabilities Integration and Development System (JCIDS) Capabilities-Based Assessment (CBA) through sustainment activities, it is important to recognize how the system context influences system requirements. An up-to-date CONOPS for the system is basic to understanding the system context, notably mission and task threads and data exchanges that have an impact on the system. Systems engineers of individual systems should ensure SoS considerations and risks are addressed throughout the acquisition life cycle by:

- Identifying system dependencies and interoperability needs (See DAG section 4.3.18.13. Interoperability and Dependencies);
- Factoring these into the development of system concepts, requirements, and risks; and
- Addressing these through trade analysis, system architecture and design, interface development and management, and verification and validation.

Both from an individual system perspective and the SoS perspective, Program Managers and Systems Engineers have found it difficult to coordinate and balance the acquisition objectives and strategies for a given system with those of the SoS and other constituent systems. A senior governance body is useful to provide a forum for discussion and decision. This forum should address technical plans, configuration management, and strategies with respect to interfaces, interdependences, risks, and risk mitigation. It is critical to address all equities and make collective decisions that can be implemented in changes to a system's configuration.

One SoS best practice is to monitor closely interdependent programs, with checkpoints at scheduled design reviews to assess program progress, assess related risks, and determine actions to mitigate potentially negative impacts.

Table 4.2.1.2.T1 lists SoS considerations for systems at each stage of acquisition. At each phase, the SE approach to addressing SoS-related dependencies should be addressed in the Systems Engineering Plan (SEP).

Table 4.2.1.2.T1. Key SoS Considerations for Systems by Acquisition Phase

	Pre-MDD	MSA	TD	EMD	P&D and O&S
Focus	• Define role of the system in supporting a mission	• In the Analysis of Alternatives (AoA), consider the	• Assess the technical approaches and risks for	• Develop, verify, and validate the detailed	• Verify the as-built interface s meet

	capability, including relationship to other systems in the SoS which support that capability.	alternatives in the context of the larger SoS supporting the capability. • In the operational analysis and concept engineering for the preferred materiel solution, consider the new system in the SoS context, identify dependencies and relationships with other systems, including key interfaces and technical risks based on SoS considerations to be addressed in Technology Development (TD). • Identify the nature of the dependencies and interfaces, including the parties involved, and an initial plan for addressing these including initial memoranda of agreement (MOAs).	addressing system requirements including considerations for the system as a component operating in a SoS context (including dependencies, interoperability, and interfaces). • Address considerations of changes needed in other systems for the systems in acquisition to meet capability objectives.	design that addresses system requirements, considering the SoS context including recognized dependencies and interfaces.	specs and support operational needs. • Support effective system operation in a SoS context.
Evidence/Produc	• End-to-end depiction (e.g., mission thread) of capability gap in context of systems	• AoA criteria or results relevant to SoS dependencies or interfaces • Definition of	• An interface management plan that is a part of a configuration management plan including	• Interface documentation, test plans and reports • Progress on MOAs with system's	• Test reports

	currently supporting capability	key system dependencies or interfaces that influence system requirements • Initial management plans with supporting MOAs, including draft Interface Control Agreements (ICAs) for collaborations with other systems in a SoS • Risks associated with SoS dependencies (both programmatic and technical) and interoperability requirements, including environment, safety, and occupational health (ESOH), and security risks to be accepted by Joint Authorities	ICAs • Risks associated with SoS dependencies and interoperability requirements	dependencies • Risks associated with SoS dependencies and interoperability requirements	
Measure/ Metrics	• Activities supported by the system in relationship to other systems and the context • Physical environment information needs DOTLPF for the system and the SoS	• SoS-related requirements in draft system specification and/or Pre-A Request for Proposal (RFP) • MOAs with key parties in SoS dependencies or relationships	• Final interface specifications • MOAs and schedule for interface management plan • Progress with respect to schedule and plan milestones • Progress with respect to	• Successful development and test of interfaces • Progress with respect to SoS schedule and plan milestones • Progress with respect to expected performance.	• Successful test results

	• Identification of stakeholders		expected performance.		
Responsibilities/ Inter-dependencies	• Provided by the JCIDS analysis and the evidence provided at MDD	• Systems engineers of the systems involved in the SoS or SoS SE if one exists (All) • End users • Requirements developers • Program Manager (MOA) • Contracting (RFP)	• System developers of this system and the other systems involved with the dependencies of interface; shared configuration management (CM) • Interface Management Working Group (IMWG) • End users	• Developers • IMWG • Testers • End users	• Developers • Testers • End users

For a more detailed discussion of SE for SoS, refer to the SoS Initiatives page on the DASD(SE) website.

4.2.2. Pre-Materiel Development Decision

4.2.2. Pre-Materiel Development Decision

The objectives of the pre-Materiel Development Decision (MDD) efforts are to obtain a clear understanding of user needs, identify a range of technically feasible candidate materiel solution approaches, consider near-term opportunities to provide a more rapid interim response, and develop a plan for the next acquisition phase, including the required resources. This knowledge supports the Milestone Decision Authority's (MDA) decision to authorize entry into the acquisition life cycle and pursue a materiel solution. An additional objective is to characterize trade space, risks, and mission interdependencies to support the start of the Analysis of Alternatives (AoA).

Policy in this area comes from two perspectives: the Joint Capabilities Integration and Development System (JCIDS) defined in CJCSI 3170.01 and the Defense Acquisition System (DAS) defined in DoDD 5000.01.

DTM 10-017, "Development Planning to Inform Materiel Development Decision (MDD) Reviews and Support Analyses of Alternatives (AoA)", issued September 2010, introduced specific policy on development planning in support of defense acquisition.

Development planning (DP) encompasses the engineering analysis and technical

planning activities that provide the foundation for informed investment decisions on the path a materiel development follows to effectively, affordably, and sustainably meet operational needs. Development planning activities are initiated prior to the Materiel Development Decision, continue throughout the Materiel Solution Analysis phase, and eventually transition to the program environment.

Attention to critical systems engineering (SE) processes and functions, particularly during early phases in acquisition, is essential to ensuring that programs deliver capabilities on time and on budget. The effective execution of pre-MDD SE efforts provides the foundation for user-driven requirements and technically feasible solution options that ensure an executable program. At MDD, the MDA not only decides whether an investment is made to fill the capability gap but also determines the fundamental path the materiel development will follow. This decision should be based on effective development planning.

An important aspect of the pre-MDD effort is narrowing the field of possible solutions to a reasonable set that is analyzed in the AoA. Early recognition of constraints, combined with analysis of technical feasibility, can eliminate many initial ideas because they lack the potential to meet the need in a timely, sustainable, and cost-effective manner. Conversely, the range of alternatives analyzed in the AoA are chosen from a sufficiently broad solution space. Whenever possible, the Systems Engineer should try to engage with the end user before the Initial Capabilities Document (ICD) and associated operational architecture is validated by the Joint Requirements Oversight Council (JROC) (see DAG section 4.3.12. Stakeholder Requirements Definition Process).

Studies have found that "programs that considered a broad range of alternatives tended to have better cost and schedule outcomes than the programs that looked at a narrow scope of alternatives." (Reference GAO-09-665 Analysis of Alternatives, page 6.)

The work performed in this time frame should be well documented so the Program Manager and Systems Engineer, when assigned, can benefit from the mutual understanding of the basis of need (requirements) and the art of the possible (concepts/materiel solutions). To achieve these benefits, the Systems Engineer should proactively collaborate with the Science and Technology (S&T) and user communities.

Roles and Responsibilities

Often there is no assigned Program Manager or Systems Engineer at this point in the weapon system's life cycle. Instead, a designated Service representative is orchestrating and leading the preparations for MDD. This leader, motivated by the entrance criteria for MDD, is responsible for synthesizing the necessary information to satisfactorily address the four policy evidence needs stated in DTM 10-017. For a more detailed discussion of development planning policy, refer to the white paper on the pre-MDD Activities.

The designated Service representative should make use of appropriate models and

simulations (DAG section 4.3.19.1 Modeling and Simulation) to develop required MDD evidence. The designated Service representative also should consider issuing a Request for Information (RFI) to industry to help identify and characterize alternative solutions.

Inputs

Table 4.2.2.T1 summarizes the primary inputs and technical outputs associated with this part of the life cycle. Unlike the sections that follow, this pre-MDD period is the bridge between JCIDS and the DAS. It is the period before the pre-systems acquisition period of the DAS.

Table 4.2.2.T1. Inputs Associated with Pre-MDD

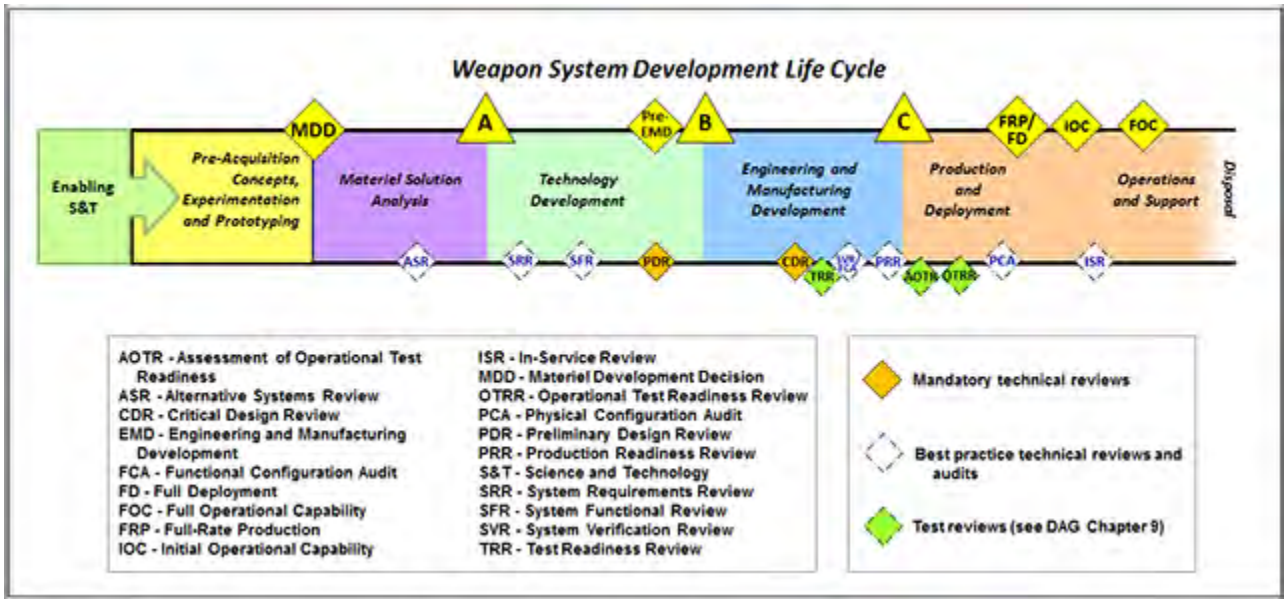
Inputs for Pre-MDD
Draft Initial Capabilities Document (ICD) • Product of Capability-Based Assessment (CBA) or equivalent, see CJCSI 3170.01
Other analyses • Other prior analytic, experimental, prototyping, and/or technology demonstration efforts may be provided by the S&T community

The MDD review requires an ICD that represents an operational capability need validated in accordance with CJCSI 3170.01. The Joint Staff provides this document, which is generally the output of a Capability-Based Assessment (CBA) or other studies. The designated Service representative should have access to both the ICD and supporting studies. Other technical information (such as models and simulations) may be useful for understanding both the need and its context. The S&T community can contribute pertinent data and information on relevant technologies, prototypes, experiments, and/or analysis. An example is available of how a program may provide evidence at the MDD review to support the MDA decision.

Activities

Figure 4.2.2.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.2.F1. Weapon System Development Life Cycle



During pre-MDD, SE activities focus on

- Achieving an in-depth understanding of the operational capability gaps defined in the ICD and identifying the sources of the gap(s) which, if addressed by a materiel solution, could achieve the needed capability
- Identifying an appropriate range of candidate materiel solutions from across the trade space to meet the need
- Identifying near-term opportunities to provide a more rapid interim response to the capability need
- Working with the S&T community (across Government, industry, and academia) as well as other collaborators to build the technical knowledge base for each candidate materiel solution in the AoA Guidance to include experimentation and prototyping
- Analyzing trade space to determine performance versus cost benefits of potential solutions
- Planning for the technical efforts required during the next phase

Outputs and Products

This effort ends after a successful MDD review in which the MDA approves entry into the Defense Acquisition System. This decision is documented in a signed Acquisition Decision Memorandum (ADM), which specifies the approved entry point, typically the Materiel Solution Analysis (MSA) phase. Outputs of pre-MDD efforts provided in Table 4.2.2.T2 also include approved AoA Guidance and an AoA Study Plan, which should be informed by SE.

Table 4.2.2.T2. Technical Outputs Associated with Pre-MDD

Technical Outputs from Pre-MDD
Informed advice to the ICD
Informed advice to the AoA Guidance and Study Plan
Informed advice to the plan and budget for the next phase, including support to the AoA and non-AoA technical efforts required to prepare for the initial milestone review
Informed advice to the ADM

All potential materiel solutions pass through an MDD before entering the DAS. However, the MDA may authorize entry at any point in the acquisition life cycle based on the solution's technical maturity and risk. Technical risk has several elements: technology risk, engineering risk, and integration risk. If the Service-recommended entry point is beyond the MSA phase, for example part way through the Technology Development (TD) phase, the program provides evidence that all MSA and TD phase-specific entrance criteria and statutory requirements are met, and that the solution's technical maturity supports entry at the point in the phase being proposed. Emphasis should be placed on the soundness of supporting technical information and plans in order to inform the MDA's decision, as opposed to which documents may or may not be complete.

As the next section explains, the MSA phase is made up of more than an AoA; it includes technical tasks to determine the preferred materiel solution based on the AoA results and technical tasks to prepare for the initial milestone review. Therefore, the technical plan and budget presented at the MDD should reflect the full range of activities required in the next phase.

4.2.3. Materiel Solution Analysis Phase

4.2.3. Materiel Solution Analysis Phase

The objective of the Materiel Solution Analysis (MSA) phase is to select and adequately describe a preferred materiel solution to satisfy the phase-specific entrance criteria for the next program milestone designated by the Milestone Decision Authority (MDA). Usually, but not always, the next milestone is a decision to invest in technology maturation and preliminary design in the Technology Development (TD) phase. The systems engineering (SE) activities in the MSA phase result in several key products. First, a system model and/or architecture is developed that captures operational context and envisioned concepts, describes the system boundaries and interfaces, and addresses operational and functional requirements. Second, a preliminary system performance specification is developed that defines the performance of the preferred materiel solution. Third, the Systems Engineer advises the Program Manager on what is to be prototyped, why, and how.

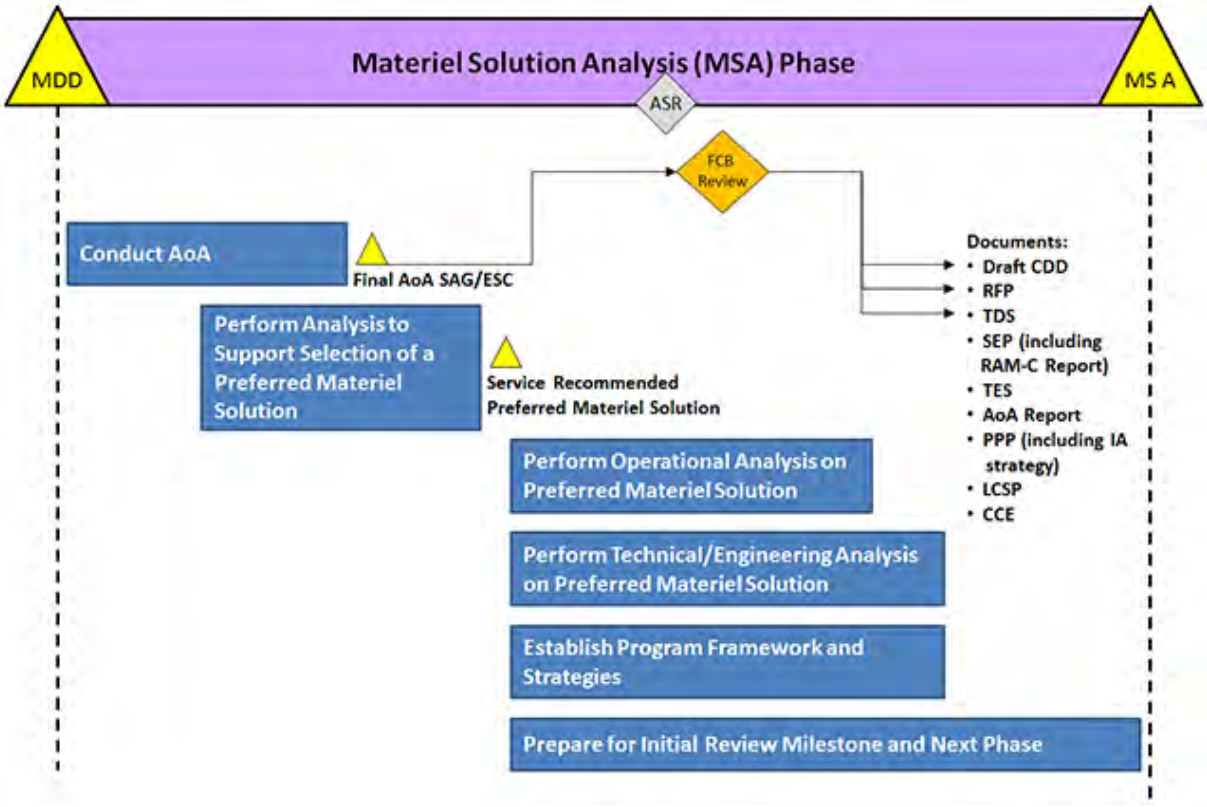
During the MSA phase, the program team identifies a materiel solution to address user

capability gaps partially based on an Analysis of Alternatives (AoA) (i.e., analysis of the set of candidate materiel solutions) led by the Director, Cost Analysis and Program Evaluation (CAPE) and conducted by an organization independent from the Program Manager. Once the Service sponsor selects a preferred materiel solution, the program team focuses engineering and technical analysis on this solution to ensure development plans, schedule, funding, and other resources match customer needs and match the complexity of the preferred materiel solution. SE activities should be integrated with MSA phase-specific test, evaluation, logistics, and sustainment activities identified in DAG Chapter 9 Test and Evaluation and Chapter 5 Life-Cycle Logistics.

This phase has two major blocks of activity: (1) the AoA and (2) the post-AoA operational analysis and concept engineering to prepare for a next program milestone designated by the MDA (see Figure 4.2.3.F1).

The AoA team considers a range of alternatives and evaluates them from multiple perspectives as directed by the AoA Guidance and AoA Study Plan. Engineering considerations including technical risk should be a component of the AoA Guidance and be addressed in the AoA Study Plan.

Figure 4.2.3.F1. Activities in Materiel Solution Analysis Phase



The objective of the AoA is to analyze and characterize each alternative (or alternative approach) relative to the others. The AoA does not result in a recommendation for a

preferred alternative; it provides information that the Service sponsor uses to select which materiel solution to pursue. The Systems Engineer may participate in the AoA to help analyze performance, feasibility, and to optimize alternatives. Using the AoA results, the Service sponsor may conduct additional engineering analysis to support the selection of a preferred materiel solution from the remaining trade space of candidate materiel solutions. After choosing the preferred materiel solution, the Service sponsor matures the solution in preparation for the next program milestone designated by the MDA.

After the AoA, program systems engineers establish the technical performance requirements consistent with the draft Capability Development Document (CDD), required at next program milestone designated by the MDA, assuming it is Milestone A. These requirements form the basis for the system performance specification placed on contract for the TD Phase. These requirements also inform plans to mitigate risk in the TD phase.

During MSA, several planning elements are addressed to frame the way forward for the MDA's decision at the next program milestone. SE is a primary source for addressing several of these planning elements. The planning elements include:

- Capability need, architecture
- System concept, architecture
- Key interfaces (including external interfaces and dependencies)
- Acquisition approach
- Engineering/technical approach/strategy
- Test and evaluation approach/strategy
- Program management approach
- External dependencies/agreements
- Schedule
- Resources
- Risks

See DAG section 4.3.2. Technical Planning Process. These planning elements are documented in various program plans such as the Technology Development Strategy (TDS), Test and Evaluation Strategy (TES), Program Protection Plan (PPP), next-phase Request for Proposal (RFP), and the Systems Engineering Plan (SEP). The SEP describes the SE efforts necessary to provide informed advice to these other planning artifacts (see the SEP Outline).

SE provides, for example, the technical basis for TD phase planning and execution, including identification of critical technologies, development of a competitive prototyping strategy, and establishment of other plans that drive risk-reduction efforts. This early SE effort lays the foundation for the TD phase contract award(s) and preliminary designs, which confirm the system's basic architecture.

Roles and Responsibilities

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Program Manager focuses on the following MSA activities, which rely on and support SE efforts:

- Prepare for and support source selection activities for the upcoming phase solicitation and contract award
- Support the requirement community with development of the draft CDD, assuming the next phase is TD
- Develop the TDS, which incorporates necessary risk-reduction activities
- Staff the program office with qualified (trained and experienced) systems engineers

In addition to the general roles and responsibilities described in DAG section 4.1.4. Engineering Resources, during this phase it is the Systems Engineer's responsibility to:

- Lead and manage the execution of the technical activities in this phase
- Measure and track program technical maturity
- Identify technologies that should be included in an assessment of technical risk
- Perform trade studies
- Support preparations for the RFP package
- Develop the system performance specification. See DAG section 4.3.7 Configuration Management Process. A particular program's naming convention for specifications should be captured in the SEP and other plans and processes tailored for the program.
- Ensure integration of key design considerations into the system performance specification.
- Develop technical approaches and plans, and document them in the SEP.
- Ensure the phase technical artifacts are consistent and support objectives of the next phase.

Inputs

Table 4.2.3.T1 summarizes the primary inputs associated with this pre-systems acquisition part of the life cycle (see DoDI 5000.02). The table assumes the next phase is TD, but most of the technical outputs would be applicable going into any follow-on phase.

Table 4.2.3.T1. Inputs Associated with MSA Phase

Inputs for MSA Phase
Initial Capabilities Document (ICD) • Product of Capability Based Assessment (CBA) or equivalent. See **CJCSI 3170.01**

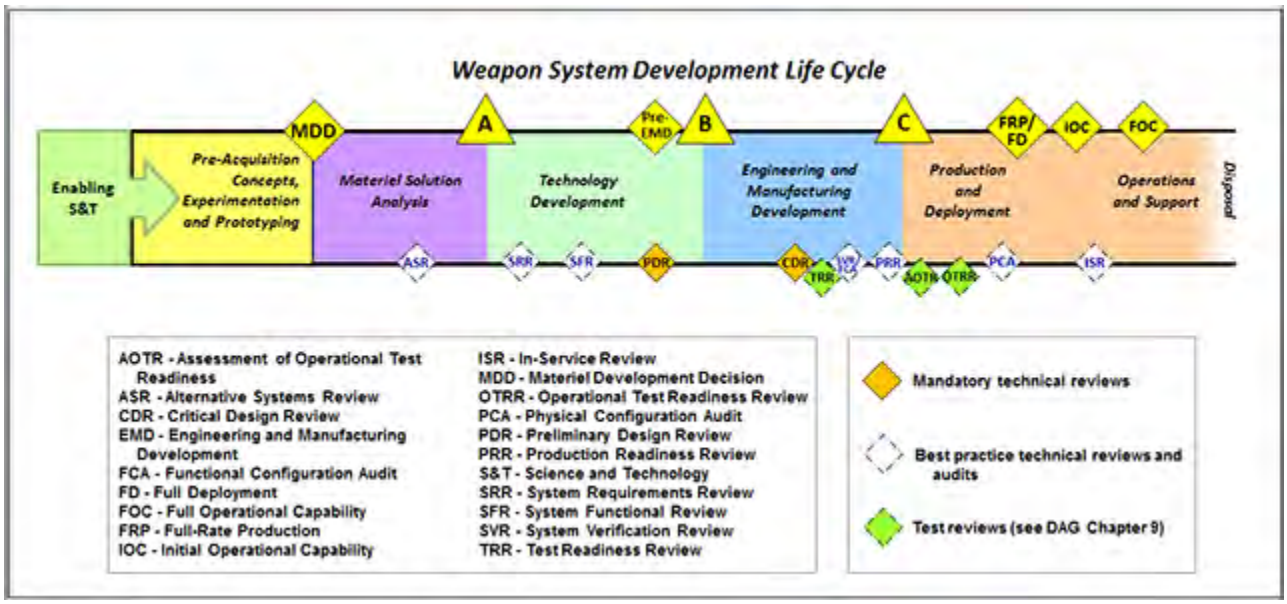
AoA Guidance and AoA Study Plan
Acquisition Decision Memorandum (ADM) (may contain additional direction)
Other analyses • Other prior analytic, prototyping, and/or technology demonstration efforts conducted by the S&T community; technology insertion/transition can occur at any point in the life cycle

The ICD, AoA Guidance, and AoA Study Plan should be available prior to the start of the MSA phase. Results of other related analyses may be available, for example from the Capability Based Assessment (see DAG section 4.3.10. Stakeholder Requirements Definition Process) or other prior analytic and/or prototyping efforts conducted by the S&T community.

Activities

The MSA phase activities begin after a favorable MDD review has been held (see DAG section 4.2.2. Pre-Materiel Development Decision) and end when the phase-specific entrance criteria for the next program milestone, designated by the MDA, have been met. Figure 4.2.3.F2 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.3.F2. Weapon System Development Life Cycle



Referring back to Figure 4.2.3.F1, which shows the major blocks of technical activities in the MSA phase:

- **Conduct AoA.** Includes all activities and analyses conducted by the AoA Study team under the direction of the Senior Advisory Group / Executive Steering

Committee (SAG/ESC) and CAPE, or Service equivalent. Concludes with a final ESC/SAG; produces AoA Report. Systems engineers should support this activity, though in DoD policy the AoA is to be conducted by an organization independent from the Program Manager.

- **Perform Analysis to Support Selection of a Preferred Materiel Solution.** Includes all engineering activities and technical analysis performed to support Service selection of the preferred materiel solution by balancing cost, performance, schedule, and risk.
- **Perform Operational Analysis on Preferred Materiel Solution**. Supports the definition of the performance requirements in the operational context, Functional Capabilities Board (FCB) review, and the development of the draft CDD (see CJCSI 3170.01 Joint Capabilities Integration and Development System (JCIDS) and DAG section 4.3.10. Stakeholders Requirements Definition Process). The Systems Engineer should support the operational requirement/user/operational test community to ensure the concept of operations (CONOPS) is detailed enough to verify and validate system performance and operational capability. This activity could include the development of design reference missions/use cases that assist in the verification and validation process. Through analysis, the Systems Engineer also helps to identify key technology elements, determine external interfaces, establish interoperability requirements, and identify critical program information.
- **Perform Engineering and Technical Analysis on Preferred Materiel Solution.** This includes all engineering activities and technical analysis performed on the Service-selected preferred materiel solution in support of the development and maturation of a materiel solution concept, associated system specification, and technical plans for the next phase.
- **Establish Program Framework and Strategies.** All activities to converge on the overarching strategies and plans for the acquisition and sustainment of the system. Attention should be given to identifying and documenting agreements with external organizations. This documentation should include, for example, the contributions of S&T organizations and plans for transitioning technology into a program.
- **Prepare for Initial Review Milestone and Next Phase.** Includes all activities to compile technical and programmatic analysis and plans to meet the entrance criteria for the next program milestone designated by the MDA. See DoDI 5000.02 for phase exit criteria and PDUSD(AT&L) memorandum, "Improving Milestone Process Effectiveness."

The technical review typically conducted in the MSA phase is the Alternative Systems Review (ASR) (see DAG section 4.2.9. Alternative Systems Review).

For a more detailed discussion of MSA phase activities, refer to the white paper on the MSA Activities Model.

Outputs and Products

The knowledge gained during this phase, based on both the AoA and other analyses, should provide confidence that a technically feasible solution approach matches user needs and is affordable with reasonable risk, see Table 4.2.3.T2. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 4.2.3.T2. Technical Outputs Associated with MSA Phase

Technical Outputs from MSA Phase
Informed advice to the draft Capability Development Document (CDD)
Informed advice to the AoA Report
Informed advice to the selection of the preferred materiel solution • Selection of the preferred materiel solution is documented in the ADM
Informed advice to the ADM
SEP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Reliability, Availability, Maintainability, and Cost Rationale Report (RAM-C Report) • Attachment to SEP as directed by DTM 11-003
Reliability Growth Curves (RGC) • Attachment to SEP as directed by DTM 11-003
PPP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc.
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades
Environment, Safety, and Occupational Health (ESOH) planning
Assessment of technical risk

Technical Outputs from MSA Phase
Consideration of technology issues • DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2
Initial identification of critical technologies
Interdependencies / interfaces / memoranda of agreement (MOAs) • Understanding of the unique program interdependencies, interfaces, and associated MOAs
Draft system performance specification
Other technical information: such as architectures, systems models, and simulations generated during the phase
Prototyping strategy • Relationship between draft system specification and competitive prototyping objectives is established and plans for next phase are consistent with this, both from a competitive prototyping and preliminary system design perspective • Includes identification of key system elements to be prototyped prior to Milestone B • Documented in the TDS as directed by DTM 09-027
Informed advice to Affordability Assessment • Affordability targets are established and treated as Key Performance Parameters (KPPs) at the next program milestone designated by the MDA • Identify the likely design performance points where trade-off analyses occur during the next phase • Value engineering results, as appropriate (see DAG section 4.3.19.3. Value Engineering) • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
Informed advice to the Life-Cycle Sustainment Plan (LCSP) • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See DAG Chapter 5 Life-Cycle Logistics
Informed advice to the Test and Evaluation Strategy (TES) • DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Informed advice to the developmental test and evaluation (DT&E) planning including Early Operational Assessments (EOAs) • See DAG Chapter 9 Test and Evaluation

Technical Outputs from MSA Phase
Informed advice to the Request for Proposal (RFP) • Informed advice including system specification, SOW, CDRLs, and source selection criteria
Informed advice to the Technology Development Strategy (TDS) • Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule, and risks • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies

4.2.4. Technology Development Phase

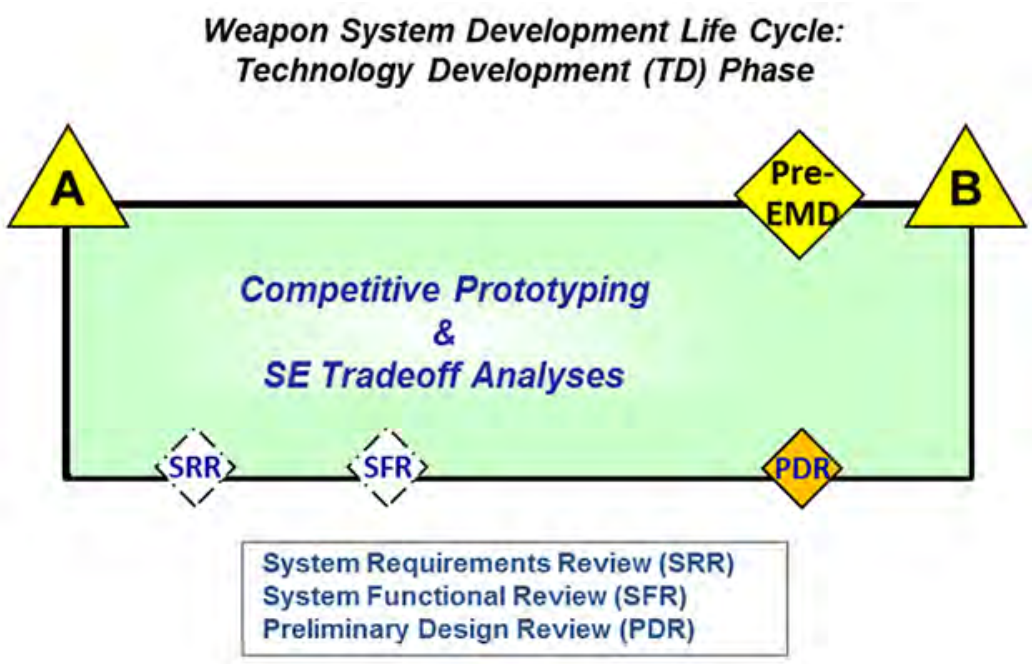
4.2.4. Technology Development Phase

The primary objective of the Technology Development (TD) phase is to reduce technical risk and develop a sufficient understanding of the materiel solution to support sound investment decisions at the pre- Engineering and Manufacturing Development (EMD) Review and at Milestone B regarding whether to initiate a formal acquisition program. The Systems Engineer supports the production of a preliminary system design that achieves a suitable level of system maturity for low-risk entry into EMD (see Figure 4.2.4.F1.). Usually the Systems Engineer implements a strategy of competitive prototyping on a system element or subsystem level, balancing capability needs and design considerations to synthesize system requirements for a preliminary end-item design for the system.

The major efforts associated with the TD phase are:

- Determine the appropriate set of technologies to integrate into a full system
- Mature the technologies including demonstrating and assessing them in a relevant environment
- Conduct competitive prototyping of the system and/or system elements
- Perform trade studies, refine requirements, and revise designs
- Develop the preliminary design, including functional and allocated baselines, specifications, interface control drawings/documents, architectures, and system models
- Perform developmental test, as appropriate

Figure 4.2.4.F1. Systems Engineering Activities in the Technology Development Phase



SE activities should be integrated with TD phase-specific test and evaluation and logistics and sustainment activities identified in DAG Chapter 9 Test and Evaluation and Chapter 5 Life-Cycle Logistics, respectively.

During the TD phase, the program develops and demonstrates prototype designs to reduce technical risk, validate design approaches, validate cost estimates, and refine requirements. In, addition, the TD phase efforts ensure the level of expertise required to operate and maintain the product is consistent with the force structure. Technology development is an iterative process of maturing technologies and refining user performance parameters to accommodate those technologies that do not sufficiently mature (requirements trades). The Initial Capabilities Document, the Technology Development Strategy (TDS), Systems Engineering Plan (SEP), and draft Capability Development Document (CDD) guide the efforts of this phase.

There are two key technical objectives in the TD phase: technical risk reduction and initial system development activity, culminating in preliminary design. The Systems Engineer in the TD phase manages activities to evaluate prototyped solutions (preferably competitive prototypes) against performance, cost, and schedule constraints to balance the total system solution space. This information can then be used to inform the finalization of the system performance specification as a basis for functional analysis and preliminary design.

Effective systems engineering (SE), applied in accordance with the SEP and gated by technical reviews, reduces program risk, identifies potential management issues in a timely manner, and supports key program decisions. The TD phase provides the Program Manager with a preliminary design and allocated baseline that are realistic and credible.

Roles and Responsibilities

The program office team provides technical management and may employ industry, Government laboratories, the Service science and technology (S&T) community, or Federally Funded Research and Development Centers (FFRDCs)/universities to accomplish specific risk-reduction or prototype tasks as described in the SEP.

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Program Manager focuses on the following TD activities, which rely on and support SE efforts:

- Award TD phase contract(s)
- Provide resources for technical reviews
- Plan and execute the Technology Readiness Assessment (TRA)
- Influence development of the CDD
- Develop the Acquisition Strategy (AS)
- Support pre-EMD review
- Ensure the Government preserves the rights they need consistent with the life-cycle acquisition and support strategy; during TD, proprietary development and design can often lead to issues with data rights (see DAG section 4.3.8. Technical Data Management Process)

In addition to the general roles and responsibilities described in DAG section 4.1.4. Engineering Resources, during this phase it is the Systems Engineer's responsibility to:

- Lead and manage the execution of the technical activities as documented in the SEP
- Plan and execute technical reviews, including the System Requirements Review (SRR), System Functional Review (SFR), and Preliminary Design Review (PDR)
- Measure and track program maturity using technical performance measures, requirements stability, and integrated schedules
- Support award of TD phase contract(s), as necessary
- Balance and integrate key design considerations
- Maintain the Systems Engineering Plan (SEP), including generating the update in support of Milestone B
- Lead initial development of the system to include functional analysis, definition of the functional and allocated baselines, and preliminary design (see DAG sections 4.3.11. Requirements Analysis Process and 4.3.12. Architecture Design Process)
- Support configuration management of the baselines, since they are required in later technical reviews, audits, and test activities (e.g., functional baseline at the

Functional Configuration Audits (FCAs))
- Conduct technical activities in support of the pre-EMD review
- Conduct a rigorous and persistent assessment of technical risk, determine risk mitigation plans, and work with the Program Manager to resource the mitigation plans
- Support the Technology Readiness Assessment (TRA) including creation of the plan, the pre-EMD preliminary TRA, and the TRA final report
- Support requirements management and monitor for unnecessary requirements growth (e.g., derived versus implied requirements)
- Manage interfaces and dependencies

Inputs

Table 4.2.4.T1 summarizes the primary inputs associated with this pre-systems acquisition part of the life cycle (see DoDI 5000.02).

Table 4.2.4.T1. Inputs Associated with TD Phase

Inputs for TD Phase
Draft Capability Development Document (CDD)
Analysis of Alternatives (AoA) Report and AoA Sufficiency Report
Preferred materiel solution • Selection of preferred materiel solution is documented in the ADM
Acquisition Decision Memorandum (ADM) (may contain additional direction)
SEP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report • Attachment to SEP as directed by DTM 11-003
Reliability Growth Curves (RGC) • Attachment to SEP as directed by DTM 11-003
Program Protection Plan (PPP) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection

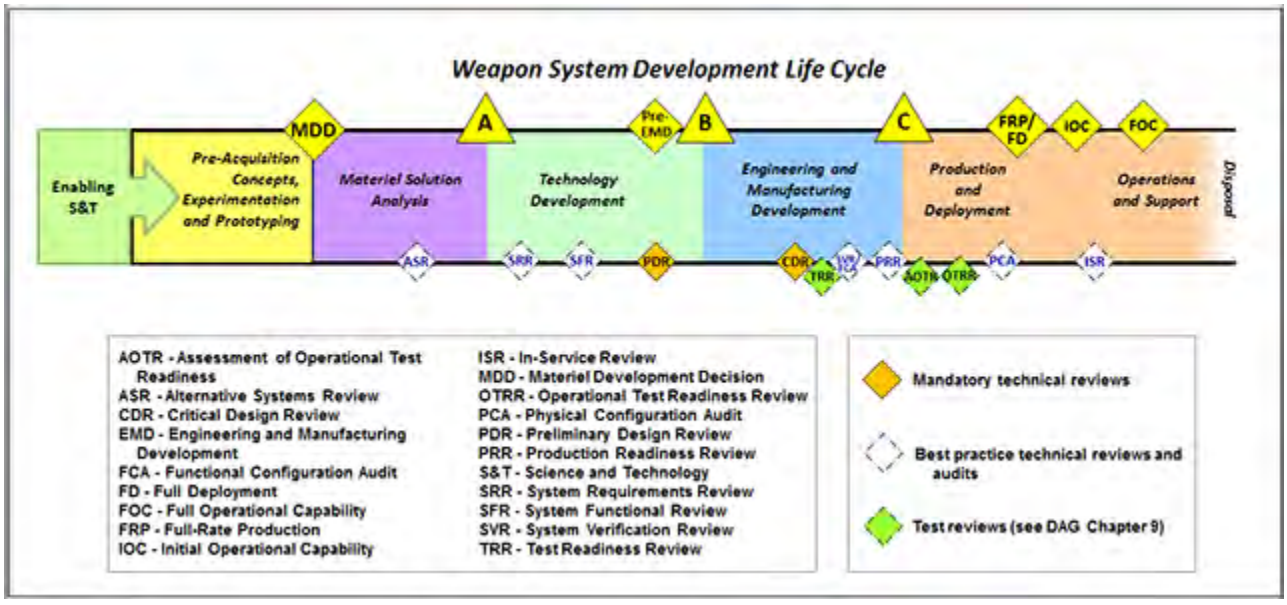
Inputs for TD Phase
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc.
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades
Environment, safety, and occupational health (ESOH) planning
Risk assessment
Consideration of technology issues • DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2
Initial identification of critical technologies • MSA phase may have identified an initial list of critical technologies
Interdependencies / interfaces / memoranda of agreements (MOAs)
Draft system performance specification
Other technical information such as models and simulations generated during the MSA phase
Prototyping strategy • Includes identification of key system elements to be prototyped prior to Milestone B, see DTM 09-027
Affordability Assessment • Affordability targets are established and treated as a Key Performance Parameters (KPPs) at Milestone A • Affordability targets drive engineering trade-offs and sensitivity analyses about capability priorities in the TD phase • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
TDS • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies
Life Cycle Sustainment Plan (LCSP) • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See DAG Chapter 5 Life-Cycle Logistics

Inputs for TD Phase
Test and Evaluation Strategy (TES) • DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Informed advice to the developmental test and evaluation (DT&E) assessments • Includes Early Operational Assessments (EOAs) • See DAG Chapter 9 Test and Evaluation
Draft and final Request for Proposal (RFP)
Security Classification Guide (SCG)
Other analyses • Other prior analytic, prototyping, and/or technology demonstration efforts done by the S&T community. Technology insertion/transition can occur at any point in the life cycle

Activities

The TD phase activities begin when a favorable Milestone A decision has been made (see DAG section 4.2.3. Materiel Solution Analysis Phase) and end with a successful Milestone B decision. Figure 4.2.4.F2 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.4.F2. Weapon System Development Life Cycle



The TD phase addresses a set of critical activities leading to the decision to establish a

program of record. The SE activities provide the technical foundation for this decision. Depending on the nature of the technology development strategy, the order and characteristics of these activities may change. During the TD phase, systems engineers follow comprehensive, iterative processes to accomplish the following:

- **Perform Competitive Prototyping**. As mentioned earlier, prototyping is an engineering technique employed for several reasons. Competitive prototyping (CP) has as a primary objective to acquire more innovative solutions at better value by ensuring competition. At this point in the life cycle, the CP strategy should focus on mitigating key technical risk areas. The program office should have a clear understanding of technical, engineering, and integration risks at Milestone A. Current policy does not require full-up system prototypes; therefore, competitive prototyping may include prototyping critical technologies, system elements, integration of system elements, or full-up prototypes. Because a primary objective of this type of prototyping is to support a follow-on award choice between developers, contract incentives should be aligned to CP strategy goals. Contract goals should require the solutions demonstrated during CP be used in the subsequent PDR/CDR designs. The CP strategy should be identified in the SEP and TDS, tasks specified in RFPs/Task Orders, technically managed by the program office, and included in the TES with specific test objectives.
- **Perform Technology Maturation**. The TDS identifies technologies requiring further maturation before they can be implemented within a solution. Technology maturation involves design, development, integration, and testing. There could be one or more risk areas related to hardware, software, or information technology, and there may be multiple industry contracts/Government efforts for maturing the technology. The TES should stipulate the test and evaluation approach for assessing the results of the technology maturation activities (see DAG Chapter 9 Test and Evaluation ; Chief Developmental Tester). The Systems Engineer participates in the technology readiness assessment (TRA). The TRA focuses only on technology maturity as opposed to engineering and integration risk. DoDI 5000.02 and OSD TRA Guidance provide policy and guidance for TRAs.
- **Perform System Trade Analysis**. The Systems Engineer assesses alternatives with respect to performance, cost, schedule and risk, and makes a recommendation to the Program Manager. The SE assessment should consider the full range of relevant factors, for example affordability targets, technology maturity, development and fielding constraints, and user-identified needs and shortfalls. System trades should be used to inform and shape the CDD and cost and schedule objectives to be documented in the Acquisition Program Baseline (APB).
- **Develop System Architecture.** See DAG section 4.3.12. Architecture Design Process for additional information.
- **Develop Functional Baseline.** See DAG section 4.3.7. Configuration Management Process for additional information.
- **Develop Allocated Baseline.** See DAG section 4.3.7. Configuration Management Process for additional information.

- **Develop Preliminary Design.** See DAG section 4.2.12. Preliminary Design Review for additional information.
- **Develop Allocated Technical Performance Measures (TPMs).** The allocated baseline establishes the first physical representation of the system as subsystem elements with system-level capabilities allocated to subsystem-level technical performance measures.
- **Complete PDR Report.** After the PDR, the Program Manager develops the PDR Report with support from the Systems Engineer. The Program Manager provides the report to the MDA to support a Milestone B decision. The report includes recommended requirements trades based upon an assessment of cost, schedule, performance, and risk.
- **Support pre-EMD review.** The purpose of the MDA-level review is to assess the AS, RFP, and key related planning documents and determine whether program plans are affordable and executable and reflect sound business arrangements. Specific SE attention is given to engineering trades and their relationship to program requirements and risk management.
- **Finalize Documents.** The Systems Engineer updates the SEP and PPP and provides inputs for updating the LCSP, TEMP, and other program documents.

Technical reviews typically conducted in the TD phase are:

- System Requirements Review (SRR) (see DAG section 4.2.10. System Requirements Review)
- System Functional Review (SFR) (see DAG section 4.2.11. System Functional Review)
- Software Specification Review (SSR) for programs with significant software development; a SSR is typically performed before, and in support of, a PDR. The SSR technical assessment establishes the software requirements baseline for the system elements under review (e.g., computer software configuration items (CSCI)) to ensure their preliminary design and ultimately the software solution has a reasonable expectation of being operationally effective and suitable.
- Preliminary Design Review (PDR) mandated (unless formally waived) to confirm the development of the allocated baseline (see DAG section 4.2.12. Preliminary Design Review)

Test activities during the TD phase that depend on SE support and involvement include developmental test and evaluation of system and/or system element prototypes and Early Operational Assessments (EOAs). Developmental Test and Evaluation (DT&E) activities, for example, should be closely coordinated between the engineering and test communities since DT&E activities support:

- Technical risk identification, risk assessment, and risk mitigation;
- Providing empirical data to validate models and simulations; and
- Assessing technical performance and system maturity (see DAG Chapter 9 Test and Evaluation).

Outputs and Products

The technical outputs identified in Table 4.2.4.T2 are some of the inputs necessary to support SE activities in the EMD phase. The outputs should support the technical recommendation at Milestone B that an affordable solution has been found for the identified need with acceptable risk, scope, and complexity. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 4.2.4.T2. Technical Outputs Associated with TD Phase

Technical Outputs from TD Phase
Informed advice to CDD
Informed advice to Acquisition Decision Memorandum (ADM) and 2366a certification
Preliminary system design • Updated functional and allocated baselines • Associated technical products including associated design and management decisions
SEP (updated) • If programs enter the acquisition life cycle at Milestone B, this is their initial SEP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Updated Integrated Master Plan (IMP), Integrated Master Schedule (IMS), and memoranda of agreement (MOAs)/ memoranda of understanding (MOUs)
RAM-C Report (updated) • Attachment to SEP as directed by DTM 11-003; if programs enter the acquisition life cycle at Milestone B, this is their initial RAM-C Report
RGC (updated) • Attachment to SEP and TEMP as directed by DTM 11-003
PPP (updated) • If programs enter the acquisition life cycle at Milestone B, this is their initial PPP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc.

Technical Outputs from TD Phase
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades • Interdependencies defined
Environment, safety, and occupational health (ESOH) analyses • Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule
Assessment of technical risk • Include SoS risks associated with governance, interdependencies, and complexity
Consideration of technology issues • See DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2.
Technology Readiness Assessment (TRA) • TRA Plan • Confirmation at the end of TD phase that critical technologies have been demonstrated in a relevant environment • Preliminary TRA required at pre-EMD review • TRA final report
Interdependencies / interfaces / memoranda of agreement (MOAs) • Understanding of the unique program interdependencies, interfaces, and associated MOAs
Updated system performance specification
System preliminary design including functional baseline and allocated baseline
Other technical information such as models and simulations generated during the TD phase
Prototyping strategy and results of TD prototyping activities • Including identification of key system elements to be prototyped in EMD Phase and documented in the Acquisition Strategy (AS)
Preliminary Design Review (PDR) Report and Post PDR Assessment (produced by DASD(SE) for MDAPs) • See DoDI 5134.16 • See DTM 09-025 • See DAG Chapter 10 Decisions, Assessments, and Periodic Reporting

Technical Outputs from TD Phase
Informed advice to Acquisition Program Baseline (APB) • APB inputs include the SE affordability assessments, schedule inputs, and performance inputs
Establishes technical information that is the basis of the cost analysis requirements description (CARD) and manpower estimates
Informed advice to Affordability Assessment • Affordability targets continue to be treated as KPPs at Milestone B; results of engineering trade-off analyses showing how the program established a cost-effective design point for cost/affordability drivers • Should cost goals defined at Milestone B to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability • Value engineering results, as appropriate (see DAG section 4.3.19.3. Value Engineering) • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
Informed advice to Acquisition Strategy (AS) • Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule, and risks • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies
Informed advice to LCSP (updated) • System support and maintenance objectives and requirements established; updated will cost values and affordability targets as documented in the Life-Cycle Sustainment Plan (LCSP), including Informed advice to manpower estimates • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See DAG Chapter 5 Life-Cycle Logistics
Initial Information Support Plan (ISP) • See DAG Chapter 7 Acquiring Information Technology, Including National Security Systems
Informed advice to Test and Evaluation Master Plan (TEMP) • DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Early developmental test and evaluation (DT&E) assessments, including Early Operational Assessments (EOAs) • See DAG Chapter 9 Test and Evaluation

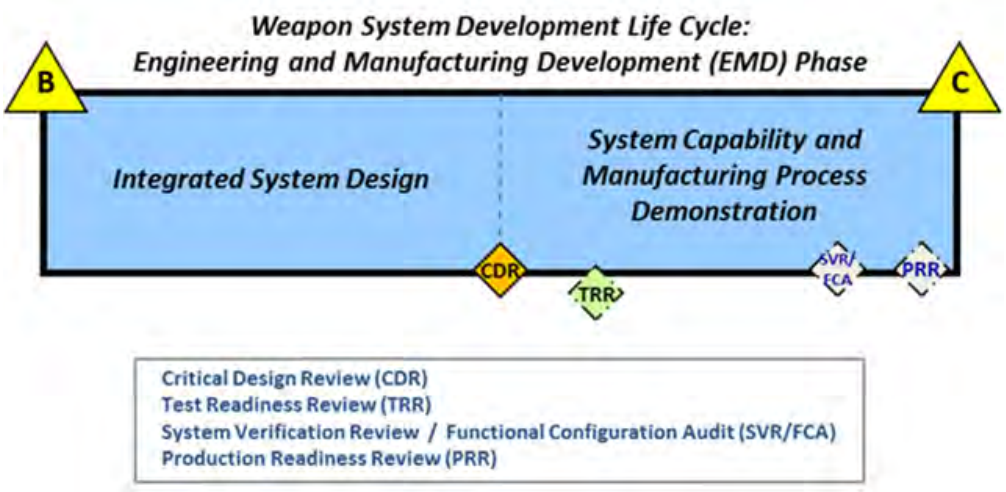
Technical Outputs from TD Phase
Informed advice to draft and final Request for Proposal (RFP) • Informed advice including system specification, SOW, CDRLs, and source selection criteria

4.2.5. Engineering and Manufacturing Development Phase

4.2.5. Engineering and Manufacturing Development Phase

The primary objective of the Engineering and Manufacturing Development (EMD) phase is to develop the product baseline, verify it meets the system functional and allocated baselines, and transform the preliminary design into a producible design, all within the schedule and cost constraints of the program. Systems engineering (SE) activities support development of the detailed design, verification that requirements are met, reduction in system-level risk, and assessment of readiness to begin production and/or deployment. The core SE activities support the two efforts associated with the EMD phase as defined in DoDI 5000.02 for weapon systems acquisition and identified in figure 4.2.5.F1: integrated system design and system capability and manufacturing process demonstration.

Figure 4.2.5.F1. Systems Engineering Activities in the Engineering and Manufacturing Development Phase



Primary SE focus areas in EMD include:

- Complete the detailed build-to design of the system
- Establish the product baseline
- Conduct integration and tests of system elements and the system (where

feasible)
- Demonstrate system maturity and readiness to begin production for operational test and /or deployment and sustainment activities

The EMD phase includes technical assessment and control efforts, including value engineering techniques described in DAG section 4.3.19.3. Value Engineering, to effectively manage risks and increase confidence in meeting system performance, schedule, and cost goals. SE activities should be integrated with EMD phase-specific test and evaluation and logistics and sustainment activities identified in DAG Chapter 9 Test and Evaluation and Chapter 5 Life-Cycle Logistics, respectively. The planning, scheduling, and conduct of event-driven technical reviews (Critical Design Review (CDR), Functional Configuration Audit (FCA), System Verification Review (SVR), and Production Readiness Review (PRR)) are vital to provide key points for assessing program maturity and the effectiveness of risk-reduction strategies.

A well-planned EMD phase Systems Engineering Plan (SEP) builds on the results of previous activities and significantly increases the likelihood of a successful program compliant with the approved Acquisition Program Baseline (APB).

Implementing the technical planning as defined in the approved SEP guides the execution of the complex and myriad tasks associated with completing the detailed design and integration, and supports developmental test and evaluation activities. The SEP also highlights the linkage between Technical Performance Measures (TPM), risk management, and earned-value management activities to support tracking of cost growth trends. Achieving predefined EMD technical review criteria provides confidence that the system meets stated performance requirements (including interoperability and supportability requirements) and that design and development have matured to support the initiation of the Production and Deployment (P&D) phase.

Roles and Responsibilities

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Program Manager focuses on the following EMD activities, which rely on and support SE efforts:

- Conduct activities in support of the EMD contract award
- Resource and conduct event-driven CDR, FCA, SVR, and PRR, and assess whether review criteria are met
- Establish and manage the initial product baseline established at the CDR
- Determine path forward on all major (Class I) baseline changes (see DAG section 4.3.7. Configuration Management Process for definition of Class I)
- Accept system deliveries (i.e., DD-250), as appropriate

In addition to the general roles and responsibilities described in DAG section 4.1.4 Engineering Resources, during this phase it is the Systems Engineer's responsibility to:

- Manage the system design to satisfy the operational requirements within the constraints of cost and schedule and to evaluate the system design, identify deficiencies, and make recommendations for corrective action
- Conduct or support the technical evaluation in support of source selection for the EMD contract award
- Maintain requirements traceability and linkage to the initial product baseline
- Conduct event-driven technical reviews, advising the Program Manager on review criteria readiness
- Lead preparation and conduct of technical reviews
- Track and report major (Class I) baseline changes and recommend the path forward in accordance with the Configuration Management (CM) process (see DAG section 4.3.7. Configuration Management Process for definition of Class I)
- Support determination of production rates and delivery schedules
- Support test and evaluation activities: identify system evaluation targets driving system development and support operational assessments as documented in the Test and Evaluation Master Plan (TEMP) (see DAG Chapter 9 Test and Evaluation)
- Align the SEP with the TEMP on SE processes, methods, and tools identified for use during test and evaluation
- Analyze deficiencies discovered from operational assessments and verification methods (developmental test and evaluation); develop and implement solutions to including, but not limited to, rebalancing of system requirements
- Support logistics and sustainment activities as documented in the Life-Cycle Sustainment Plan (LCSP) (see DAG Chapter 5 Life-Cycle Logistics)
- Maintain the SEP including generating the update in support of Milestone C
- Ensure manufacturing process development and maturation efforts
- Develop approaches and plans to verify mature fabrication and manufacturing processes and determine manufacturing readiness (see the Manufacturing Readiness Level (MRL) Deskbook as one source for assessing manufacturing readiness)
- Conduct a rigorous production risk assessment and determine risk mitigation plans
- Identify system design features that enhance producibility (efforts usually focus on design simplification, fabrication tolerances, and avoidance of hazardous materials)
- Conduct producibility trade studies to determine the most cost-effective fabrication and manufacturing process
- Assess Low-Rate Initial Production (LRIP) feasibility within program constraints (may include assessing contractor and principal subcontractor production experience and capability, new fabrication technology, special tooling, and production personnel training requirements)
- Identify long-lead items and critical materials
- Support update to production costs as a part of life-cycle cost management
- Continue to support the configuration management process to control changes to the product baseline during test and fielding

Inputs

Table 4.2.5.T1. summarizes the primary inputs associated with this systems acquisition part of the life cycle (see DoDI 5000.02).

Table 4.2.5.T1. Inputs Associated with EMD Phase

Inputs for EMD Phase
Capability Development Document (CDD)
Acquisition Decision Memorandum (ADM) (may contain additional direction)
SEP • If programs enter the acquisition life cycle at Milestone B, this is their initial SEP • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report • Attachment to SEP as directed by DTM 11-003; if programs enter the acquisition life cycle at Milestone B, this is their initial RAM-C Report
Reliability Growth Curves (RGCs) • Attachment to TEMP as directed by DTM 11-003
Program Protection Plan (PPP) • If programs enter the acquisition life cycle at Milestone B, this is the initial PPP • Includes Security Classification Guide (SCG), Counterintelligence Support Plan, Criticality Analysis, Anti-Tamper Plan, and Acquisition Information Assurance (IA) Strategy • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc.
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades • Interdependencies defined

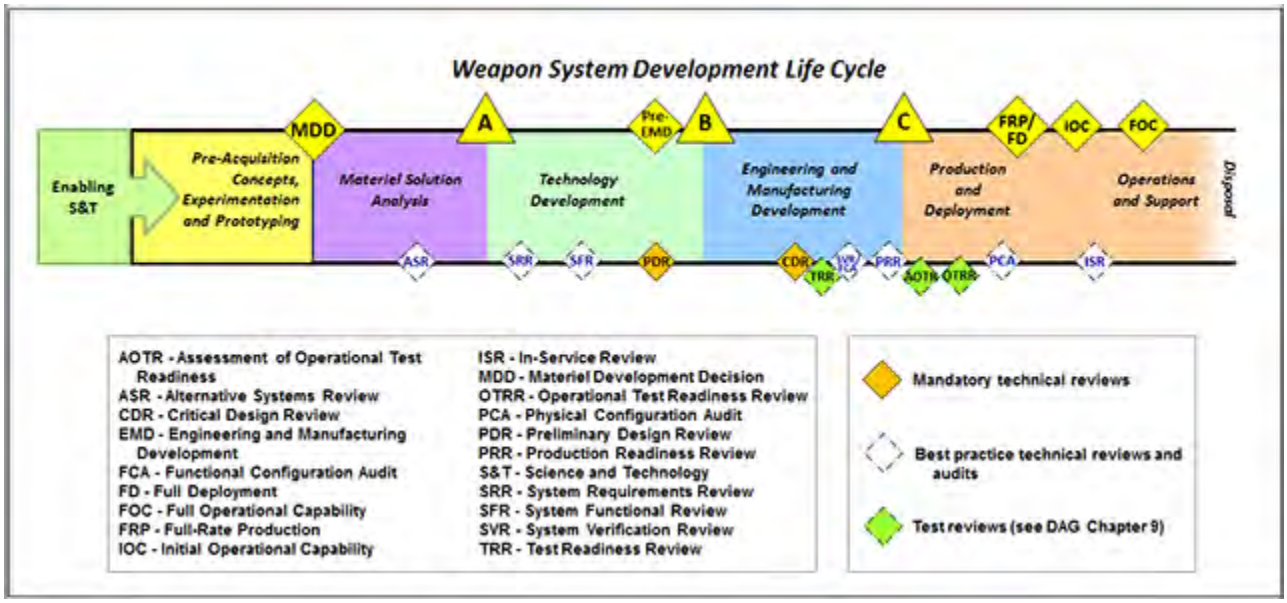
Inputs for EMD Phase
Environment, safety, and occupational health (ESOH) analyses • Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule
Assessment of technical risk
Consideration of technology issues • See DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2
Technology Readiness Assessment (TRA) • Confirmation that critical technologies have been demonstrated in a relevant environment
Interdependencies / interfaces / memoranda of agreement (MOAs)
System performance specification including verification matrix
Other technical information such as models and simulations generated during the TD phase
Prototyping strategy
System Threat Assessment Report (STAR)
Acquisition Program Baseline (APB)
Affordability Assessment • Affordability targets treated as KPPs; results of engineering trade-off analyses show cost/schedule/performance trade space around affordability drivers • Should cost goals designed to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
Acquisition Strategy (AS) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies
Life-Cycle Sustainment Plan (LCSP) (updated) • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See also DAG Chapter 5 Life-Cycle Logistics
Initial Information Support Plan (ISP) • See DAG Chapter 7 Acquiring Information Technology, Including National Security Systems

Inputs for EMD Phase
Test and Evaluation Master Plan (TEMP) • System Test Objectives • See DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Informed advice to the developmental test and evaluation (DT&E) planning including Operational Assessments (OAs) • System test objectives • See DAG Chapter 9 Test and Evaluation
Draft and final Request for Proposal (RFP)
Security Classification Guide (SCG) (updated)
Other analyses • Other prior analytic, prototyping, and/or technology demonstration efforts performed by the S&T community. Technology insertion/transition can occur at any point in the life cycle

Activities

The EMD phase activities begin when a favorable Milestone B decision has been made (see DAG section 4.2.4. Technology Development Phase) and end with a successful Milestone C decision. Figure 4.2.5.F2 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.5.F2. Weapon System Development Life Cycle



SE activities to support the integrated system design effort include:

- Realization of the system architecture
- Performance of system element trade-offs
- Use of prototypes to mature system designs and drawings. If the program strategy includes competitive development, this may include competitive prototyping during the EMD phase.
- Development of the initial product baseline and a stable design that conforms to program cost, schedule, and performance requirements
- Support for the establishment of the developmental test and evaluation environment and associated resources (e.g., people, equipment, test cases, and test ranges)
- Support of materiel readiness and logistical support efforts
- Preparation for production by identifying critical manufacturing processes, key product characteristics, and any manufacturing risks

SE activities to support the system capability and manufacturing process demonstration effort include:

- Build, integrate, and test system elements
- Fabricate and assemble the system elements and system to the product baseline
- Identify the process to proactively manage and mitigate Diminishing Manufacturing Sources and Material Shortages (DMSMS) issues in future life-cycle phases
- Integrate the system and verify compliance with the functional and allocated baselines through developmental test and evaluation (DT&E) efforts (see DAG Chapter 9 Test and Evaluation for more on DT&E)
- Determine the root cause of problems, identify corrective actions, and manage to completion
- Address problem/failure reports through the use of a comprehensive data-collection approach such as Failure Reporting, Analysis and Corrective Action System (FRACAS)
- Refine the initial product baseline and support the development of the Capability Production Document (CPD)
- Complete producibility activities supporting manufacturing readiness or implementation and initial deployment activities for information systems
- Support initiation of materiel readiness and logistical support activities including fielding options and training development
- Perform Environment, Safety, and Occupational Health (ESOH) risk management analyses and ESOH risk acceptance
- Produce NEPA/EO 12114 documentation
- Perform corrosion risk assessment
- Complete certifications as appropriate (see DAG section 4.1.5. Certifications)

Technical reviews and audits typically conducted in EMD:

- Critical Design Review (CDR) (mandated, establishes initial product baseline, see DAG section 4.2.13. Critical Design Review)
- System Verification Review/Functional Configuration Audit (SVR/FCA) (see DAG section 4.2.14. System Verification Review/Functional Configuration Audit)
- Production Readiness Review (PRR) (DAG section 4.2.15. Production Readiness Review)

Test activities during the EMD phase that depend on SE support and involvement include Test Readiness Reviews (TRRs), Developmental Test and Evaluation (DT&E), and Operational Assessments (OAs). The Systems Engineer, in collaboration with the Chief Developmental Tester, should identify system evaluation targets driving system development and support operational assessments as documented in the Test and Evaluation Master Plan (TEMP). Associated SE activities and plans should be in the SEP (see DAG section 4.1.2. Systems Engineering Plan, 4.2.8. Technical Reviews and Audits Overview, and DAG Chapter 9 Test and Evaluation).

Outputs and Products

The technical outputs and products identified in Table 4.2.5.T2 and are some of the inputs necessary to support SE processes in the P&D phase. They should support the technical recommendation at Milestone C that manufacturing processes are mature enough to support Low-Rate Initial Production (LRIP) and generate production-representative articles for operational test and evaluation (OT&E). Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 4.2.5.T2. Technical Outputs Associated with EMD Phase

Technical Outputs from EMD Phase
Informed advice to CPD
Informed advice to Acquisition Decision Memorandum (ADM) and 2366b certification
Verified system • Updated functional, allocated, and product baselines; verified production processes, and verification results/ decisions • Associated technical products including associated design and management decisions
SEP (updated) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Updated IMP, IMS, and MOAs/MOUs
RAM-C Report (updated) • Attachment to SEP as directed by DTM 11-003

Technical Outputs from EMD Phase
RGC (updated) • Attachment to TEMP as directed by DTM 11-003
PPP (updated) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011) • See DAG Chapter 13 Program Protection
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc.
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades • Interdependencies updated
ESOH analyses • Updated Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/E.O. 12114 Compliance Schedule
Assessment of technical risk • Risk assessment identifying mitigation plans for acceptable risks to allow the program to initiate production, deployment, and operational test and evaluation activities • Update system of systems (SoS) risks associated with governance, interdependencies, and complexity
Consideration of technology issues • See DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2
Manufacturing readiness • Assessment of manufacturing readiness supports MS C and initiation of production • Manufacturing processes have been effectively demonstrated in a pilot line environment
Interdependencies / interfaces / memoranda of agreement (MOAs) • Understanding of the unique program interdependencies, interfaces, and associated MOAs

Technical Outputs from EMD Phase
System performance specification (updated if necessary) including verification matrix • System element specifications including verification matrix
Product baseline
Other technical information such as models and simulations generated during the EMD phase
Results of EMD prototyping activities
Manufacturing prototyping activities support P&D phase
Post-Critical Design Review (CDR) Assessment (produced by DASD(SE) for Major Defense Acquisition Programs)
Informed advice to APB • Updated will cost values and affordability targets as documented in the Acquisition Program Baseline and Acquisition Strategy
Establishes technical information that is the basis of the updates to the Cost Analysis Requirements Description (CARD) and manpower estimates
Informed advice to Affordability Assessment • Should cost goals updated to achieve efficiencies and control unproductive expenses without sacrificing sound investment in product affordability. • Value engineering results, as appropriate. See DAG section 4.3.19.3. Value Engineering. • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
Manufacturing, performance, and quality metrics critical to program success are identified and tracked • 30%, 60%, and 100% completed manufacturing drawings
Production budget/cost model validated and resources considered sufficient to support LRIP and FRP • Inputs to MS C, LRIP, and FRP DR
Informed advice to Acquisition Strategy (AS) • Informed advice on engineering approaches and strategies, external dependencies, resource requirements, schedule, and risks • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies

Technical Outputs from EMD Phase
Informed advice to LCSP (updated) • System Support and Maintenance Objectives and Requirements established • Updated will cost values and affordability targets as documented in the LCSP, including Informed advice to manpower estimates • Confirmation of logistics and sustainment needs (i.e., facilities, training, support equipment) and implementation supporting initial deployment efforts • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See also DAG Chapter 5 Life-Cycle Logistics
ISP of Record • See DAG Chapter 7 Acquiring Information Technology, Including National Security Systems
Informed advice to TEMP (updated) • System test objectives • See DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Informed advice to the DT&E assessments • System test objectives • See DAG Chapter 9 Test and Evaluation
Informed advice to draft & final RFP for LRIP • Informed advice including system specification, SOW, CDRLs, and source selection criteria

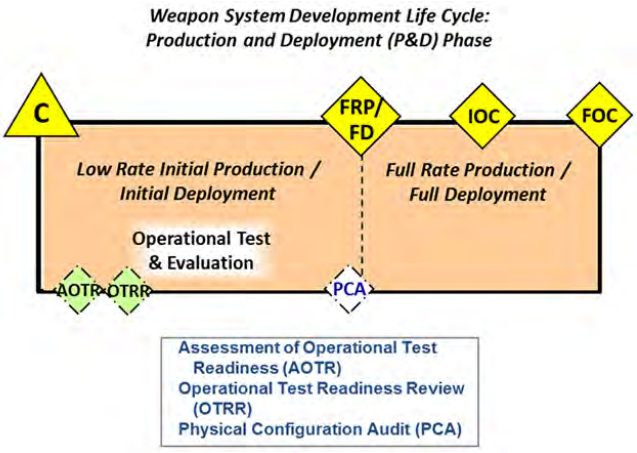
4.2.6. Production and Deployment Phase

4.2.6. Production and Deployment Phase

The objective of the Production and Deployment (P&D) phase is to validate the product design and to deliver the quantity of systems required for full operating capability, including all enabling system elements and supporting material and services. Systems engineering (SE) in P&D delivers the final product baseline as validated during operational testing, and supports deployment and transition of capability to all end users, the warfighters, and supporting organizations. SE activities, for example maintenance approach, training, and technical manuals, should be integrated with P&D phase-specific test and evaluation and logistics and sustainment activities identified in DAG Chapter 9 Test and Evaluation and Chapter 5 Life-Cycle Logistics, respectively. This phase typically has several major efforts as shown in Figure 4.2.6.F1: Low-Rate Initial Production (LRIP), Operational Test and Evaluation (OT&E), Full-Rate Production (FRP) and Full Deployment (FD), and deployment of capability in support of the Initial

and Full Operational Capabilities. The Full-Rate Production Decision Review (FRP DR) and/or Full Deployment Decision Review (FD DR) serves as a key decision point between LRIP (and OT&E) and FRP/FD.

Figure 4.2.6.F1. Production and Deployment Phase



Manufacturing development should be complete at Milestone C, but improvements or redesigns may require unanticipated, additional manufacturing process development and additional testing (e.g., delta qualification or delta first article test). For example, it may be discovered that changing the product design may provide enhancements in manufacturing or other supporting processes. At the conclusion of LRIP, all manufacturing development should be completed, with no significant manufacturing risks carried into FRP. The dynamic nature of the varied production elements requires a proactive approach to mitigate emerging risks.

Readiness for OT&E is a significant assessment of a system's maturity (see DAG Chapter 9 Test and Evaluation). The Systems Engineer plays a key role in ensuring systems are ready to enter OT&E. Scarce resources are wasted when an operational test is halted or terminated early because of technical problems that should have been resolved before the start of OT&E.

During deployment, units attain Initial Operational Capability (IOC), then Full Operational Capability (FOC).

Besides ensuring a successful FOC, the SE activities:

- Mature manufacturing, production, and deployment procedures
- Respond to deficiencies and develop corrective actions
- Support validation of system performance associated with OT&E
- Validate the production configuration prior to FRP / FD

Roles and Responsibilities

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Program Manager focuses on the following P&D activities, which rely on and support SE efforts:

- Conduct activities in support of the production contract award(s)
- Resource and conduct event-driven technical reviews (including the Physical Configuration Audit (PCA), Post Implementation Review (PIR), and FRP and/or FD DR) and ensure that criteria are met
- Manage and control the final product baseline
- Manage risks, in particular the manufacturing, production, and deployment risks
- Accept system deliveries (i.e., DD-250)

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Systems Engineer is responsible to:

- Analyze deficiencies discovered from OT&E, acceptance tests, production reports, and maintenance reports and provide correction actions
- Conduct rigorous production risk assessments; plan and resource effective risk mitigation actions
- Continue conducting producibility trade studies to determine the most cost-effective fabrication/manufacturing process
- Develop approaches and plans to validate fabrication/manufacturing processes
- Assess full-rate production feasibility within program constraints. This may include assessing contractor and principal subcontractor production experience and capability, new fabrication technology, special tooling, and production personnel training requirements
- Identify long-lead items and critical materials; plan for obsolescence and implement DMSMS measures to mitigate impacts to production and sustainment
- Update production costs as a part of life-cycle cost management
- Support updates to the production schedules
- Support technical reviews and production decisions
- Support materiel readiness and logistical activities, including fielding and training
- Continue to support the Configuration Management Board to control changes to the product baseline during test and fielding

- Update and maintain system certifications and interfaces with external systems, as necessary

Inputs

Table 4.2.6.T1 summarizes the primary inputs associated with this systems acquisition part of the life cycle.

Table 4.2.6.T1. Inputs Associated with P&D Phase

Inputs for P&D Phase
Capability Production Document (CPD)
Acquisition Decision Memorandums (ADM) associated with Milestone C, LRIP, and FRP DR and FD DR • ADMs may contain additional direction • Milestone C may not coincide with LRIP • FRP DR and FD DR ADMs are issued during P&D phase
SEP • Updated functional, allocated, and product baselines; verified and validated production processes, and validation results / decisions • Updated technical products including associated design and management decisions • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG section 4.1.2 Systems Engineering Plan
Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report • Attachment to SEP as directed by DTM 11-003
Reliability growth curves (RGCs) • Attachment to TEMP as directed by DTM 11-003
PPP • Updated at FRP DR and/or FD DR • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Trade study results • Results could include knees-in-the-curves sensitivity analyses, product selections, etc. • P&D phase trade studies may support manufacturing or other system mods (technology insertion, technology refresh, etc.)

Inputs for P&D Phase
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades
Environment, Safety, and Occupational Health (ESOH) analyses • Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule
Risk assessment • Risk mitigation plans • Acceptable risks for achieving Initial Operational Capability (IOC) and Full Operational Capability (FOC) • Updated Risk Management Plan to reflect change from acquisition to deployment and initiation of sustainment activities
Consideration of technology issues • See DoDI 5000.02, Enclosure 4, Tables 2-1 and 2-2
Manufacturing readiness • Assessment of manufacturing readiness supports MS C and initiation of production
Interdependencies / interfaces / memoranda of agreement (MOAs) • Understanding of the unique program interdependencies, interfaces, and associated MOA
System performance specification (updated if necessary) including verification matrix • System element specifications (updated if necessary) including verification matrix
Manufacturing, performance and quality metrics critical to program success are identified and tracked • 30%, 60%, and 100% completed manufacturing drawings
Initial product baseline
Product acceptance test
Other technical information such as models and simulations generated during the EMD phase
Results of EMD prototyping activities
Manufacturing prototyping activities supporting P&D phase
System Threat Assessment Report (STAR)
Acquisition Program Baseline (APB)

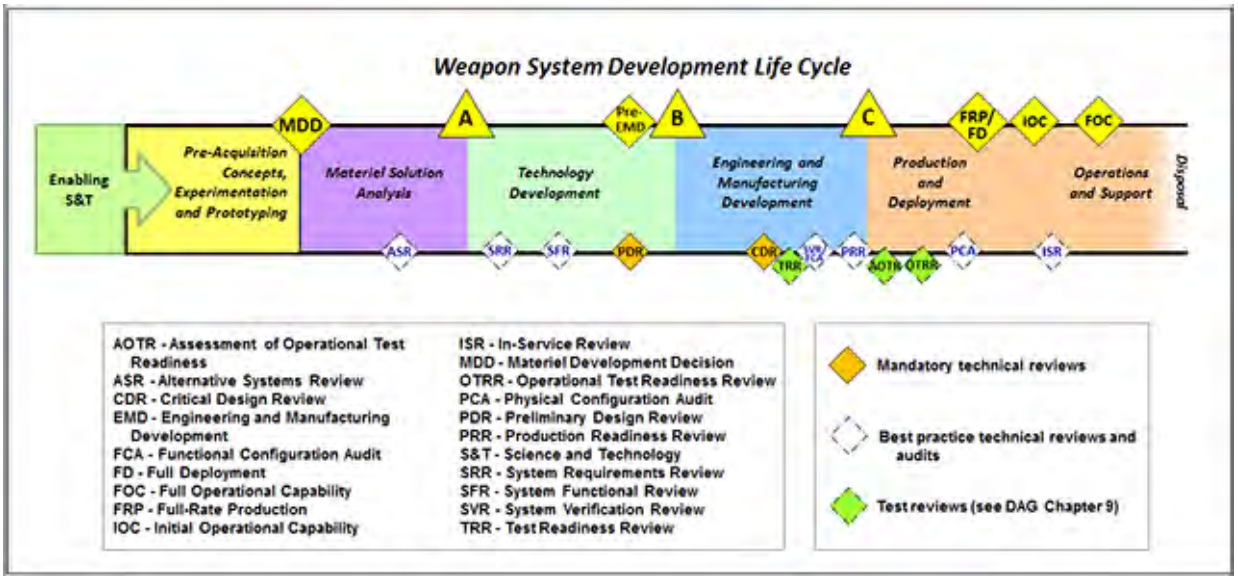
Inputs for P&D Phase
Affordability Assessment • Affordability targets treated as KPPs • Should cost goals to achieve efficiencies and control unproductive expenses • Updated will cost values and affordability targets as documented in the Life-Cycle Sustainment Plan (LCSP), including informed advice to manpower estimates • Value engineering results, as appropriate (see DAG section 4.3.19.3. Value Engineering) • See DAG Chapter 3 Affordability and Life-Cycle Resource Estimates
Supply chain sources
Updated Manufacturing processes
Production budget/cost model validated and resources considered sufficient to support LRIP and FRP
Acquisition Strategy (AS) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • See DAG Chapter 2 Program Strategies
LCSP • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See DAG Chapter 5 Life-Cycle Logistics
Human Systems Integration (HSI) analyses • Manpower, personnel, and training (MPT) requirement updates • Refinement of HSI inputs to specifications, human system interfaces design, multi-domain verification, testing, and usability evaluations • See DAG Chapter 6 Human Systems Integration
TEMP • System test objectives • See DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Developmental test and evaluation (DT&E) assessments • System test objectives • See DAG Chapter 9 Test and Evaluation
Draft and final RFP
Security Classification Guide (SCG)
Information Support Plan (ISP) of Record • See DAG Chapter 7 Acquiring Information Technology, Including National Security Systems

Inputs for P&D Phase
Other analyses • Other prior analytic, prototyping, and/or technology demonstration efforts completed by the science and technology (S&T) community; technology insertion/transition can occur at any point in the life cycle

Activities

The P&D phase SE activities begin when a favorable Milestone C decision has been made (see DAG section 4.2.5. Engineering and Manufacturing Development Phase) and end when FOC is achieved. Figure 4.2.6.F2 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.6.F2. Weapon System Development Life Cycle



SE activities that occur throughout the P&D phase include:

- Provide technical support to prepare for the Operations and Sustainment (O&S) phase, reviewing and providing inputs on the maintenance approach, acquisition strategy, training, and technical manuals
- Determine root cause of problems, identify corrective actions, and manage to completion
- Analyze system deficiencies generated during OT&E, acceptance testing, production, and deployment
- Address problem/failure reports through the use of a comprehensive data collection approach like a Failure Reporting, Analysis and Corrective Action System (FRACAS)
- Manage and control of configuration updates (hardware, software, and

specifications) to the product baseline
- Re-verify and validate production configuration

SE provides inputs to OT&E readiness assessments including:

- Results of prior DT&E
- Analysis of the system's progress in achieving performance metrics (see DAG section 4.3.4. Technical Assessment Process)
- Assessment on satisfaction of approved OT&E entrance criteria
- Assessment of technical risk
- Assessment of software maturity and status of software trouble reports
- Identification of any potential design constraints affecting the system's expected performance during OT&E

In both the Production and Deployment and O&S phases the Systems Engineer should identify and plan for potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS)). DMSMS problems are an increasing concern as the service lives of DoD weapon systems are extended and the product life cycle for high-technology system elements decreases.

The PCA is a SE audit typically conducted in the P&D phase (see DAG section 4.2.16. Physical Configuration Audit for additional information regarding the PCA).

Test activities during the P&D phase that depend on SE support and involvement include the Assessment of Operational Test Readiness (AOTR) for MDAPs, Operational Test Readiness Reviews (OTRRs), initial and follow-on OT&E (IOT&E and FOT&E), and live-fire test and evaluations (LFT&E), as appropriate (see DAG Chapter 9 Test and Evaluation). In addition, any corrective actions or design changes implemented in response to test identified deficiencies require additional regression testing.

The Systems Engineer, in collaboration with the Chief Developmental Tester, should identify technical support needed for operational assessments and document in the Test and Evaluation Master Plan (TEMP). Associated SE activities and plans should be in the SEP (see DAG section 4.1.2. Systems Engineering Plan, 4.2.8. Technical Reviews and Audits Overview, and DAG Chapter 9 Test and Evaluation).

Outputs and Products

The technical outputs and products from the P&D phase identified in Table 4.2.6.T2 are some of the inputs necessary to support SE processes in the O&S phase. They should support the program's transition into full operations and sustainment. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 4.2.6.T2. Technical Outputs Associated with P&D Phase

Technical Outputs from P&D Phase
Informed advice to CPD Update • CPD may be updated to justify system enhancements and modifications from the P&D phase
Informed advice to ADM
Updated IMP, IMS, and MOAs/MOUs
Validated system • Updated functional, allocated, and product baselines; verified and validated production processes, and validation results / decisions • Associated technical products including associated design and management decisions
PPP (updated) • Updated at FRP DR and/or FD DR • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Trade study results • P&D Phase trade studies may support manufacturing or other system mods (technology insertion, technology refresh, etc.)
Assumptions and constraints • Rationale for all assumptions, constraints, and basis for trades
ESOH analyses • Updated Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) and NEPA/EO 12114 Compliance Schedule
Assessment of technical risk (updated) • Risk assessment identifying mitigation plans, acceptable risks for achieving FOC • Updated Risk Management Plan (RMP) to reflect change from acquisition to sustainment
Interdependencies / interfaces / memoranda of agreement (MOAs) • Understanding of the unique program interdependencies, interfaces, and associated MOA
System performance specification (updated if necessary) including verification matrix; system element specifications (updated if necessary) including verification matrix
Manufacturing and production metrics
PCA results and an updated product baseline
Acceptance test data to assess product conformance and to support DD250 of end items
Other technical information such as models and simulations generated during the P&D phase

Technical Outputs from P&D Phase
Technical information that is the basis of the updates to the Cost Analysis Requirements Description (CARD) and manpower estimates
Industrial base capabilities; updated manufacturing processes and supply chain sources
Informed advice to Life-Cycle Sustainment Plan (LCSP) • Updated at FRP DR and/or FDDR • Updated will cost values and affordability targets as documented in the LCSP, including informed advice to manpower estimates • Value engineering results, as appropriate (see DAG section 4.3.19.3. Value Engineering) • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • See DAG Chapter 5 Life-cycle Logistics
Human Systems Integration (HSI) analyses • Final manpower and personnel requirements • Training program implementation • HSI participation in Engineering Change Proposal (ECP) process • See DAG Chapter 6 Human Systems Integration
Informed advice to TEMP (updated) • System Test Objectives • DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Operational Test and Evaluation (OT&E) Assessments/Reports • System Test Objectives • See DAG Chapter 9 Test and Evaluation
Draft and final RFP(s) for production and SE support to O&S activities

4.2.7. Operations and Support Phase

4.2.7. Operations and Support Phase

The objective of the Operations and Support (O&S) phase is to execute a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its total life cycle. Planning for this phase begins in the Materiel Solution Analysis (MSA) phase, matures through the Technology Development (TD) and Engineering and Manufacturing Development (EMD) phases, and is documented in the Life-Cycle Sustainment Plan (LCSP). Systems engineering (SE) in the O&S phase assesses whether the fielded system and enabling system elements continue to provide the needed capability in a safe, sustainable, and cost-effective manner. SE efforts consist of data collection, assessment, and corrective action cycles to maintain a system's operational suitability and operational

effectiveness.

Sustainment activities supporting system operations begin in this phase and should address two major efforts: life-cycle sustainment and disposal. SE efforts during life-cycle sustainment include Environment, Safety, and Occupational Health (ESOH) assessments, technology refresh, functionality modification, and life-extension modifications.

When the system no longer provides an effective or efficient capability to the warfighter, the Department should make an informed decision to either modify or dispose of it. However, a related proactive aspect in the Production and Deployment and O&S phases is engineering analysis to identify potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS)). DMSMS problems are an increasing concern as the service lives of DoD weapon systems are extended and the product life cycle for high-technology system elements decreases (see DAG section 4.3.18.8 Diminishing Manufacturing Sources and Material Shortages).

Roles and Responsibilities

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Program Manager focuses on the following O&S activities, which rely on and support SE efforts:

- Work with the user to document performance and sustainment requirements in performance agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities
- Employ effective Performance-Based Life-Cycle Product Support implementation and management
- Maintain operational readiness
- Follow acquisition program practices for major modifications or Service Life Extension Program (SLEP)

In addition to the general responsibilities identified in DAG section 4.1.4. Engineering Resources, the Systems Engineer is responsible for the following tasks:

- Refine the maintenance program to minimize total life-cycle cost while achieving readiness and sustainability objectives
- Assess end-user feedback and conduct engineering investigations as required
- Lead teams to translate end-user feedback into corrective action plans and recommend technical changes
- Develop and implement approved system proposed changes to ensure end-user needs continue to be met
- Conduct ESOH risk assessments and maintain oversight of critical safety item supply chain management
- Conduct analysis to identify and mitigate potential obsolescence impacts (i.e., Diminishing Manufacturing Sources and Material Shortages (DMSMS))

- Support implementation of follow-on development efforts in response to formal decisions to extend the weapon system's service life (SLEP) or to initiate a major modification (may be treated as a stand-alone acquisition program)
- Update and maintain system certifications and external SoS interfaces

Inputs

Table 4.2.7.T1 summarizes the primary inputs associated with this sustainment part of the life cycle.

Table 4.2.7.T1. Inputs Associated with O&S Phase

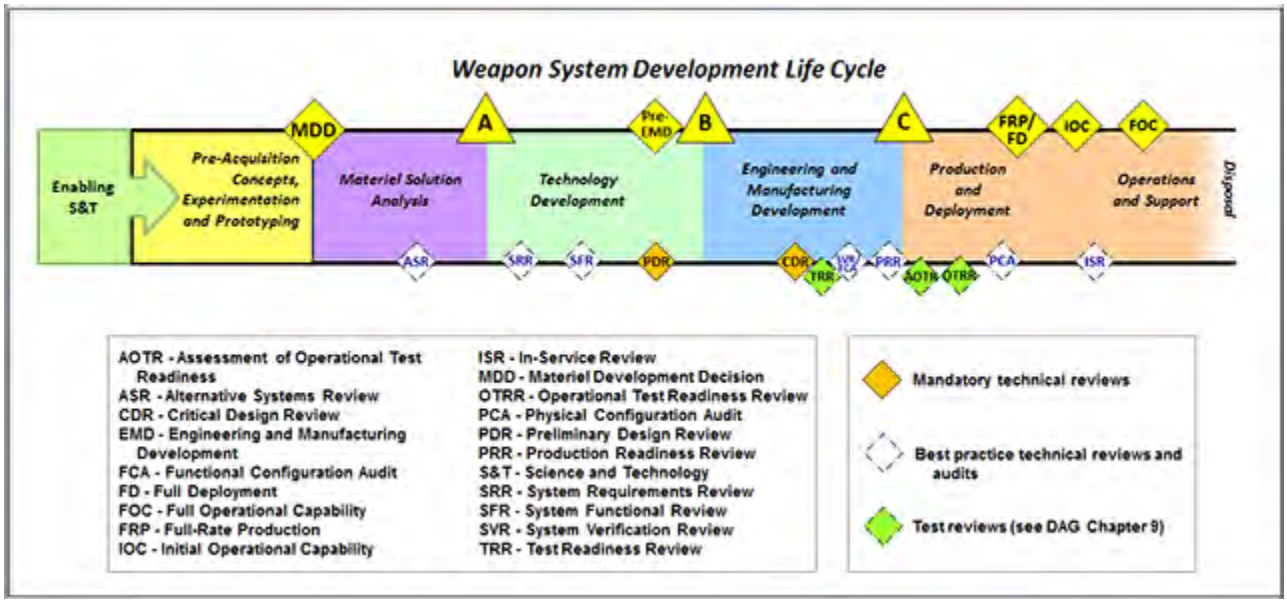
Inputs for O&S Phase
Acquisition Decision Memoranda (ADMs) associated with Milestone C and Full Deployment (FD) decision review (DR) • ADMs may contain additional direction • O&S may start as early as Milestone C (e.g., software) and overlap P&D phase • FD DR would involve O&S
Trade study results • P&D phase trade studies may support manufacturing or other system modifications (technology insertion, technology refresh, etc.)
ESOH analyses (updated) • ESOH analyses continue during O&S to include hazard analysis and supporting NEPA/EO 12114 compliance for modifications and disposal
Risk assessment
Interdependencies / interfaces / memoranda of agreement (MOAs)
System performance specification
Field failures
Other technical information, such as models and simulations generated during the P&D phase
LCSP • PDUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 201 • See DAG Chapter 5 Life-Cycle Logistics
Test and Evaluation Master Plan (TEMP) • DOT&E memorandum, "DOT&E TEMP Guidebook," February 27, 2012 • See DAG Chapter 9 Test and Evaluation
Request for Proposal (RFP) for SE support to O&S activities

Inputs for O&S Phase
Program Protection Plan (PPP) • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • See DAG Chapter 13 Program Protection
Other analyses • End-user feedback and trouble reports • Other prior analytic, prototyping, and/or technology demonstration efforts conducted by the science and technology (S&T) community • Technology insertion/transition can occur at any point in the life cycle

Activities

The O&S phase overlaps with the Production and Deployment phase, since O&S activities begin when the first system is fielded. O&S ends when a system is demilitarized and disposed of. Figure 4.2.7.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.7.F1. Weapon System Development Life Cycle



SE activities should be integrated with O&S phase-specific test and evaluation and logistics and sustainment activities identified in DAG Chapter 9 Test and Evaluation and Chapter 5 Life-Cycle Logistics, respectively. The O&S activities in which the Systems Engineer should participate include:

- Determine root cause of problems, identify corrective actions, and manage to completion

- Address problem/failure reports through the use of a comprehensive data collection approach such as a Failure Reporting, Analysis and Corrective Action System (FRACAS)
- Process and analyze mission data
- Manage preplanned product improvements (P3I)
- Develop and implement technology refresh schedules
- Conduct technology insertion efforts as needed to maintain or improve system performance
- Update system safety assessments
- Perform engineering analysis to investigate the impact of DMSMS issues
- Work with vendors and the general technical community to determine opportunities for technology incursion to increase reliability and affordability

The disposal activities in which the Systems Engineer should participate include:

- Support demilitarizing and disposing of the system; in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment
- Document lessons learned
- Archive data

The technical review conducted in O&S is the In-Service Review (ISR) (see DAG section 4.2.17. In-Service Review). ISRs are typically used to track, monitor, and assess system performance from the time an Initial Operational Capability (IOC) is reached until retirement or disposal of the system. They are often used to prioritize system modifications due to deficiencies or integration of additional capability, or to respond to external needs associated with SoS implementations.

Outputs and Products

The technical outputs and products identified in Table 4.2.7.T2 are necessary to support SE processes to sustain the system, including modifications. Technical outputs associated with technical reviews in this phase are addressed later in this chapter.

Table 4.2.7.T2. Technical Outputs Associated with O&S Phase

Technical Outputs from O&S Phase
Safe and reliable system that meets operational needs
Trade study results • O&S phase trade studies support system modifications and/or disposal efforts
Assessment of technical risk
Interdependencies / interfaces / memoranda of agreement (MOAs)
In-service performance and failure data
Value engineering results, as appropriate • See DAG section 4.3.19.3. Value Engineering

Technical Outputs from O&S Phase
Engineering Change Proposal (ECP) packages

4.2.8. Technical Reviews and Audits Overview

4.2.8. Technical Reviews and Audits Overview

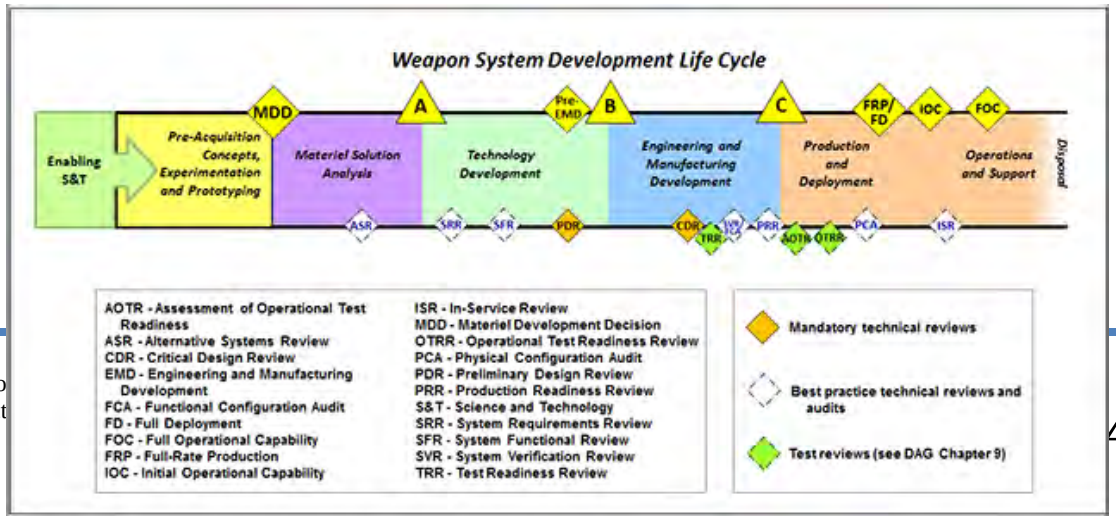
For DoD weapon systems development, a properly tailored series of technical reviews and audits provide key points throughout the life cycle to evaluate significant achievements and assess technical maturity and risk. DoDI 5000.02, Enclosure 4 presents the statutory, regulatory, and milestone requirements for acquisition programs. Properly align the technical reviews to support knowledge-based milestone decisions to streamline the acquisition life cycle and save precious taxpayer dollars. As a companion to DoDI 5000.02, see the OUSD(AT&L) memorandum, "Expected Business Practice: Document Streamlining - Program Strategies and Systems Engineering Plan" dated April 20, 2011.

Technical reviews and audits allow the Program Manager and Systems Engineer to jointly define and control the program's technical effort by establishing the success criteria for each review and audit. A well-defined program facilitates effective monitoring and control through increasingly mature points (see Technical Maturity Point table in DAG section 4.2.1. Life-Cycle Expectations).

Technical reviews of program progress should be event driven and conducted when the system under development meets the review entrance criteria as documented in the SEP. Systems engineering (SE) is an event-driven process based on successful completion of key events as opposed to arbitrary calendar dates. As such, the SEP should discuss the timing of events in relation to other SE and program events. While the initial SEP and Integrated Master Schedule have the expected occurrence in the time of various milestones (such as overall system CDR), the plan should accommodate and be updated to reflect changes to the actual timing of SE activities, reviews, and decisions.

Figure 4.2.8.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.8.F1. Weapon System Development Life Cycle



Properly structured, technical reviews and audits support the Defense Acquisition System by:

- Providing a disciplined sequence of activities to define, assess, and control the maturity of the system's design and technical baseline, reducing risk over time
- Facilitating an accurate technical assessment of the system's ability to satisfy operational requirements established in capability requirements documents
- Providing a framework for interaction with the Joint Capabilities Integration and Development System (JCIDS) and Planning, Programming, Budgeting, and Execution (PPBE) processes
- Providing a technical assessment and assurance that the end product fulfills the design and process requirements

Successful development of a complex weapon system requires a knowledge-based approach. Increasing levels of knowledge are a natural consequence of design maturation; however, successful programs establish a deliberate acquisition approach whereby major investment decision points are supported by requisite levels of knowledge. The Government Accountability Office's (GAO) study on Assessments of Selected Weapons Programs (GAO-12-400SP) provides quantitative evidence to affirm this best practice.

Figure 4.2.8.F1 illustrates the notional sequence of technical reviews and audits. It also provides typical timing associated with the acquisition phases. Technical reviews should occur when the requisite knowledge is expected and required. The guidance provided in DAG sections 4.2.9. through 4.2.17. defines the entrance and exit criteria for the level of maturity expected at each technical review and audit. OSD established the expected reviews and audits for each acquisition phase in the outline for the Systems Engineering Plan (SEP). These policy and guidance documents provide a starting point for the Program Manager and Systems Engineer to develop the program's unique set of technical reviews and audits. Tailoring is expected to best suit the program objectives (see DAG section 4.1. Introduction). The SEP captures the output of this tailoring and is reviewed and approved to solidify the program plan.

Programs that tailor the timing and scope of these technical reviews and audits to satisfy program objectives increase the probability of successfully delivering required capability to the warfighter. Technical reviews provide the forum to frame important issues and define options necessary to balance risk in support of continued development.

The technical baseline (including the functional, allocated and product baselines) established at the conclusion of certain technical reviews inform all other program activity. Accurate baselines and disciplined reviews serve to integrate and synchronize the system as it matures, which facilitates more effective milestone decisions and ultimately provides better warfighting capability for less money. The technical baseline provides an accurate and controlled basis for:

- Managing change
- Cost estimates, which inform the PPBE process and ultimately the Acquisition Program Baseline (APB)
- Program technical plans and schedules, which also inform the APB
- Contracting activity
- Test and Evaluation efforts
- Risk analysis and risk balancing
- Reports to acquisition executives and Congress

The Program Manager and the Systems Engineer need to keep in mind that technical reviews and audits provide visibility into the quality and completeness of the developer's work products. These requirements should be captured in the contract specifications or Statement of Work. The program office should consider delivering the SEP with the Request for Proposal (RFP) and having it captured in the contractor's SE Management Plan (SEMP); this best practice also should include delineating entrance criteria and associated design data requirements needed to support the reviews. The configuration and technical data management plans should clearly define the audit requirements.

For complex systems, reviews and audits may be conducted for one or more system elements depending on the interdependencies involved. These incremental system element-level reviews lead to an overall system-level review or audit (e.g., PDR, CDR, or PRR). After all incremental reviews are complete, an overall summary review is conducted to provide an integrated system analysis and capability assessment that could not be conducted by a single incremental review. Each incremental review should complete a functional or physical area of design. This completed area of design may need to be reopened if other system elements drive additional changes in this area. If the schedule is being preserved through parallel design and build decisions, any system deficiency that leads to reopening design may result in rework and possible material scrap.

Test readiness reviews (TRR) are used to assess a contractor's readiness for testing configuration items, including hardware and software. They typically involve a review of earlier or lower-level test products and test results from completed tests and a look forward to verify the test resources, test cases, test scenarios, test scripts, environment, and test data have been prepared for the next test activity. TRRs typically occur in the EMD and P&D phase of a program.

Roles and Responsibilities

For each technical review, a technical review chair is identified and is responsible for evaluating products, determining the criteria are met, and determining that actions items are closed. The Service chooses the technical review chair who could be the Program Manager, Systems Engineer, or independent subject matter expert selected according to the Service's guidance. This guidance may identify roles and responsibilities

associated with technical reviews and audits. It also may specify the types of design artifacts required for various technical reviews. In the absence of additional guidance, each program should develop and document its tailored design review plan in the SEP.

The following notional duties and responsibilities associated with the Program Manager and Systems Engineer should be considered in the absence of specific Service or lower level (e.g., System Command or Program Executive Officer) guidance:

The Program Manager is responsible for:

- Co-developing with the Systems Engineer the technical objectives of the program that guide the technical reviews and audits
- Co-developing with the Systems Engineer the earned value credit derived from the review
- Approving, funding, and staffing the planned technical reviews and audits; documenting this plan in the SEP and applicable contract documents
- Ensuring the plan includes independent subject matter experts to participate in each review (maintaining objectivity during these reviews with respect to satisfying the pre-established review criteria)
- Ensuring the plan provides timely and sufficient data to satisfy the statutory and regulatory requirements of DoDI 5000.02
- Controlling the configuration of each baseline and convening configuration steering boards when user requirement changes are warranted. This can lead to an unscheduled gateway into the Functional Capabilities Board (FCB) and JCIDS process not identified in Figure 4.2.8.F1 above.

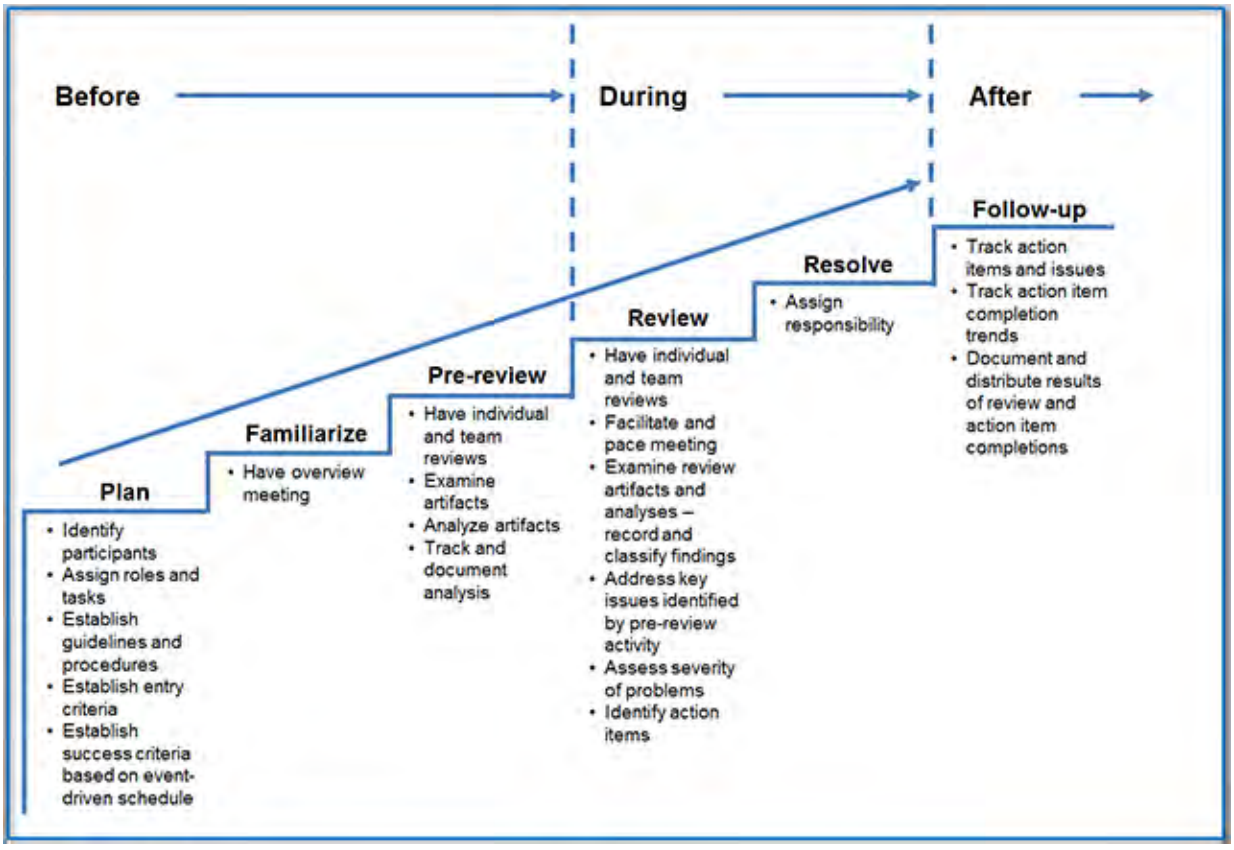
The Systems Engineer is responsible for:

- Co-developing with the Program Manager the technical objectives of the program that guide the technical reviews and audits
- Developing and documenting the technical review and audit plan in the SEP, carefully tailoring each event to satisfy program objectives and SEP outline guidance associated with the minimum technical reviews and audits. Technical review checklists are available on the DASD(SE) website.
- Ensuring the plan is event based with pre-established review criteria for each event, informed by the knowledge point objectives in Table 4.2.1.T1
- Identifying the resources required to support the plan, paying particular attention to the importance of the integrating activity leading up to the official review and audit. See Figure 4.2.8.F2.
- Ensuring technical reviews and audits are incorporated into the IMP and IMS
- Coordinating with Chief Development Tester to provide at each technical review: reliability growth progress to plan/assessments, DT&E activities to-date, planned

activities, assessments to-date, and risk areas

- Ensuring a status of applicable design considerations are provided at each technical review
- Establishing technical reviews and audits and their review criteria in the applicable contract documents (e.g., Statement of Work, IMP)
- Monitoring and controlling execution of the established plans
- Coordinating with the appointed technical review chairperson on the technical review plans and supporting execution of the technical reviews
- Assigning responsibilities for closure actions and recommend to the chairperson and Program Manager when a system technical review should be considered complete, see Figure 4.2.8.F2

Figure 4.2.8.F2. Technical Review Process



The Program Manager and Systems Engineer should identify key stakeholders who have an interest or role in the review, which may include:

- Technical review chairperson
- Program Executive Office

- Contracting Officer
- Defense Contract Management Agency (DCMA) and Defense Contract Audit Agency (DCAA)
- Product Support Manager
- Product Improvement Manager/Requirements Officer
- End-user Community
- Chief Developmental Tester
- Interdependent Acquisition Programs
- Business Financial Manager
- Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))
- Service Technical Leadership such as chief engineers
- Independent Subject Matter Experts

Review Criteria

Specific review criteria are provided in each technical review and audit section below. These criteria should be achieved and all action items closed before a technical review is considered complete. The Systems Engineer may want to consider the technical review-specific checklists available at DAU's website as a resource.

Contract incentives are frequently tied to completion of technical reviews. The developer may have a strong incentive to call the review complete as soon as possible. The review chairperson and Systems Engineer should exercise best judgment in an objective, informed manner to ensure the reviews are not prematurely declared complete.

4.2.9. Alternative Systems Review

4.2.9. Alternative Systems Review

The Alternative Systems Review (ASR) is held to support a dialogue between the end user and acquisition community and leads to a draft performance specification for the preferred materiel solution. The ASR typically occurs during the Materiel Solution Analysis (MSA) phase, after completion of the Analysis of Alternatives (AoA) and before Milestone A. It focuses technical efforts on requirements analysis.

The ASR should evaluate whether there is sufficient understanding of the technical maturity, feasibility, and risk of the preferred materiel solution, in terms of addressing the operational capability needs in the Initial Capabilities Document (ICD) and meeting affordability, technology, and operational effectiveness and suitability goals.

The ASR helps the Program Manager and Systems Engineer ensure that further engineering and technical analysis needed to draft the system performance

specification is consistent with customer needs.

CJCSI 3170.01 calls for a Functional Capabilities Board (FCB) review prior to Milestone A. This FCB review should ensure compatibility between the operational capability needs in the ICD and the maturity, feasibility, and risks of the preferred materiel solution.

Roles and Responsibilities

The unique Program Manager responsibilities associated with an ASR include:

- Approve, fund, and staff the ASR

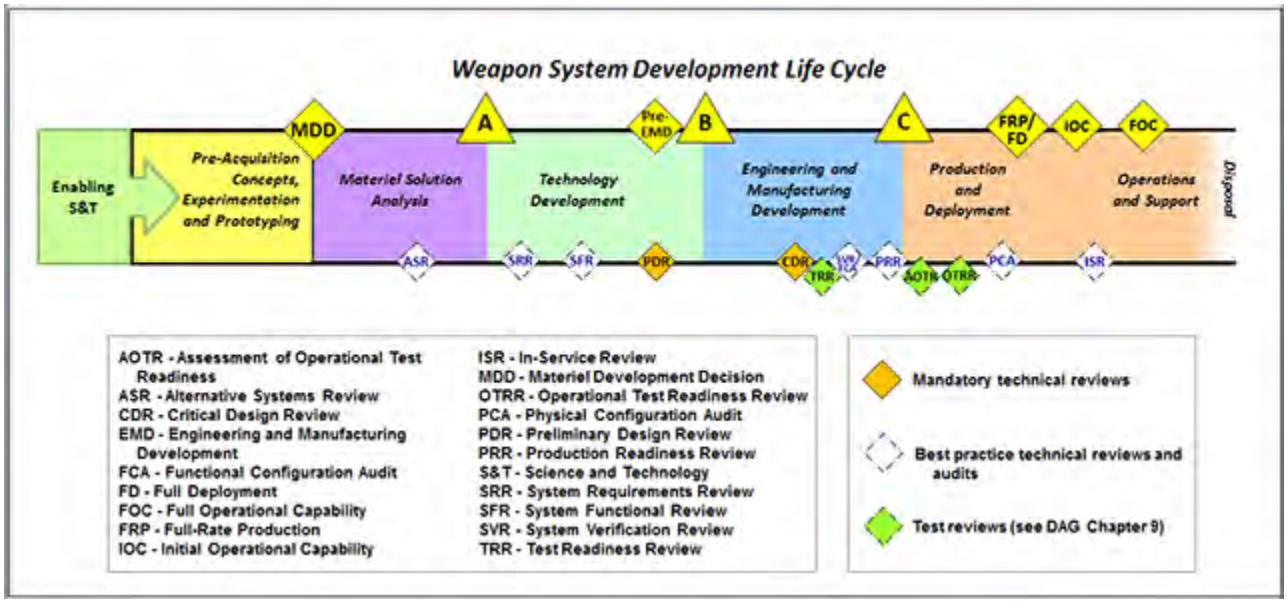
The unique Systems Engineer responsibilities associated with an ASR include:

- Ensure adequate plans are in place to complete the necessary technical activities for the ASR
- Ensure results of all technical trade studies are captured in documents that are carried through to the next phase
- Ensure technical risk items are identified and analyzed, and appropriate mitigation plans are in place. This activity should include, for example, the identification of critical technologies and identification of key interfaces with supporting or enabling systems

Inputs and Review Criteria

The ASR typically occurs after the AoA is complete and after a preferred materiel solution is selected by the lead Service or Component but before the FCB review. Figure 4.2.9.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.9.F1. Weapon System Development Life Cycle



This timing allows the focus of the ASR to be on the preferred materiel solution rather than on all the alternatives and allows for some post-AoA technical analysis to be completed and inform the FCB deliberations.

- The AoA results are an input to the ASR. The AoA should have evaluated a number of candidate materiel solutions and identified those alternatives that can meet the user requirements within the remaining trade space (including cost and affordability constraints).
- After the AoA is complete, the operational requirements community and the acquisition community collaboratively identify one or more preferred materiel solution(s) with the potential to be affordable, operationally effective and suitable, sustainable, and technically and technologically achievable (i.e., able to provide a timely solution to the stated operational capability need at an acceptable level of risk). This preferred materiel solution is also an input to the ASR.
- The draft concept of operations (CONOPS) should be available as an input to the ASR. It should have been available for use in the AoA and can then be used to support development of missions and operational scenarios used to evaluate the preferred materiel solution.

Table 4.2.9.T1 defines the suggested ASR artifacts and associated review criteria. The review should not begin until these criteria are considered met. This is a best practice review.

Table 4.2.9.T1. ASR Products and Criteria

Product	ASR Criteria
Refined Joint Requirements	• Joint context and initial CONOPS updated to reflect current user position about capability gap(s), supported missions, interfacing/enabling systems in the operational architecture; overall system of systems (SoS) context • Required related solutions and supporting references (ICD and CDDs) identified • Joint refined thresholds and objectives initially stated as broad measures of effectiveness and suitability (e.g., KPPs, KSAs, need date)
Initial Architecture for the Preferred Materiel Solution(s)	• High-level description of the preferred materiel solution(s) is available and sufficiently detailed and understood to enable further technical analysis in preparation for Milestone A • SoS interfaces and external dependencies are adequately defined
System Performance Specification	• Clear understanding of the system requirements consistent with the ICD and draft CDD (if available) • System requirements are sufficiently understood to enable system functional definition • Draft system performance specification has sufficiently conservative requirements to allow for design trade space • Relationship between draft system specification and competitive prototyping objectives is established
Preferred Materiel Solution(s) Documentation	• Comprehensive rationale is available for the preferred materiel solution(s), based on the AoA • Key assumptions and constraints associated with preferred materiel solution(s) are identified and support the conclusion that this solution can reasonably be expected to satisfy the ICD (or draft CDD if available) in terms of technical, operational, risk, and schedule/cost (affordability) criteria • Results of trade studies/technical demonstrations for concept risk reduction, if available • Initial producibility assessments of solution concepts
Risk Assessment	• Technical risks are identified, and mitigation plans are in development • Initial hazard analysis/system safety analysis for preferred solution(s) complete

Outputs and Products

The Technical Review Chair determines when the review is complete. ASR technical outputs should include, but not be limited to, the following products, including supporting rationale and trade study results:

- Refined description of the preferred materiel solution to support further development

- Informed advice to the user-developed draft Capability Development Document (CDD) required at Milestone A

4.2.10. System Requirements Review

4.2.10. System Requirements Review

The System Requirements Review (SRR) is a multi-disciplined technical review to ensure that the developer is ready to proceed with the initial system design. This review assesses whether the system requirements as captured in the system performance specification:

- Are consistent with the preferred materiel solution (including its support concept) from the Materiel Solution Analysis (MSA) phase
- Are consistent with available technologies resulting from the prototyping efforts
- Adequately consider the maturity of interdependent systems

All system requirements and performance requirements derived from the Initial Capabilities Document (ICD) or draft Capability Development Document (CDD) should be defined and consistent with cost, schedule, risk, and other system constraints; and with end user expectations. Also important to this review is a mutual understanding (between the program office and the developer) of the technical risk inherent in the system performance specification.

For Major Defense Acquisition Programs (MDAPs), the PDUSD(AT&L) memorandum, "Improving Milestone Process Effectiveness" requires a Milestone A review before approving release of the final Request for Proposal (RFP) for the Technology Development (TD) phase; therefore, it is suggested that the program office perform a review similar to an SRR to assess readiness and risks of the technical content of the draft RFP(s) prior to Milestone A. This program office review most likely occurs after the Functional Capabilities Board (FCB) review of the AoA and other analytic results.

If the program's Technology Development Strategy (TDS) includes competing contractual efforts during the TD phase, an SRR should be held with each participating developer to ensure the requirements are thoroughly and properly understood. This review also ensures that system of systems (SoS) requirements, in the form of logical and physical interfaces and desired performance outcomes, have been levied on the system to be procured and are consistent with the ICD and/or draft CDD. These requirements are documented in the system performance specification and managed through external communication and technical interfaces in accordance with the Systems Engineering Plan (SEP).

Roles and Responsibilities

The unique Program Manager responsibilities associated with an SRR include:

- Approve, fund, and staff the SRR as planned in the SEP developed by the Systems Engineer
- Manage and approve changes to the system performance specification
- Establish the plan to SFR in applicable contract documents including the SE Master Plan, Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the plan includes independent subject matter experts to participate in each review

The unique Systems Engineer responsibilities associated with an SRR include:

- Ensure all performance requirements, both explicit and derived, are defined and traceable (both directions) between requirements in the draft CDD including Key Performance Parameters (KPPs), Key System Attributes (KSAs), other system attributes, and the system performance specification (see CJCSI 3170.01 JCIDS)
- Ensure verification methods are identified for all system requirements
- Ensure risk items associated with system requirements are identified and analyzed, and mitigation plans are in place
- Ensure adequate plans are in place to complete the technical activities to proceed from SRR to the System Functional Review (SFR)
- Ensure plans to proceed to SFR allow for contingencies

Inputs and Review Criteria

Figure 4.2.10.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle. The SRR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP at Milestone A.

Figure 4.2.10.F1. Weapon System Development Life Cycle

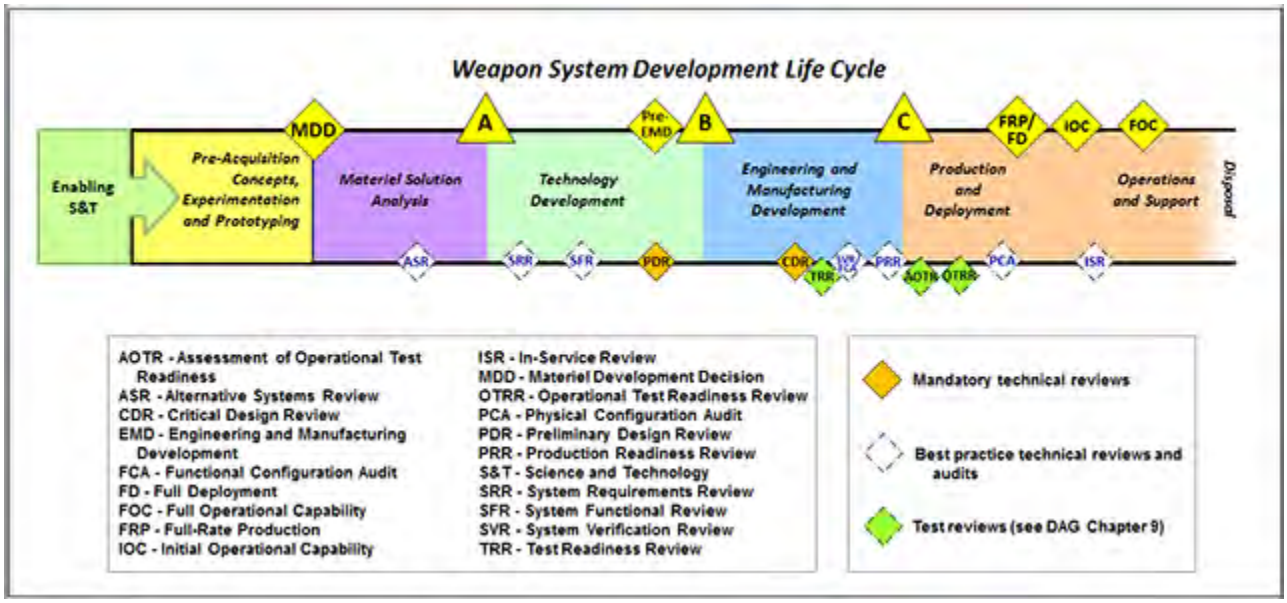


Table 4.2.10.T1 defines the suggested SRR products and associated review criteria. The review should not begin until these criteria are established, evidence has been received to support a case for success, and any prior technical review is completed and its action items closed. This is also an opportunity to assess whether technical requirements from all acquisition documentation (e.g., Program Protection Plan (PPP), Test and Evaluation Master Plan (TEMP), Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report) are flowed to specifications. If the program's TDS includes competing contractual efforts, an SRR should be held with each developer. A risk assessment tool for SRR preparation is the DoD SRR Checklist. This is a best practice review.

Table 4.2.10.T1. SRR Products and Criteria

Product	SRR Criteria
Cost Estimate	• Preliminary Cost Analysis Requirements Description (CARD) is consistent with the approved system performance specification • Preliminary software development estimates established with effort, schedule, and cost analysis • Updated cost estimate fits within the existing budget
Risk Assessment	• Technical risks are identified, and mitigation plans are in place • Risk Management Plan (RMP) is complete and adequate

Product	SRR Criteria
System Performance Specification	• Contractor clearly demonstrates an understanding of the system requirements consistent with the ICD and draft CDD • System requirements are sufficiently detailed and understood to enable system functional definition and functional decomposition • System requirements are assessed to be verifiable (see Chief Developmental Tester in DAG Chapter 9 Test and Evaluation) • Requirements can be met given the technology maturation achieved and evidence from competitive prototyping • External interfaces to the system have been documented in interface control documents • SoS technical interfaces are adequately defined, including interdependences associated with schedule, test, and configuration changes • Preliminary identification of all software components (tactical, support, deliverable, non-deliverable, etc.) are completed • Human Systems Integration (HSI) and sustainment requirements have been reviewed and included in the overall system design (see DAG section 4.3.18.10 and DAG Chapter 6 Human Systems Integration) • Contractor has adequately expanded the system specification to reflect tailored, derived, and correlated design requirements • Bidirectional requirements traceability between the draft CDD, the Statement of Work (SOW), and the System Specification has been documented • System performance specification is approved, including stakeholder concurrence, with sufficiently conservative requirements to allow for design trade space

Product	SRR Criteria
Technical Plans	• Contractors Systems Engineering Management Plan (SEMP) is complete and adequate • Cost and critical path drivers have been identified • The program schedule is executable with an acceptable level of technical and cost risk • Adequate processes and metrics are in place for the program to succeed • SE is properly staffed • Program is executable within the existing budget • Software functionality in the system specification is consistent with the software sizing estimates and the resource-loaded schedule • Programming languages and architectures, security requirements, and operational and support concepts have been identified • Hazards have been reviewed and mitigating courses of action have been allocated within the overall system design • Key technology elements have been identified, readiness assessed, and maturation plans developed • Software development strategy is complete and adequate • Program technical risks are adequately identified and documented such that there is a clear understanding regarding the contractor's ability to meet the specification requirements • Draft verification methodologies have been adequately defined for each specification requirement • Certifying agencies have been identified and certification requirements are understood • Draft test plans have been developed in support of the TD phase (See Chief Developmental Tester in DAG Chapter 9 Test and Evaluation) • Government and contractor configuration management (CM) strategies are complete and adequate • The Modeling and Simulation (M&S) Plan for life-cycle support (including life-cycle costs / total ownership costs (LCC/TOC), training devices, tactics, air vehicle, mission system etc.) is complete and adequate to support system design and operation • The manufacturing and production strategy is complete and adequate • Integrated Master Schedule (IMS) adequately identifies the critical path and is resourced at reasonable levels, based on realistic performance/efficiency expectations • Unique work requirements for competitive prototyping have been identified • Product support plan and sustainment concepts have been defined with the corresponding metrics

Output and Products

The Technical Review Chair determines when the review is complete. Once the products have been reviewed and approved in SRR, they provide a sound technical basis for proceeding with system functional definition and preliminary design.

4.2.11. System Functional Review

4.2.11. System Functional Review

The System Functional Review (SFR) is held to evaluate whether the system functional baseline satisfies the end-user requirements and capability needs and whether functional requirements and verification methods support achievement of performance requirements. At completion of the SFR, the system's functional baseline is normally taken under configuration control.

The functional baseline describes the system's performance (functional, interoperability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics. It is directly traceable to the operational requirements contained in the Initial Capabilities Document (ICD) and draft Capability Development Document (CDD). The Program Manager establishes Government control of the functional baseline at the SFR and verifies it through Functional Configuration Audits (FCA) leading up to the system level FCA or the System Verification Review (SVR). For additional information, see DAG section 4.3.7. Configuration Management Process.

A successful SFR, which typically occurs during the Technology Development (TD) phase, reduces the risk of continuing the technical effort toward the Preliminary Design Review (PDR). The SFR is used to:

- Assess whether a balanced definition of the system's major elements has been developed, including their functionality and performance requirements
- Assess whether the system functional baseline is technically achievable with regard to cost, schedule, and performance
- Confirm that the system performance specification (typically put on contract) is realistic and provides a sound technical foundation for preliminary design
- Establish functional baseline and verification criteria to be used during FCA

Roles and Responsibilities

The unique Program Manager responsibilities associated with an SFR include:

- Approve, fund, and staff the SFR as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer
- Manage and approve changes to the system performance specification
- Establish the plan to PDR in applicable contract documents including the SE

Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the plan includes independent subject matter experts to participate in each review
- Control the configuration of the Government-controlled subset of the functional baseline
- Chair the configuration control board (CCB) for the system performance specification and other documentation used to control the system functional baseline

The unique Systems Engineer responsibilities associated with an SFR include:

- Ensure adequate plans are in place to complete the necessary technical activities to proceed from SFR to PDR
- Ensure plans to proceed to PDR allow for contingencies
- Ensure all performance requirements, both explicit and derived, are defined and traceable (both directions) between requirements in the draft CDD to include Key Performance Parameters (KPPs), Key System Attributes (KSAs), other system attributes, and the system performance specification (see CJCSI 3170.01 JCIDS)
- Ensure verification methods are identified for all requirements
- Ensure risk items associated with functional requirements are identified and analyzed, and mitigation plans are in place

Inputs and Review Criteria

The SFR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP at Milestone A. Figure 4.2.11.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.11.F1. Weapon System Development Life Cycle

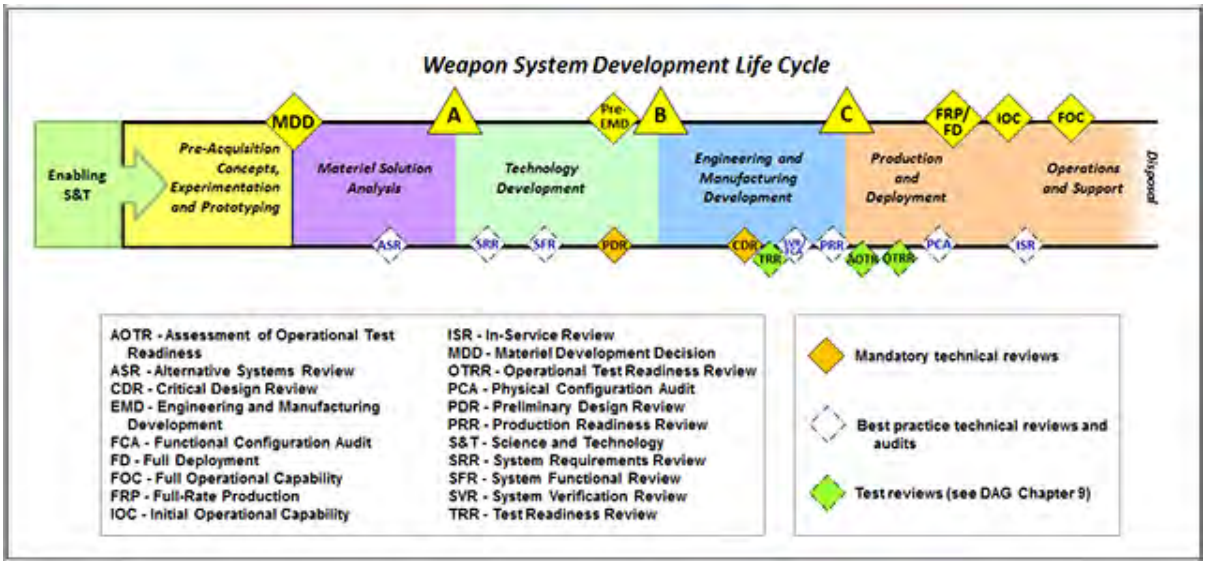


Table 4.2.11.T1 defines the suggested SFR products and associated review criteria. The review should not begin until these criteria are considered met and any prior technical review is completed and its action items closed. If the program's Technology Development Strategy (TDS) includes competing contractual efforts, an SFR should be held with each participating developer. A readiness assessment tool for SFR preparation is the DoD SFR Checklist. This is a best practice review.

Table 4.2.11.T1. SFR Products and Criteria

Product	SFR Criteria
System Functional Baseline Documentation	• Understood and assessed to be achievable within cost and schedule constraints • Established functional baseline by mapping requirements to hardware, software, and human elements of the system • Documented performance requirements traced to (draft) CDD requirements and reflecting clear linkage to the system of system (SoS) context(s) (including use in multiple operational environments) • Documented performance requirements reflect design considerations • Documented verification requirements, including testing, for FCA/SVR
Major System Element Definition	• Documented preliminary allocated requirements optimized through analyses (including functional analysis and sensitivity analysis), trade studies, and risk assessments

Risk Assessment	• Identified and documented risks, including ESOH mitigation measure requirements, at levels that warrant continued engineering development
Technical Plans	• Established detailed plan/schedule, sufficiently resourced to continue design and development

Outputs and Products

The Technical Review Chair determines when the review is complete. Once the products have been reviewed and approved in SFR, they provide a sound technical basis for proceeding into preliminary design.

4.2.12. Preliminary Design Review

4.2.12. Preliminary Design Review

The Preliminary Design Review (PDR) ensures the preliminary design and basic system architecture are complete, and that there is technical confidence the capability need can be satisfied within cost and schedule goals. The PDR provides the acquisition community, end user, and other stakeholders with an opportunity to understand the trade studies conducted during the preliminary design, and thus confirm that design decisions are consistent with the user's performance and schedule needs prior to formal validation of the Capability Development Document (CDD). The PDR also establishes the system's allocated baseline.

The allocated baseline describes the functional and interface characteristics for all system elements (allocated and derived from the higher-level product structure hierarchy) and the verification required to demonstrate achievement of those specified characteristics. The allocated baseline for each lower-level system element (hardware and software) is usually established and put under configuration control at the system element Preliminary Design Review (PDR). This process is repeated for each system element and culminates in the Program Manager establishing the complete allocated baseline at the system-level PDR. The Program Manager then verifies the allocated baseline at the Functional Configuration Audit (FCA) and/or System Verification Review (SVR) (see DAG section 4.3.7 Configuration Management Process).

The PDR is mandatory. According to DoD policy and guidance, PDR requirements include the following:

- PDR is completed prior to Milestone B for all Major Defense Acquisition Programs (MDAPs) (DTM 09-027)
- Component Acquisition Executive determines the timing of PDR relative to the Pre-Engineering and Manufacturing Development (EMD) review (DTM 09-027

and PDUSD(AT&L) memorandum, "Improving Milestone Process Effectiveness")

- PDR Report is provided to the Milestone Decision Authority (MDA) prior to the Post-PDR Assessment and should reflect any requirements trades based upon the Program Manager's assessment of cost, schedule, and performance risk (DoDI 5000.02)
- PDR Report should follow the PDR Report template which prescribes the content and responsibilities associated with all PDR completion memos

Any tailoring with respect to establishing an allocated baseline at PDR prior to Milestone B should be consistent with the approved Technology Development Strategy (TDS) and documented in the Systems Engineering Plan (SEP). In a competitive environment, each developer should establish an allocated baseline to meet the definition prescribed in the Request for Proposal (RFP) and associated system performance specification, consistent with their individual design approach. Since the functional and allocated baselines are critical to providing the Engineering and Manufacturing Development (EMD) bidders with a complete technical package, best practices would dictate that the PDR be completed prior to the pre-EMD Review, although this timing is optional under policy. The tailoring strategy may also include conduct of a delta-PDR after Milestone B if the allocated baseline has changed significantly.

A successful PDR confirms that the system's preliminary design:

- Satisfies the operational and suitability requirements of the draft CDD, as documented in the system performance specification
- Is affordable, producible, sustainable, and carries an acceptable level of risk
- Is composed of technologies demonstrated in a relevant environment that can be integrated into a system with acceptable levels of risk
- Is complete and ready for detailed design
- Provides the technical basis for the Milestone B investment decision and Acquisition Program Baseline (APB)
- Is fully captured in the specifications for each system element and all interface documentation (including system of systems (SoS) interdependencies)

In addition, the PDR represents agreement that the proposed plan to proceed to the Critical Design Review (CDR) is executable and properly resourced. The PDR establishes the allocated baseline, which is placed under formal configuration control at this point. The maximum benefit of the PDR process is realized when the allocated baseline is complete with the following attributes:

- All system-level functional performance requirements have been decomposed (or directly allocated) to the lowest level of the specification tree for all system elements uniquely identified
- All external interfaces to the system, as addressed at the System Requirements

Review, have been documented in interface control documents

- All internal interfaces of the system (system element to system element) have been documented in interface control documents
- Verification requirements to demonstrate achievement of all specified allocated performance characteristics have been documented
- Design constraints have been captured and incorporated into the requirements and design

Some of the benefits realized from a PDR with the attributes identified above would be to:

- Establish the technical basis for the Cost Analysis Requirements Description (CARD), documenting all assumptions and rationale needed to support an accurate cost estimate for the APB; technically informed cost estimates enable better should cost / will cost management
- Establish the technical requirements for the detailed design, EMD contract specifications, and Statement of Work; inform the CDD
- Establish an accurate basis to quantify risk and identify opportunities
- Provide core evidence for the PDR Report
- Provide the technical foundation for section 2366b of title 10, United States Code certification required for all MDAPs

Some design decisions made at PDR may precipitate discussions with the operational requirements community because they could have an impact on the CDD. Depending upon the nature/urgency of the capability required and the current state of the technology, incremental development might be required. In this case the Sponsor should document these increments in the CDD and the Program Manager and Systems Engineer should update relevant program plans.

Roles and Responsibilities

The Program Manager and Systems Engineer may hold incremental PDRs for lower-level system elements, culminating with a system-level PDR. The system PDR assesses the preliminary design as captured in system performance specifications for the lower-level system elements; it further ensures that documentation for the preliminary design correctly and completely captures each such specification. The Program Manager and Systems Engineer evaluate the designs and associated logistics elements to determine whether they correctly and completely implement all allocated system requirements, and whether they have maintained traceability to the CDD.

Though many Service systems commands or PEOs define the roles and responsibilities of the Program Manager and Systems Engineer, the following notional duties and

responsibilities should be considered:

The Program Manager's responsibilities include the following:

- Approve, fund, and staff the system PDR as planned in the SEP developed by the Systems Engineer
- Establish the plan to CDR in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the SEP includes independent subject matter experts to participate in each review
- Control the configuration of the Government-controlled subset of the functional and allocated baselines; convene Configuration Steering Boards when changes are warranted
- Submit the PDR Report for approval consistent with the template guidance

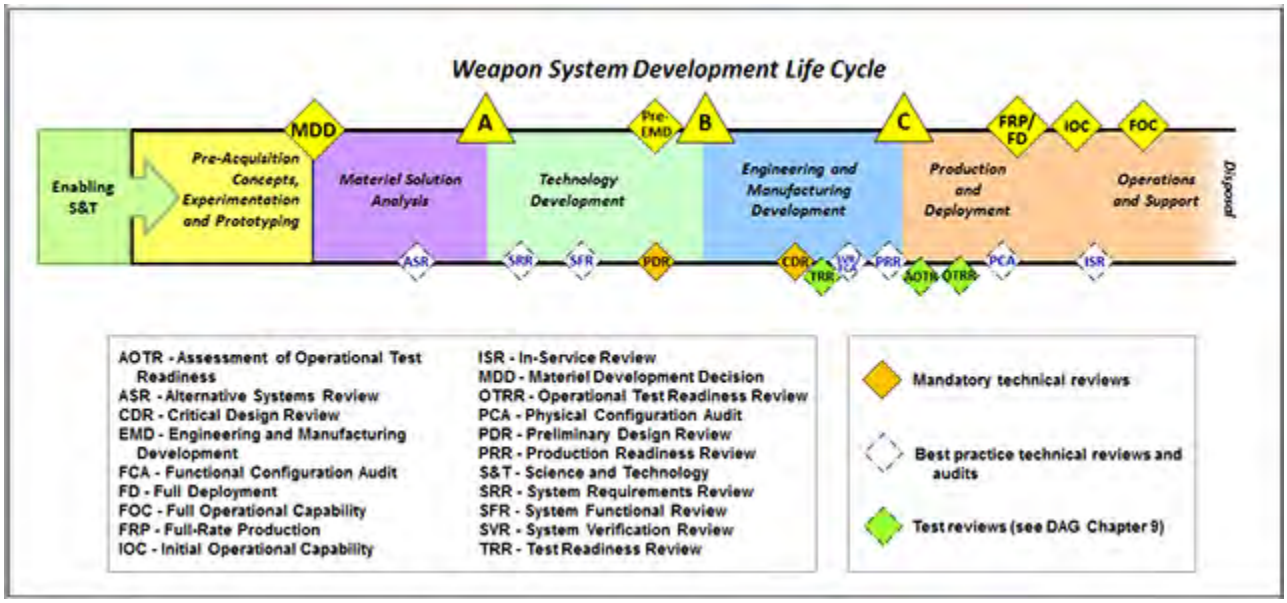
The Systems Engineer's responsibilities include the following:

- Develop and execute the system PDR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives
- Ensure that the pre-established PDR criteria have been met
- Provide industry with an opportunity to participate in this PDR planning (pre-contract award is a best practice, where applicable)
- Support development of the PDR Report
- Ensure assessments and risks associated with all design constraints and considerations are conducted, documented, and provided (e.g., reliability and maintainability, corrosion, and Environment, Safety, and Occupational Health (ESOH) considerations)
- Determine the root cause of problems, identify corrective actions, and manage to completion
- Monitor and control the execution of the PDR closure plans
- Document the plan to CDR in the SEP and elsewhere as appropriate

Inputs and Review Criteria

Figure 4.2.12.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.12.F1. Weapon System Development Life Cycle



The PDR review criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP no later than Milestone A. Table 4.2.12.T1 defines the products and associated review criteria. The system-level PDR review should not begin until these criteria are considered met and any prior technical review is complete and its action items closed. A readiness assessment tool for PDR preparation is the DoD PDR Checklist. The PDR is a mandatory technical review.

Table 4.2.12.T1. PDR Products and Criteria

Product	PDR Criteria
Cost Estimate	• System cost model has been updated, allocated to lower system element levels, and tracked against targets; production cost model constructed • Updated CARD is consistent with the proposed allocated baseline
Risk Assessment	• All risk assessments and risk mitigation plans have been updated, documented, formally addressed, and implemented • Test and evaluation strategy defined in the Test and Evaluation Master Plan (TEMP) accounts for risks with a mitigation plan; necessary integration and test resources are documented within the TEMP and current availability align with the program IMS (SE coordinates with the Chief Developmental Tester in this area; refer to DAG Chapter 9 Test and Evaluation) • ESOH risks are known and being mitigated • Risks are at an acceptable level to continue with detailed design • Unique software risks identified/assessed and mitigation plans developed and implemented

Product	PDR Criteria
System Baseline Documentation (Allocated)	• Analysis of system performance is complete and is assessed to meet requirements • Preliminary design satisfies design considerations (see DAG section 4.3.11 Requirements Analysis Process) • Producibility assessments of key technologies are complete • Preliminary system-level design is producible and assessed to be within the production budget • Assessment of the technical effort and design indicates potential for operational test and evaluation success (operationally effective and suitable) • All Critical Safety Items (CSIs) and Critical Application Items (CAIs) are identified • Functional failure mode, effects, and criticality analysis (FMECA) is completed • Estimate of system reliability and maintainability updated, based on engineering analyses, initial test results, or other sources of demonstrated reliability and maintainability • Computer system and software architecture designs have been established; all Computer Software Configuration Items (CSCIs), Computer Software Components (CSCs), and Computer Software Units (CSUs) have been defined • Software Requirements Specifications (SRSs) and Interface Requirement Specifications (IRSs), including verification plans, are complete and baselined for all CSCs and satisfy the system functional requirements • Interface control documents trace all software interface requirements to the CSCIs and CSUs • Preliminary software design has been defined and captured • All required software-related documents are baselined and delivered • System-allocated baseline documentation is sufficiently complete and correct to enable detailed design to proceed with proper configuration management
System Baseline Documentation (Functional and/or Allocated)	• Preliminary design (hardware and software), including interface descriptions, is complete and satisfies all requirements in the system functional baseline • Requirements trace between functional and allocated baselines is complete and consistent

Product	PDR Criteria
Technical Plans	• All entry criteria stated in the contract (e.g., Statement of Work (SOW), SEP, approved SEMP and system specification) have been satisfied • Integrating activities of any lower-level PDRs have occurred; identified issues are documented in action plans • Plan to CDR is accurately documented in the SEP as well as the IMP and IMS • Program is properly staffed • Adequate processes and metrics are in place for the program to succeed • Program schedule, as depicted in the updated IMS (see DAG Section 4.3.2.2. Integrated Master Plan/Integrated Master Schedule) is executable within acceptable technical and cost risks • Program is executable with the existing budget and the approved product baseline • Trade studies and system producibility assessments are under way • Majority of manufacturing processes have been defined, characterized, and documented • Logistics (sustainment) and training systems planning and documentation are sufficiently complete to support the review • Life Cycle Sustainment Plan (LCSP) is approved, including updates on program sustainment development efforts and schedules based on current budgets and firm supportability design features • LCSP includes software support requirements • Long-lead and key supply chain elements are identified • Computer system and software design/development approach have been confirmed through analyses, demonstrations, and prototyping in a relevant environment • Software increments have been defined and capabilities allocated to specific increments • Software trade studies addressing commercial-off-the-shelf, reuse, and other software-related issues are completed • Software development process is defined in a baselined Software Development Plan and reflected in the IMP and IMS • Software development schedules reflect contractor software processes and IMP/IMS software events for current and future development phases • Software development environment and test/integration labs have been established with sufficient fidelity and capacity • Software metrics have been defined and a reporting process has been implemented; metrics are being actively tracked and assessed • TEMP addresses all CSCI plans, test facilities, and test plans, including testing required to support incremental approaches and regression tests • Software development estimates (i.e., size, effort (cost), and schedule) are updated

Outputs and Products

The Technical Review Chair determines when the review is complete. Completion of the

PDR establishes that:

- Technical data for the allocated baseline are complete, satisfy the system specification, and provide a sufficient foundation for detailed design to proceed
- Risks have been balanced and are acceptable with any risk mitigation plans approved and documented in the IMS
- Feasibility, cost and schedule are determined to be within acceptable risk margins
- IMS is updated (including systems and software critical path drivers) and includes all activities required to complete CDR (assuming same developer responsible for PDR and CDR)
- Corrective action plans for issues identified in the PDR have been completed
- CARD is updated and reflects the design in the allocated baseline
- LCSP is updated to reflect development efforts and schedules

4.2.13. Critical Design Review

4.2.13. Critical Design Review

The Critical Design Review (CDR) confirms the system design is stable and is expected to meet system performance requirements, confirms the system is on track to achieve affordability and should cost goals as evidenced by the detailed design documentation, and establishes the system's initial product baseline. The system CDR occurs during the EMD phase and typically marks the end of the integrated system design efforts and readiness to continue with system capability and manufacturing process demonstration activities.

The CDR provides the acquisition community with evidence that the system, down to the lowest system element level, has a reasonable expectation of satisfying the requirements of the system performance specification as derived from the Capability Development Document (CDD) within current cost and schedule constraints.

The CDR establishes the initial product baseline for the system and its constituent system elements. It also establishes requirements and system interfaces for enabling system elements such as support equipment, training system, maintenance, and data systems. At this point the system has reached the necessary level of maturity to start fabricating, integrating, and testing pre-production articles with acceptable risk.

The product baseline describes the detailed design for production, fielding/deployment, and operations and support. The product baseline prescribes all necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. It is traceable to the system performance requirements contained in the Capability Development Document (CDD). The initial system element product baseline is established and placed under configuration control at the system element CDR and verified later at the Physical Configuration Audit (PCA). In accordance with DoDI

5000.02, the Program Manager assumes control of the initial product baseline for all Class I configuration changes at the completion of the system level CDR to the extent that the competitive environment permits. This does not necessarily mean that the Program Manager takes delivery and acceptance of the Technical Data Package (TDP) (for more information, see DAG section 4.3.7. Configuration Management Process).

Roles and Responsibilities

The Systems Engineer documents the approach for the CDR in the Systems Engineering Plan (SEP). This includes identification of criteria, and artifacts defining the product baseline.

The Program Manager reviews and approves the approach, ensures the required resources are available, and recommends independent review participants.

The Program Manager and Systems Engineer may hold incremental CDRs for lower-level system elements, culminating with a system-level CDR. The system CDR assesses the final design as captured in system performance specifications for the lower-level system elements; it further ensures that documentation for the detailed design correctly and completely captures each such specification. The Program Manager and Systems Engineer evaluate the detailed designs and associated logistics elements to determine whether they correctly and completely implement all allocated system requirements, and whether they have maintained traceability to the CDD.

The Program Manager's responsibilities include:

- Approve, fund, and staff the system CDR as planned in the SEP developed by the Systems Engineer
- Establish the plan to the System Verification Review (SVR) in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the plan includes independent subject matter experts to participate in each review
- Control the configuration of the Government-controlled subset of the functional, allocated, and product baselines; convene Configuration Steering Boards (CSBs) when changes are warranted

The Systems Engineer's responsibilities include:

- Develop and execute the system CDR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives
- Ensure that the pre-established review criteria have been met to ensure the design has been captured in the allocated baseline and initial product baseline
- Ensure assessments and risks associated with all design constraints and considerations are conducted, documented, and provided (e.g., reliability and maintainability, corrosion, and Environment, Safety, and Occupational Health

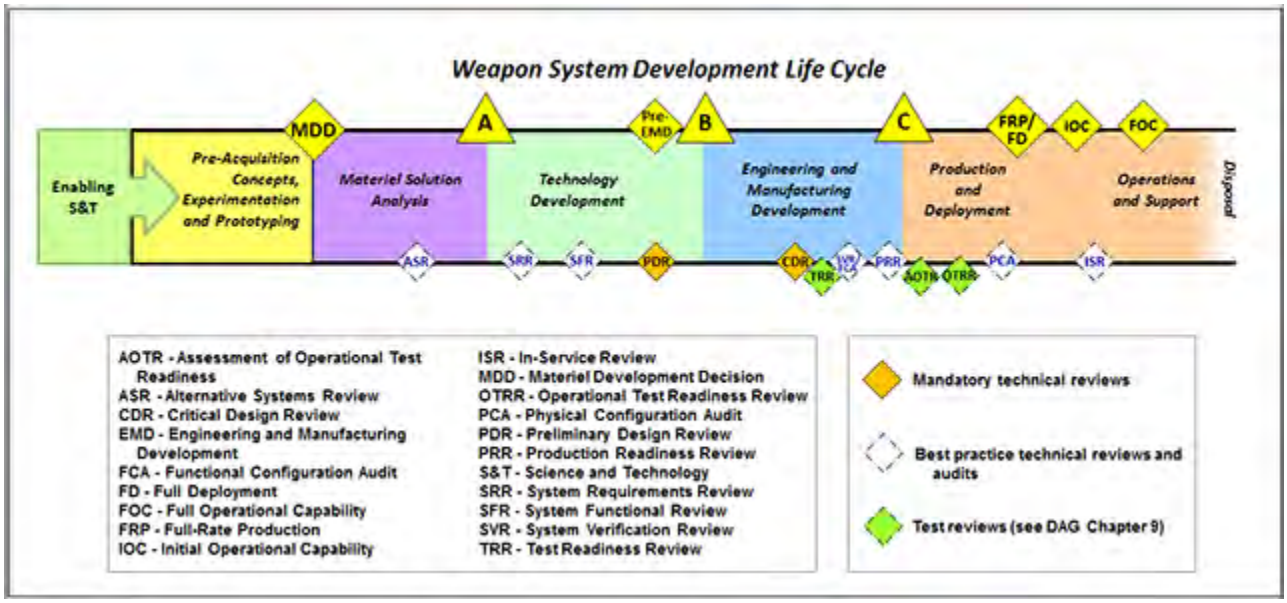
(ESOH) considerations)
- Determine the root cause of problems, identify corrective actions, and manage to completion
- Monitor and control the execution of the CDR closure plans
- Document the plan to SVR in the SEP and elsewhere as appropriate

The USD(AT&L) memorandum, "Expected Business Practice: Post-Critical Design Review Reports and Assessments" directs the DASD(SE)) to participate in CDRs for Major Defense Acquisition Programs (MDAPs), and prepare a brief assessment of the program's design maturity and technical risks that may require Milestone Decision Authority (MDA) attention.

Inputs and Review Criteria

Figure 4.2.13.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.13.F1. Weapon System Development Life Cycle



The March 2012 Government Accountability Office (GAO) report, "Assessments of Selected Weapon Programs," suggests a best practice is to achieve design stability at the system-level CDR. A general rule is that 75 to 90 percent of (manufacturing quality) product drawings, software design specification(s), and associated instructions (100 percent for all Critical Safety Items (CSIs) and Critical Application Items (CAIs)) should be complete in order to provide tangible evidence of a stable product design. A prototype demonstration shows that the design is capable of meeting performance requirements.

The CDR review criteria are developed to best support the program's technical scope

and risk and are documented in the program's SEP no later than Milestone B. Table 4.2.13.T1 defines the products and associated review criteria. The system-level CDR review should not begin until these criteria are considered met and any prior technical review is complete and its action items closed. A readiness assessment tool for CDR preparation is the DoD CDR Checklist. The CDR is a mandatory technical review.

Table 4.2.13.T1. CDR Products and Criteria

Product	CDR Criteria
Cost Estimate	• Updated Cost Analysis Requirements Description (CARD) is consistent with the approved initial product baseline • System production cost model has been updated, allocated to subsystem level, and tracked against targets
System Baseline Documentation (Functional and/or Allocated and/or Product)	• Detailed design (hardware and software), including interface descriptions are complete and satisfy all requirements in the system functional baseline • Requirements trace among functional, allocated, and initial product baselines are complete and consistent

Product	CDR Criteria
System Baseline Documentation (Product)	• Key product characteristics having the most impact on system performance, assembly, cost, reliability, and sustainment or ESOH have been identified to support production decisions • Initial product baseline documentation is sufficiently complete and correct to enable hardware fabrication and software coding to proceed with proper configuration management • Assessment of the technical effort and design indicates potential for operational test and evaluation success (operationally effective and suitable) (see DAG Chapter 9 Test and Evaluation) • 100% of Critical Safety Items and Critical Application Items have completed drawings, specifications and instructions • Failure mode, effects, and criticality analysis (FMECA) is complete • Estimate of system reliability and maintainability based on engineering analyses, initial test results or other sources of demonstrated reliability and maintainability • Detailed design satisfies sustainment and Human Systems Integration (HSI) requirements (see DAG Chapter 6 Human Systems Integration) • Software functionality in the approved initial product baseline is consistent with the updated software metrics and resource-loaded schedule • Software and interface documents are sufficiently complete to support the review • Detailed design is producible and assessed to be within the production budget • Process control plans have been developed for critical manufacturing processes • Critical manufacturing processes that affect the key product characteristics have been identified, and the capability to meet design tolerances has been determined • Verification (developmental test and evaluation (DT&E)) assessment to date is consistent with the product baseline and indicates the potential for test and evaluation success (see Test and Evaluation Master Plan (TEMP) and Chief Developmental Tester in DAG Chapter 9 Test and Evaluation)
Risk Assessment	• All risk assessments and risk mitigation plans have been updated, documented, formally addressed, and implemented • Test and evaluation strategy defined in the TEMP accounts for risks with a mitigation plan; necessary integration and test resources are documented in the TEMP and current availabilities align with the Program's IMS (Systems Engineer coordinates with Chief Developmental Tester in this area; see DAG Chapter 9 Test and Evaluation) • ESOH risks are known and being mitigated

Product	CDR Criteria
Technical Plans	• PDR is successfully completed; all PDR actions are closed • Integrating activities of any lower-level CDRs have occurred; identified issues are documented in action plans • All entry criteria stated in the contract (e.g., SOW, SEP, approved SEMP, and system specification) have been satisfied • Adequate processes and metrics are in place for the program to succeed • Program schedule as depicted in the updated IMS (see DAG section 4.3.2.2. Integrated Master Plan/Integrated Master Schedule) is executable (within acceptable technical/cost risks) • Program is properly staffed • Program is executable with the existing budget and the approved initial product baseline • Detailed trade studies and system producibility assessments are under way • Materials and tooling are available to meet the pilot line schedule • Logistics (sustainment) and training systems planning and documentation are sufficiently complete to support the review • Life-Cycle Sustainment Plan (LCSP), including updates on program sustainment development efforts and schedules based on current budgets, test and evaluation results, and firm supportability design features, is approved • Long-lead procurement plans are in place; supply chain assessments are complete

Outputs and Products

The Technical Review Chair determines when the review is complete. Completion of the CDR should provide the following:

- An established system initial product baseline
- Acceptable risks with mitigation plans approved and documented in the IMS
- Updated CARD (or CARD-like document) based on the system Initial product baseline
- Updated program development schedule including fabrication, test and evaluation, software coding, and critical path drivers
- Corrective action plans for issues identified in the PDR
- Updated LCSP, including program sustainment development efforts and schedules based on current budgets, test evaluation results and firm supportability design features

Note that baselines for some supporting items might not be at the detailed level and may lag the system-level CDR. Enabling systems may be on different life-cycle timelines. The CDR agenda should include a review of all this information, but any statement that all detailed design activity on these systems is complete may lead to misunderstandings. As an example, development of simulators and other training

systems tends to lag weapon system development.

4.2.14. System Verification Review/Functional Configuration Audit

4.2.14. System Verification Review/Functional Configuration Audit

The System Verification Review (SVR) is the technical assessment point at which the actual system performance is verified to meet the requirements in the system performance specification and is documented in the system functional baseline. The Functional Configuration Audit (FCA) is the technical audit during which the actual performance of a system element is verified and documented to meet the requirements in the system element performance specification in the allocated baseline. Further information on FCA can be found in MIL-HDBK-61A. SVR and FCA are sometimes used synonymously when the FCA is at the system level. The SVR/FCA typically occurs during the Engineering and Manufacturing Development (EMD) phase.

When a full-up system prototype is not part of the program's acquisition strategy, the FCA is used to validate system element functionality. Other system-level analysis is then used to ascertain whether program risk warrants proceeding to system initial production for Operational Test and Evaluation (OT&E). Verification of system performance is later accomplished on a production system.

A successful SVR/FCA reduces the risk when proceeding into initial production for the system to be used in operational test and evaluation (OT&E). The SVR/FCA is used to:

- Assess whether system development is satisfactorily completed
- Prepare the system for OT&E (see DAG Chapter 9 Test and Evaluation)
- Confirm that the product baseline meets the requirements of the functional baseline and therefore has a high likelihood of meeting the warfighter requirements documented in the Capability Development Document (CDD) and/or Capability Production Document (CPD)

Roles and Responsibilities

The unique Program Manager responsibilities associated with an SVR/FCA include:

- Approve, fund, and staff the SVR/FCA as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer
- Establish the plan to the Production Readiness Review (PRR) in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the SEP includes independent subject matter experts to participate in each technical review/audit
- Continue to control Class I changes to the system product baseline (see DAG section 4.3.7. Configuration Management Process)

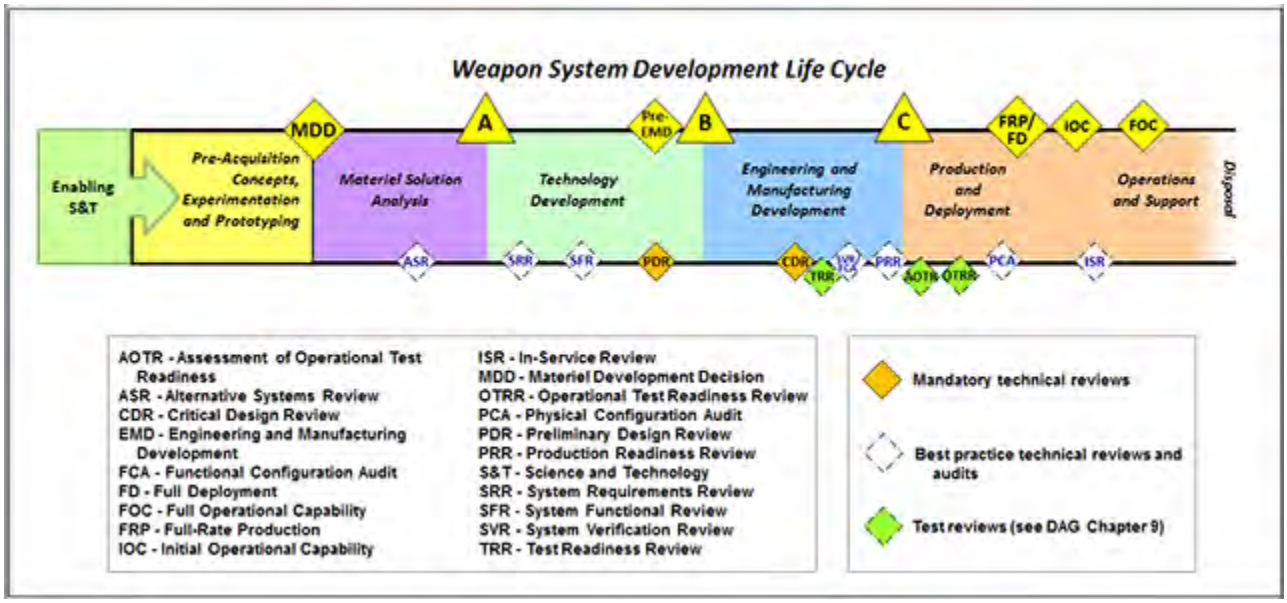
The unique Systems Engineer responsibilities associated with an SVR/FCA include:

- Develop and execute the SVR/FCA plans with established quantifiable review criteria, carefully tailored to satisfy program objectives
- Ensure the pre-established technical review/audit criteria have been met
- Ensure all requirements in the system performance specification have been verified through the appropriate verification method and have been appropriately documented
- Ensure technical risk items associated with the verified system product baseline are identified and analyzed, and mitigation plans are in place
- Monitor and control the execution of the SVR/FCA closure plans
- Ensure adequate plans and resources are in place to accomplish the necessary technical activities between SVR, PRR and Physical Configuration Audit (PCA); these plans should allow for contingencies

Inputs and Review Criteria

Figure 4.2.14.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.14.F1. Weapon System Development Life Cycle



The SVR/FCA criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP no later than Milestone B. Table 4.2.14.T1 defines the suggested SVR/FCA products and associated review criteria. The review should not begin until these criteria are considered met and any prior technical review is complete and its action items closed. A readiness assessment tool for SVR preparation is the DoD SVR Checklist. This is a best practice review.

Table 4.2.14.T1. SVR/FCA Products and Criteria

Product	SVR/FCA Criteria
System Baseline Documentation (Functional and/or Allocated) Verification	• Documented achievement of functional and/or allocated baseline requirements through the appropriate documented verification method (analysis, demonstration, examination, testing, or any combination thereof) are reviewed and verified (**Note:** verification testing may include developmental, operational (e.g., Early Operational Assessments (EOAs), Operational Assessments (OAs)) and/or live fire testing) • Assessment that the documented system product baseline for the initial production system has a low risk of operational test failure during OT&E
Risk Assessment	• Identified and documented risks (including ESOH) have been accepted at the appropriate management level prior to initial production for the system to be used in OT&E
Technical Plans	• Detailed plan/schedule has been established and sufficiently resourced to continue development

Outputs and Products

The Technical Review Chair determines when the review is complete. Once the products have been reviewed and approved in SVR/FCA, they provide a sound technical basis for proceeding into initial production for the system to be used in OT&E.

4.2.15. Production Readiness Review

4.2.15. Production Readiness Review

The Production Readiness Review (PRR) for the system determines whether the system design is ready for production, and whether the developer has accomplished adequate production planning for entering Low-Rate Initial Production (LRIP) and Full-Rate Production (FRP). Production readiness increases over time with incremental assessments accomplished at various points in the life cycle of a program.

In the early stages, production readiness assessments should focus on high-level manufacturing concerns such as the need for identifying high-risk and low-yield manufacturing processes or materials, or the requirement for manufacturing development efforts to satisfy design requirements. As the system design matures, the assessments should focus on adequate production planning, facilities allocation, producibility changes, identification and fabrication of tools and test equipment, and long-lead items. The system PRR, held prior to Milestone C, should provide evidence that the system can be produced with low risk and no breaches in cost, schedule, and performance thresholds. See also the System Capability and Manufacturing Process Demonstration described in DoDI 5000.02 Enclosure 2 paragraph 6.c.(6)(d).

For complex systems, a PRR may be conducted for one or more system elements. In addition, periodic production readiness assessments should be conducted during the Engineering and Manufacturing Development phase to identify and mitigate risks as the design progresses. The incremental reviews lead to an overall system PRR. See DAG section 4.2.8. Technical Reviews and Audits Overview for more on this incremental approach.

Roles and Responsibilities

The unique Program Manager responsibilities associated with a system PRR include:

- Approve, fund, and staff the PRR as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer
- Establish the plan to Physical Configuration Audit (PCA) in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the plan includes independent subject matter experts to participate in each review
- Determine if the readiness of manufacturing processes, quality management system, and production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.) provide low-risk assurances for supporting LRIP and FRP
- Continue to control Class I changes to the system product baseline (see DAG section 4.3.7. Configuration Management Process)

The unique Systems Engineer responsibilities associated with a system PRR include:

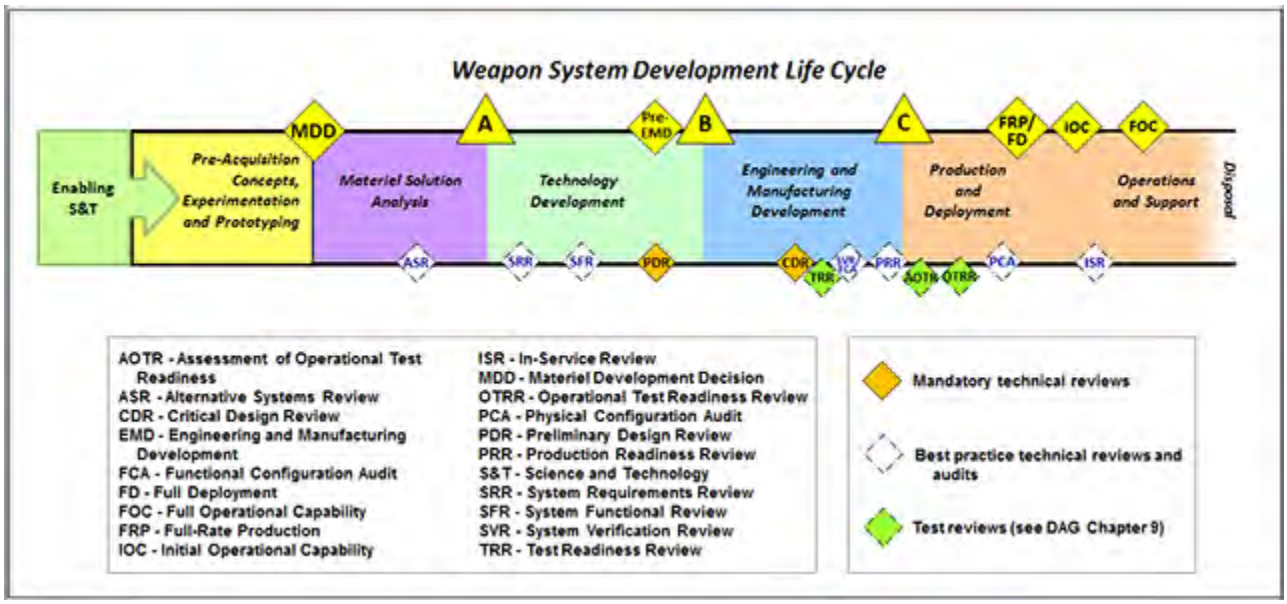
- Develop and execute the PRR plans with established quantifiable review criteria, carefully tailored to satisfy program objectives
- Ensure that the pre-established review criteria have been met to ensure the production capability forms a satisfactory, affordable, and sustainable basis for proceeding into LRIP and FRP
- Advise the Program Manager on whether production capability forms a satisfactory, affordable, and sustainable basis for proceeding into LRIP and FRP

- Ensure adequate plans and resources are in place to proceed from PRR to PCA and FRP Decision Review (DR)
- Ensure plans to proceed to PCA and FRP DR allow for contingencies
- Ensure production implementation supports overall performance and maintainability requirements
- Monitor and control the execution of the PRR closure plans

Inputs and Review Criteria

Figure 4.2.15.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.15.F1. Weapon System Development Life Cycle



The PRR criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP no later than Milestone B. Table 4.2.15.T1 defines the suggested PRR products and associated review criteria. The review should not begin until these criteria are considered met and any prior technical review is completed and its action items closed. A readiness assessment tool for PRR preparation is the DoD PRR Checklist. This is a best practice review**.**

Table 4.2.15.T1. PRR Products and Criteria

Product	PRR Criteria
Cost Estimate	• System, as designed, is producible within the production budget • Production cost model is based on the stable detailed design and supply chain, and has been validated

Product	PRR Criteria
Risk Assessment	• Producibility trade studies and risk assessments are completed • Manufacturing, production, and quality risks are identified, and a mitigation plan exists to mitigate those risk(s) • Environment, Safety, and Occupational Health (ESOH) risks are known and mitigated
System Baseline Documentation (Product)	• System product baseline is stable and under proper configuration control to enable hardware fabrication in low-rate production • Technologies are mature and proven in the final form, in operational environments • Manufacturing processes are stable and have been demonstrated in a pilot line environment • Adequate production line processes and metrics are in place for the delivery of on-time, quality products
Technical Plans	• Prior readiness reviews are completed and action items closed • Supply chain is stable and adequate to support planned LRIP and FRP • Program is properly staffed with qualified production, quality (engineering and assurance), and manufacturing personnel • Product acceptance system, including acceptance test procedures and associated equipment, has been validated and put under configuration control • Production facilities are ready and required personnel are trained • Delivery schedule is executable (technical/cost risks, long lead items) • Diminishing Manufacturing Sources and Material Shortages (DMSMS) plan is in place and mitigates the risk of obsolescence during LRIP and FRP

A follow-on PRR may be appropriate in the Production and Deployment (PD) phase for the prime contractor and major subcontractors if:

- Changes (from the Engineering and Manufacturing Development (EMD) phase system design) in materials and/or manufacturing processes are required when entering or during the Production and Deployment (P&D) phase
- Production start-up or re-start occurs after a significant shutdown period
- Production start-up is with a new contractor
- The manufacturing site is relocated

The PRR is designed as a system-level preparation tool and should be used for assessing risk as the system transitions from development to FRP. For more information see the approaches described in DAG section 4.3.18.18. Producibility, Quality, and Manufacturing Readiness.

Outputs and Products

The Technical Review Chair determines when the review is complete. Results of the PRR and associated manufacturing readiness assessments are typically documented in a written report or out-brief. The results should be reported based on the criteria documented in the SEP, using the PRR checklist. Another source of information is the Manufacturing Readiness Level Deskbook to be used as appropriate.

4.2.16. Physical Configuration Audit

4.2.16. Physical Configuration Audit

The Physical Configuration Audit (PCA) is a formal examination to verify the "to be fielded" configuration of a validated system against its design and manufacturing documentation. The objective of the PCA is to resolve any discrepancies between the production-representative item that has successfully passed Operational Test and Evaluation (OT&E) and the associated documentation currently under configuration control. A successful PCA provides the Milestone Decision Authority (MDA) with evidence that the product design is stable, the capability meets end-user needs, and production risks are acceptably low. At the conclusion of the PCA, the final product baseline is established and all subsequent changes are processed by formal engineering change action. Further information can be found in MIL-HDBK-61A.

The PCA is an event-driven technical assessment and typically occurs during the Production and Deployment (P&D) phase, after successful system validation but prior to the Full-Rate Production Decision Review (FRP DR). A PCA conducted during FRP may miss the opportunity to avoid costly defects built into production. While the system-level PCA typically occurs before the FRP DR, other system element PCAs may be conducted at various points in advance of the system-level PCA.

A properly conducted and documented PCA provides a major knowledge point in preparation for investment decisions at FRP DR. The PCA confirms:

- Any testing deficiencies have been resolved and appropriate changes implemented; changes to the product baseline have been incorporated into current design documentation
- All production-related activities (tooling, acceptance/inspection equipment, instructions, molds, jigs, and make-buy decisions) are focused on a validated and accurate design
- Any system elements that were affected/redesigned after the completion of the Functional Configuration Audit (FCA) also meet contract requirements
- The manufacturing processes, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled

Roles and Responsibilities

The unique Program Manager responsibilities associated with a system PCA include:

- Approve, fund, and staff the PCA as planned in the Systems Engineering Plan (SEP) developed by the Systems Engineer
- Establish the plan to FRP DR in applicable contract documents including the SE Management Plan (SEMP), Integrated Master Schedule (IMS), and Integrated Master Plan (IMP)
- Ensure the plan includes independent subject matter experts to participate in each review
- Determine if the readiness of manufacturing processes, quality management system, and production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.) provide low-risk assurances for supporting FRP
- Continue to control Class I changes to the system product baseline (see DAG section 4.3.7. Configuration Management Process)

The unique Systems Engineer responsibilities associated with a system PCA include:

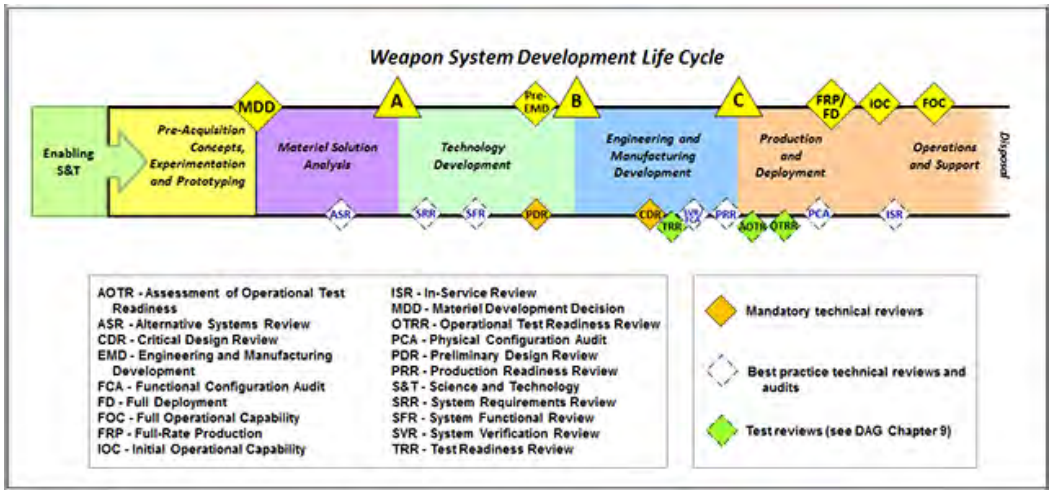
- Develop and execute the PCA plans with established quantifiable review criteria, carefully tailored to satisfy program objectives
- Coordinate with configuration management and manufacturing SMEs and the production contractor/production facility to develop an efficient approach to the PCA
- Identify method(s) of examining the production-representative item (e.g., disassembly, inspection, and reassembly) and verify the item against related design documentation
- Ensure that the pre-established review criteria have been met to ensure the production capability forms a satisfactory, affordable, and sustainable basis for proceeding with FRP
- Advise the Program Manager on whether production capability forms a satisfactory, affordable, and sustainable basis for proceeding into FRP
- Ensure adequate plans and resources are in place to get from PCA to Full Operational Capability (FOC)
- Ensure plans to get to FOC allow for contingencies
- Ensure production implementation supports overall performance and maintainability requirements
- Monitor and control the execution of the PCA closure plans

When the program does not plan to control the detailed design or purchase the item's technical data, the developer should conduct an internal PCA to define the starting point for controlling the detailed design of the item and establishing a product baseline.

Inputs and Audit Criteria

Figure 4.2.16.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.16.F1. Weapon System Development Life Cycle



The PCA criteria are developed to best support the program's technical scope and risk and are documented in the program's SEP no later than Milestone C. The PCA is conducted when these criteria are considered to be met.

Table 4.2.16.T1 defines the suggested PCA products and associated review criteria. The review should not begin until the Systems Engineer judges that all criteria have been met. The DoD PCA Checklist and can be used for assessing readiness for the audit. This is a best practice audit.

Table 4.2.16.T1. PCA Products and Criteria

Product	PCA Criteria
Verified Product Baseline Documentation	• Assessment that the system product baseline is complete and accurately reflects the configuration of the representative production item that was inspected and validated through OT&E
Risk Assessment	• Risks are identified and documented at levels low enough to continue with full-rate production and deployment
Technical Plans	• A detailed plan and schedule are established and sufficiently resourced to proceed with full-rate production and deployment

Outputs and Products

The Technical Review Chair determines when the review is complete. The primary output of the PCA is a verified product baseline that accurately reflects the validated system and supports a favorable FRP DR.

4.2.17. In-Service Review

4.2.17. In-Service Review

The In-Service Review (ISR) is a multidisciplined assessment to characterize the in-service health of the deployed system and enabling system elements (training, user manuals, documentation, etc.). The ISR provides feedback to the Program Manager on how well the system is delivering the capability to the warfighter, with acceptable operational performance. In addition, the feedback substantiates in-service support budget priorities.

DoDI 5000.02, Enclosure 2, 8.c.(1)(f) requires DoD Components to conduct continuing reviews to compare expected performance to actual performance. The ISR is typically conducted shortly after Initial Operational Capability (IOC); however, the Program Manager should schedule additional ISRs with the end user until the system is retired. Typical focus areas for additional ISRs might include: modifications, upgrades, product improvement, technology refresh, and technology insertion (see DAG Chapter 5 Life-Cycle Logistics for additional information). Additional ISRs are typically critical for systems that change more frequently, such as commercial-off-the-shelf and software-intensive systems. The DoD ISR Checklist can be used to plan and implement this review.

Roles and Responsibilities

The Program Manager establishes the relationships between the developer and the end-user to facilitate system feedback and assessment. In addition, the Program Manager determines priorities and approves changes and implementation plans.

The Systems Engineer supports efforts to translate end user feedback into corrective action plans for possible modifications, technology refresh and/or insertion, Diminishing Manufacturing Sources and Material Shortages (DMSMS) issues, and other types of system or system element improvements.

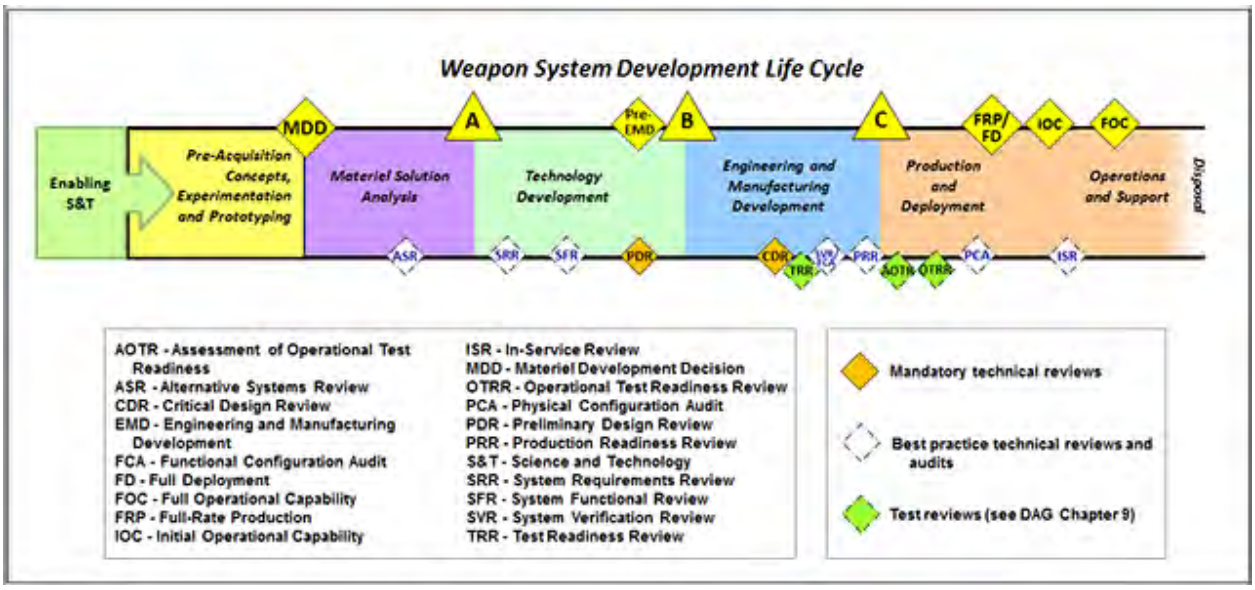
The ISR can be used to:

- Assess risk in the operational environment
- Identify trends in metrics to substantiate in-service budget or corrective actions

Inputs and Review Criteria

Figure 4.2.17.F1 provides the end-to-end perspective and the integration of SE technical reviews and audits across the acquisition life cycle.

Figure 4.2.17.F1. Weapon System Development Life Cycle



To enter an ISR, the review should not begin until these criteria are considered met:

- IOC status has been reached
- System hazard risk assessment has been performed (see DAG section 4.3.18.9. Environment, Safety, and Occupational Health)
- Trend assessment has been performed for preplanned technical metrics

Outputs and Products

The Technical Review Chair determines when the review is complete. The ISR should result in a plan of corrective action for all issues recommended by the Systems Engineer as warranting resolution. Areas of particular interest usually include:

- System problems are categorized and support the operating and support requirements determination process
- Required budgets (in terms of work years) are established to address all system problems in all priority categories
- Current levels of system operational risk and system readiness are quantified and related to current operations and systems and procurement budgets
- Future levels of system operational risk and system readiness are quantified and related to future operations and systems and procurement budgets

4.3. Systems Engineering Processes

4.3.1. Systems Engineering Processes Overview

4.3. Systems Engineering Processes

4.3.1. Systems Engineering Processes Overview

The systems engineering (SE) processes are used by contractor and Government organizations to provide a framework and methodology to plan, manage, and implement technical activities throughout the acquisition life cycle. SE planning and execution should focus on applying the processes and tools in a rigorous, integrated, and disciplined manner to achieve a system solution that balances performance, cost, schedule, and risk. The eight technical management processes provide a consistent framework for managing technical activities and identifying the technical information and events critical to the success of the program. The eight technical processes ensure the system design and the delivered capability reflect the requirements that the stakeholders have expressed. As a whole, the SE processes provide a systematic approach focused on providing needed capability to the operational end user. Successful implementation of the SE processes results in an integrated capability solution that is:

- Responsive to the needs of the user
- Balanced among multiple requirements, design considerations, and program costs and schedules
- Able to operate in complex system-of-systems (SoS) environments as required

All organizations performing SE should scale their application and use of these processes to the type of product or system being developed. This scaling should reflect the system's maturity and complexity, size and scope, life-cycle phase, and other relevant considerations. Disciplined application of the SE processes provides a technical framework that enables sound decision making, increases product knowledge and system maturity, and helps reduce risk. The following subsections, as indicated in Table 4.3.1.T1, discuss the SE processes in more detail.

Table 4.3.1.T1. Systems Engineering Processes (DAG Chapter 4 subsection)

Technical Management Processes	Technical Processes
Technical Planning (4.3.2)	Stakeholder Requirements Definition (4.3.10)
Decision Analysis (4.3.3)	Requirements Analysis (4.3.11)
Technical Assessment (4.3.4)	Architecture Design (4.3.12)
Requirements Management (4.3.5)	Implementation (4.3.13)
Risk Management (4.3.6)	Integration (4.3.14)
Configuration Management (4.3.7)	Verification (4.3.15)
Technical Data Management (4.3.8)	Validation (4.3.16)

Interface Management (4.3.9)	Transition (4.3.17)

Industry SE process standards that describe best practices in accomplishing SE include, but are not limited to, the following:

- ISO/IEC 15288, Systems and Software Engineering-System Life Cycle Processes
- ISO/IEC 26702, Application and Management of the Systems Engineering Process
- ISO/IEC/IEEE 42010, Architecture Description
- EIA 632, Processes for Engineering a System

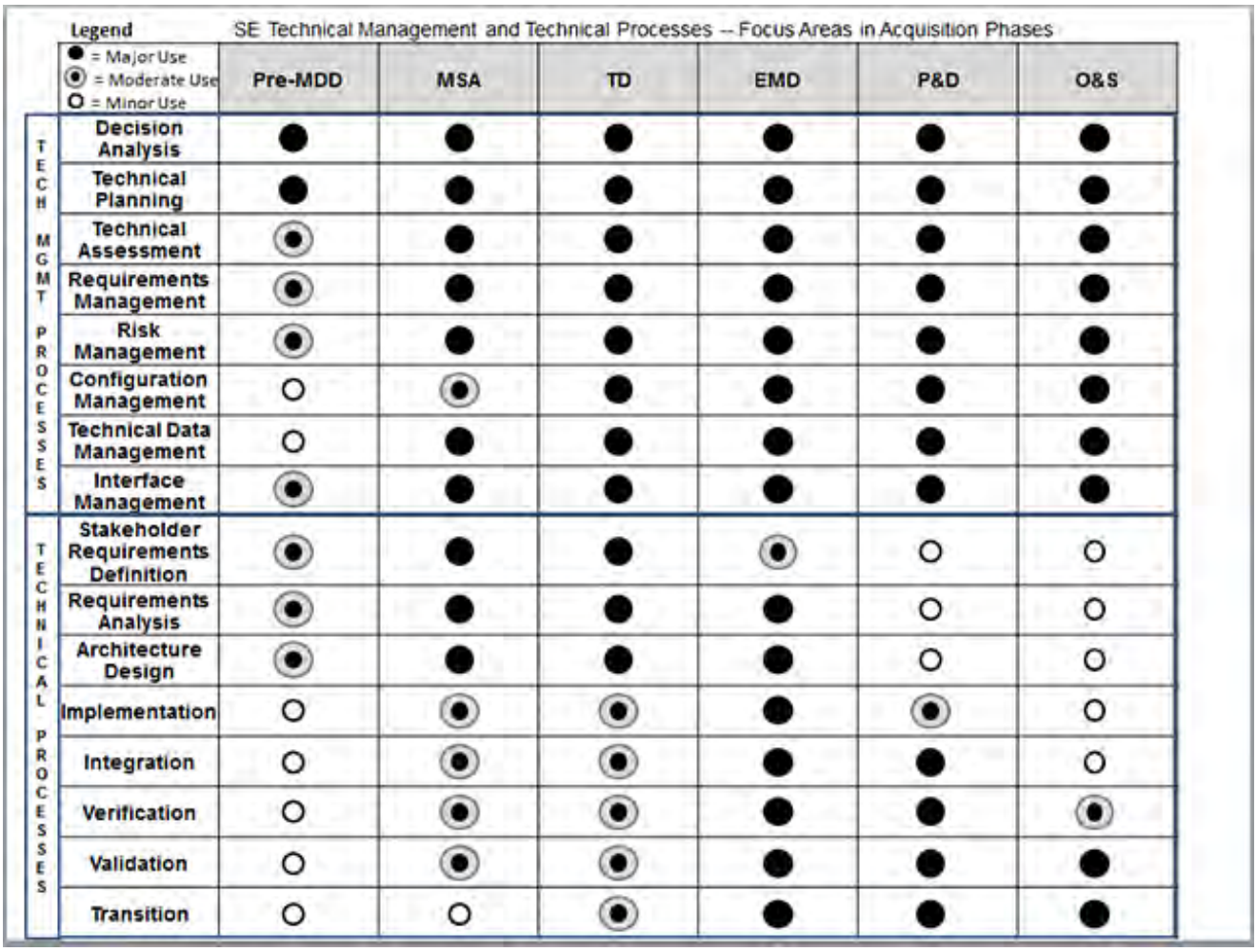
Roles, Responsibilities, and Activities

The Program Manager and Systems Engineer use the technical management processes as insight and control functions for the overall technical development of the system throughout the acquisition life cycle. They use the technical processes to design, create, and analyze the system, system elements, and enabling system elements required for production, integration, test, deployment, support, operation, and disposal.

The SE processes, and their constituent activities and tasks, are not meant to be performed in a particular time-dependent or serial sequence. The Program Manager and Systems Engineer apply the processes iteratively, recursively and in parallel (as applicable) throughout the life cycle to translate identified capability needs into balanced and integrated system solutions. The Systems Engineer is responsible for developing the plan and applying the SE processes across the program, monitoring execution throughout the life cycle, and taking necessary steps to improve process efficiency and effectiveness.

Table 4.3.1.T2 is a representation of how much effort is typically focused on each of the SE processes throughout the acquisition life cycle. The Program Manager and Systems Engineer should apply appropriate resources with requisite skill sets to ensure successful execution of each process.

Table 4.3.1.T2. Notional Emphasis of Systems Engineering Processes Throughout the Defense Weapon System Acquisition Life Cycle



Legend: ● = Major Use, ◉ = Moderate Use, ○ = Minor Use		SE Technical Management and Technical Processes -- Focus Areas in Acquisition Phases					
		Pre-MDD	MSA	TD	EMD	P&D	O&S
TECH MGMT PROCESSES	Decision Analysis	●	●	●	●	●	●
	Technical Planning	●	●	●	●	●	●
	Technical Assessment	◉	●	●	●	●	●
	Requirements Management	◉	●	●	●	●	●
	Risk Management	◉	●	●	●	●	●
	Configuration Management	○	◉	●	●	●	●
	Technical Data Management	○	●	●	●	●	●
	Interface Management	◉	●	●	●	●	●
TECHNICAL PROCESSES	Stakeholder Requirements Definition	◉	●	●	◉	○	○
	Requirements Analysis	◉	●	●	●	○	○
	Architecture Design	◉	●	●	●	○	○
	Implementation	○	◉	◉	●	◉	○
	Integration	○	◉	◉	●	●	○
	Verification	○	◉	◉	●	●	◉
	Validation	○	◉	◉	●	●	●
	Transition	○	○	◉	●	●	●

[4.3.2. Technical Planning Process]

4.3.2. Technical Planning Process

The Technical Planning process includes defining the scope of the technical effort required to develop, field, and sustain the system, as well as providing critical quantitative inputs to program planning and life-cycle cost estimates. Technical planning provides the Program Manager and Systems Engineer with a framework to accomplish the technical activities that collectively increase product maturity and knowledge and reduce technical risks. Defining the scope of the technical effort provides:

- An accurate basis for program cost and schedule estimates, documented in the Independent Cost Estimate (ICE), Cost Analysis Requirements Description

(CARD), and Acquisition Program Baseline (APB);
- A foundation for risk identification and management (see DAG section 4.3.6. Risk Management Process);
- Quantitative measures supporting the Technical Assessment process (see DAG section 4.3.4. Technical Assessment Process) identifying system maturity; and
- An accurately constructed and resourced IMS supporting the assignment of Earned Value.

The resulting program cost estimates and risk assessments are essential to support milestone decisions, establish the plan for accomplishing work against which contract performance is measured, and enable mandatory program certifications (e.g., section 2366a or section 2366b title 10 United States Code).

Technical planning includes the program's plan for technical reviews and audits (see DAG sections 4.2.8. through 4.2.17.). It should also account for resources (skilled workforce, support equipment/tools, facilities, etc.) necessary to develop, test, produce, deploy, and sustain the system.

Technical planning should be performed in conjunction with, and address, key elements and products of all the other SE processes to ensure the program's technical plan is comprehensive and coherent. For example, it should be used with the Technical Assessment process to evaluate the progress and achievements against requirements, plans, and overall program objectives. If significant variances are detected, this process includes re-planning as appropriate.

The Program Manager and Systems Engineer should ensure that technical planning remains current throughout the acquisition life cycle. They should initiate technical planning activities early in the life cycle prior to the Materiel Development Decision (see DAG section 4.2.2. Pre-Materiel Development Decision) and during the Materiel Solution Analysis (MSA) phase (see DAG section 4.2.3. Materiel Solution Analysis Phase). Beginning in MSA, programs begin to capture their technical planning in the Systems Engineering Plan (SEP) (see DAG section 4.1.2. Systems Engineering Plan), which is required at each milestone review from Milestone A to Milestone C. As the system matures and issues arise throughout the life cycle, the Program Manager and Systems Engineer should consistently look for root cause(s) and implement corrective actions in order to enable programmatic and technical success. Modifications to the SE processes and SEP may be required because of root cause and corrective action analysis and implementation.

Activities and Products

The Program Manager is ultimately responsible for all program plans. The Systems Engineer is responsible for:

- Developing, maintaining and executing the program's SEP
- Tracking alignment of the developer's Systems Engineering Management Plan

(SEMP)
- Providing key technical inputs and ensuring SEP alignment to other program plans (Technology Development Strategy/Acquisition Strategy (TDS/AS), Test and Evaluation Strategy/Test and Evaluation Master Plan (TES/TEMP), Life-Cycle Sustainment Plan (LCSP) and Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)

Technical Planning should reflect the context of the organization and comply with all applicable policies. The Program Manager and Systems Engineer should consider all relevant constraints when identifying technical tasks, sequencing these tasks, and estimating resources and budgets. Inputs to the technical planning process vary over time as the program evolves and the system matures. Technical Planning includes the following activities:

- Defining the scope and objectives of the technical effort
- Identifying constraints and risks
- Establishing roles and responsibilities
- Dividing the program scope and objective into discrete elements
- Identifying technical reviews and audits as well as their timing
- Establishing schedules and costs
- Preparing or updating planning documentation
- Scaling SE processes based on the scope and complexity of the program/system
- Identifying areas for potential tailoring (including rationale) for MDA approval

Key factors that the Systems Engineer should consider when accomplishing technical planning include:

- Capability needs (requirements, gaps, threats, operational context, concept of operations (CONOPS))
- The system concept or materiel solution
- Key interfaces and interdependencies that exist or need to be developed
- The acquisition approach and strategy, from both a business and a contract perspective
- The chosen engineering approach and development strategy
- The test and evaluation approach and strategy, for both developmental and operational testing (See DAG Chapter 9 Test and Evaluation for additional information regarding interactions with the Chief Developmental Tester)
- Program management approach, including organization, processes, and products
- External dependencies and agreements with other systems or organizations that may be in place
- Need date
- Availability of resources, including funds, personnel, facilities, etc.
- Program risks
- Risk mitigation and shrinkage strategies

In addition to the SEP, the technical planning effort supports the development of the following documents:

- Work Breakdown Structure (see DAG section 4.3.2.1. Work Breakdown Structure) - a framework for specifying program objectives
- Integrated Master Plan (see DAG section 4.3.2.2. Integrated Master Plan/Integrated Master Schedule) - an event-based plan consisting of a hierarchy of program events that need to be accomplished
- Integrated Master Schedule (see DAG section 4.3.2.2. Integrated Master Plan/Integrated Master Schedule) - an integrated, networked schedule that contains all lower-level tasks required to support program events

Other useful resources available to assist the Program Manager and Systems Engineer in the Technical Planning process can be found in the "Guidance & Tools" section of the ODASD(SE) Policy and Guidance website.

4.3.2.1. Work Breakdown Structure

4.3.2.1. Work Breakdown Structure

The Work Breakdown Structure (WBS) provides a consistent and visible framework for materiel items and contracts within a program throughout its life cycle. It provides a product-oriented division of tasks by breaking down work scope for authorization, tracking, and reporting purposes. The WBS is defined, developed, and maintained throughout the acquisition life cycle based on a disciplined application of the systems engineering (SE) process. The goal is to develop a WBS that defines the logical relationship among all program elements to a specified level. The WBS integrates technical, cost, and schedule parameters, giving the Program Manager a tool to:

- Ensure traceability of all program activities
- Identify significant risk drivers
- Forecast cost and schedule performance
- Develop corrective action plans as needed

There are two types of WBS: (1) the Program WBS and (2) the Contract WBS (including flow-down reporting requirements). The Program WBS provides a framework for specifying program objectives. Each WBS element provides logical summary levels for assessing technical accomplishments, for supporting the required event-based technical reviews, and for measuring cost and schedule performance. It represents the entire program from the Government Program Manager’s responsibility. The contract WBS is the Government - approved WBS for program reporting purposes and includes all program elements (for example, hardware, software, services, data, or facilities), which are the contractor’s responsibility. It includes the contractor’s discretionary extension to lower levels, in accordance with Government direction and the contract Statement of Work (SOW). The WBS depicts the system as a product-oriented tree, which may be found in a system model. Requirements for developing a WBS are found in MIL-STD-

881C. The Program Manager, in conjunction with the Systems Engineer, should develop a comprehensive WBS early in the program to support planning, cost and schedule estimates, and risk mitigation activities.

The WBS provides a common thread for the Earned Value Management System (EVMS), the Integrated Master Plan (IMP) and the Integrated Master Schedule (IMS), allowing consistency in understanding and communicating program cost and schedule performance. Additional information about EVMS can be found in DAG Chapter 11 Program Management Activities.

Planning tasks by WBS elements serves as the basis for mapping the development of the technical baseline for estimating and scheduling resource requirements (people, facilities, and equipment). By breaking the system into successively smaller pieces, the Program Manager can ensure all system elements and enabling system elements are identified in terms of cost, schedule, and performance goals in order to reduce risk.

4.3.2.2. Integrated Master Plan/Integrated Master Schedule

4.3.2.2. Integrated Master Plan/Integrated Master Schedule

The Integrated Master Plan (IMP) is an event-driven Government document that provides a framework against which all work is accomplished. The IMP aids in defining and documenting tasks required to define, develop, and deliver a system, and to facilitate operation and support of that system throughout its life cycle. The IMP format usually reflects an event - accomplishment - criteria hierarchical structure for program tracking and execution.

The Integrated Master Schedule (IMS) is an event-driven (not time-driven) document primarily focused with product and process development that is resource loaded and includes margin for risk mitigation. The IMS supplements the IMP and is based on the WBS. The IMS describes the work required to complete the effort in sufficient detail to fully demonstrate understanding of the scope and flow of the work, and it enables the Program Manager to better understand the links and relationships among the various activities and the resources supporting them.

DoDI 5000.02 requires use of the IMS, and the Integrated Master Plan and Integrated Master Schedule Preparation and Use Guide provides additional guidance on developing and implementing these technical planning tools.

A program should have an adequate IMP and IMS and should require the same from its contractor(s). The IMP and IMS communicate the expectations of the program team and provide traceability to the management and execution of the program by IPTs. They also provide traceability to the WBS, the contract WBS (CWBS), the Statement of Work (SOW), systems engineering (SE), and risk management, which together define the products and key processes associated with program success.

The IMP and IMS represent the basis for contractor cost reporting and the associated assessments of contract performance, as defined at the Integrated Baseline Review (IBR) (see DAG Chapter 11 Program Management Activities). The IMP and IMS help the Program Manager and Systems Engineer:

- Identify a baseline for program monitoring, reporting, and control
- Plan, execute, and track risk mitigation efforts
- Support resource analysis and leveling, exploration of alternatives, and cost/schedule trade-off studies
- Provide a roadmap for stakeholders
- Enable effective communication within the Government team and with the developer

Activities and Products

The IMP documents the significant criteria necessary to complete the accomplishments, and ties each to a key program event. The IMS expands on the IMP with an integrated network of tasks, subtasks, activities, schedule for deliverables, and milestones with sufficient logic and durations. The IMS also serves as a tool for time-phasing work and assessing technical performance. IMS activities are thus traceable to the IMP and the WBS, and allow integrated assessments of cost, schedule, technical performance, and associated risks. This traceability serves to:

- Identify critical path, milestones, and activities
- Indicate significant constraints and relationships
- Provide current status and forecast completion dates of scheduled work to enable comparison of planned and actual program accomplishments
- Establish a schedule baseline
- Provide horizontal traceability of interrelationships among activities
- Provide interdependent sequencing of all work authorized on the contract in a manner compatible with IMP events and/or key milestones

The IMP and IMS support effective management of program scope, risk, and day-to-day efforts. During the initial stages of a program, the IMP provides an early understanding of the required scope of work, key events, accomplishment criteria, and the likely program structure by depicting the progression of work through the remaining phases. Regular examination of the plan and schedule increases the documented level of detail and provides confidence that these documents have properly identified and captured all essential activities.

Early identification of and adherence to critical path tasks is essential to ensure that the program remains on track toward achieving schedule and cost goals. The IMS provides linkages between tasks to capture the relationship of predecessor and successor tasks required to initiate or complete major tasks. The IMP and IMS collectively assist stakeholder communication by establishing expectations and dependencies, particularly

for tasks performed by different organizations.

The Program Manager and Systems Engineer should determine an appropriate level of detail for the IMS. For low-risk programs, developing the IMS at too high a level of detail may fail to show critical path tasks. The IMS for a high-risk program would most likely show lower levels of detail to aid risk management/mitigation efforts but would typically carry a greater maintenance cost (tracking progress and updating status).

The initial IMP and IMS should address significant activities to provide a basis for conducting further risk assessments including identification of tasks associated with moderate to high risks that may emerge later in the life cycle. The IMS should be seen as a tool used by stakeholders during each phase of the program. The IMS should identify all risk mitigation activities for easy identification and tracking.

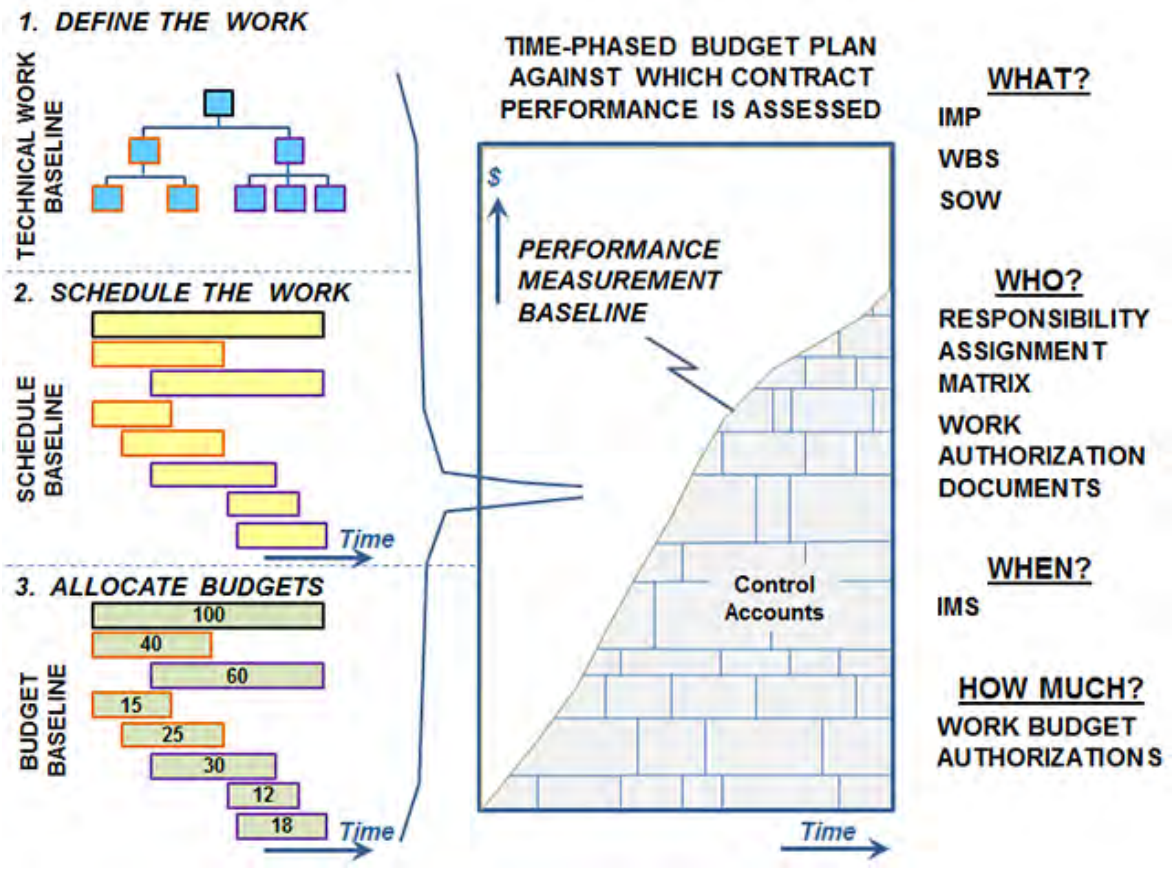
The Program Manager and Systems Engineer should monitor development of the IMS by the developer to ensure that activity durations and resources are reasonable. This oversight aids risk analysis and development of mitigation plans in the event that any of those activities become delayed or over budget. The initial IMP should be part of the preparation for the Milestone A decision.

The Systems Engineer also defines functional and life cycle inputs to integrate SE processes and products and to provide an auditable sequence of tasks and schedules that can be used to measure cost and schedule status. The development and analysis of program IMP/IMS data:

- Permit assessments of the developer's SE processes, activities, efforts, and products
- Contribute to a better understanding of the technical basis of cost and schedule variances
- Provide a framework for developing corrective actions

Figure 4.3.2.2.F1 depicts a hierarchical approach to developing and populating the IMP/IMS.

Figure 4.3.2.2.F1. IMP/IMS Hierarchy and Content



The Program Manager should review the IMP and IMS for completeness, consistency, and compatibility. In this review, the Program Manager should evaluate duration and logic relationships to ensure they accomplish program goals, identify risks, and achieve desired mitigation.

The Systems Engineer should ensure that the SEP and other technical planning documents capture technical review criteria, event-driven outcomes, and mechanisms for assessing technical maturity and risk in a manner consistent with tasks and schedules identified in the IMP/IMS.

4.3.3. Decision Analysis Process

4.3.3. Decision Analysis Process

The Decision Analysis process transforms a broadly stated decision opportunity into a traceable, defendable, and actionable plan. It encompasses one or more discrete analyses at one or more lower (e.g., system element) levels and aggregates them into a higher-level view (e.g., system "scorecard" presentation) relevant to the decision maker and other stakeholders. Decision Analysis can be the central process for formulating,

managing, and executing an effective and efficient program at any point in the life cycle.

Decision Analysis and associated trade studies should be integrated with, and mutually supportive of, aspects of several SE processes in the early stages of the program, in particular:

- Technical Planning (see DAG section 4.3.2. Technical Planning Process)
- Technical Assessment (see DAG section 4.3.4. Technical Assessment Process)
- Stakeholder Requirements Definition (see DAG section 4.3.10. Stakeholder Requirements Definition Process)
- Requirements Analysis (see DAG section 4.3.11. Requirements Analysis Process)
- Architecture Design (see DAG section 4.3.12. Architecture Design Process)

A well-executed decision analysis or trade study helps the Program Manager and the Systems Engineer understand the impact of various uncertainties, identify one or more course(s) of action that balance competing objectives, and objectively communicate the results to decision makers. As such, it provides the basis for selecting a viable and effective alternative from among many under consideration.

Decision Analysis applies to technical decisions at all levels, from evaluating top-level architectural concepts to sizing major system elements to selecting small design details. The breadth and depth of the analysis should be scaled to both the scope of the decision and the needs and expectations of the decision maker(s).

Activities and Products

Decision Analysis teams generally include a lead analyst with a suite of reasoning tools; subject matter experts with access to appropriate models and analytical tools; and a representative set of end users and other stakeholders. A robust Decision Analysis process acknowledges that the decision maker has full responsibility, authority, and accountability for the decision at hand.

Decision Analysis typically includes the following steps:

- Review requirements and assumptions to establish the overall decision context
- Frame/structure the decision in terms of supporting program/project objectives
- Identify methods and tools to be used in the analyses (see DAG section 4.3.19. Tools and Techniques)
- Develop decision criteria (objectives and measures), criteria weight, and associated rationale
- Convey and track assumptions
- Identify and define alternatives to be evaluated (for high-level analyses these are generally directed, although additional ones may arise during the course of the analysis)
- Analyze and assess alternatives against criteria

- Synthesize results
- Analyze sensitivities
- Develop decision briefing with action/implementation plan(s)
- Make appropriate recommendation(s) to decision maker as expected/requested

Sound recommendations and action plans are the principal output of a well-framed and well-executed Decision Analysis process. The ability to drill down quickly from overall trade space visualizations to detailed analyses that support the synthesized views is particularly useful to decision makers in understanding the basis of observations and conclusions.

4.3.4. Technical Assessment Process

4.3.4. Technical Assessment Process

The Technical Assessment process allows the Systems Engineer to compare achieved results against defined criteria to provide a fact-based understanding of the current level of product knowledge, technical maturity, program status, and technical risk. This assessment results in a better understanding of the health and maturity of the program, giving the Program Manager a sound technical basis upon which to make program decisions.

Disciplined technical assessment activities should begin early in the life cycle. They should initially examine the status of development planning activities and efforts in the Materiel Solution Analysis (MSA) phase. During the Technology Development (TD) and Engineering and Manufacturing Development (EMD) phases, technical assessment can provide a basis for tracking development of the system and lower-level system element designs. Disciplined technical assessment supports the establishment of the various baselines and the achievement of system verification. Technical assessment activities are also used in manufacturing and production activities during the Production and Deployment (P&D) phase, and these activities continue through the Operations and Support (O&S) phase in support of reliability growth and sustainment engineering efforts.

The Program Manager and Systems Engineer evaluate technical maturity in support of program decisions at the key event driven technical reviews and audits (see DAG sections 4.2.8. through 4.2.17.) that occur throughout the acquisition life cycle. The Program Manager and Systems Engineer use various measures and metrics, including Technical Performance Measures (TPM) and leading indicators, to gauge technical progress against planned goals, objectives, and requirements. See DAG sections 4.3.4.1. Technical Measurement and Metrics and 4.3.4.2. Technical Performance Measures for more information on measures/metrics and TPMs, respectively. The Program Support Review (PSR) (see DAG section 4.3.4.3. Program Support Review) is an assessment to identify and resolve planning and execution issues well before an upcoming acquisition milestone review.

Technical assessments against agreed-upon measures enable data-driven decisions. Evidence-based evaluations that communicate progress and technical risk are essential for the Program Manager to determine the need for revised program plans or technical risk mitigation actions throughout the acquisition life cycle.

Technical Assessment provides:

- A determination of the program's progress against plans (resource, schedule, and performance)
- A basis to identify and quantify technical risks
- A rigorous method to define corrective actions that may be needed to address and resolve identified technical risks

Activities and Products

The Program Manager should ensure that technical assessments occur throughout the life cycle, and that appropriate resources are available to allow for program office personnel and independent subject matter experts to participate. The Program Manager and Systems Engineer should jointly plan for event-driven technical reviews and audits. Review criteria (e.g., completion of baseline documents and artifacts appropriate for the review) should support objective assessments of technical progress, maturity, and risk.

When required, the Program Manager should approve the performance measurement baseline (PMB) (see DAG Chapter 11 Program Management Activities) to capture time-phased measures against the Work Breakdown Structure (WBS) (see DAG section 4.3.2.1. Technical Measurement and Metrics) and a resource-allocated Integrated Master Schedule (IMS) (see DAG section 4.3.2.2. Integrated Master Plan/Integrated Master Schedule).

The Systems Engineer assists the Program Manager in planning and conducting the Technical Assessment process. This includes advising on technical reviews and audits, defining the technical documentation and artifacts that serve as review criteria for each review/audit, and identifying TPMs. Specific activities include:

- Establishing event-driven technical planning
- Identifying appropriate measures and metrics
- Identifying performance measures to assess program health and technical progress
- Conducting analyses to determine risk and to develop risk mitigation strategies
- Conducting assessments of technical maturity, process health and stability, and risk to communicate progress to stakeholders and authorities at key decision points
- Proposing changes in the technical approach to address risk mitigation activities
- Advising the Program Manager regarding the technical readiness of the program to proceed to the next phase of effort
- Obtaining independent subject matter experts as appropriate for reviews and

audits

Technical assessments have close linkages to the Technical Planning and Decision Analysis processes (see DAG section 4.3.2. Technical Planning Process and 4.3.3. Decision Analysis Process, respectively); however, all SE processes (see DAG sections 4.3.2. through 4.3.17.) support activities that contribute to the assessment of program status, technical maturity, and risk in various areas (e.g., schedule, technology, manufacturing, threat).

Inputs to the Technical Assessment process should include approved program plans "(e.g., Acquisition Program Baseline, Systems Engineering Plan, TPMs, etc.), engineering products (i.e., drawings, specifications and reports, prototypes, system elements, and engineering development modules), and current performance metrics. Outputs may include various reports and findings (e.g., technical review reports, corrective actions, Program Support Review findings, or test reports).

4.3.4.1. Technical Measurement and Metrics

4.3.4.1. Technical Measurement and Metrics

Technical Measurement is the method of collecting and providing information to Program Managers and Systems Engineers at predefined intervals for decision making. Metrics constitute the data that identify the need for improvement (i.e., the facts and trends of process performance) and provide a basis for assessing the improvements.

Measures and metrics assist the Program Manager and the Systems Engineer in efforts to obtain insight into issues that have real or projected impacts on cost, schedule, performance, and risk. These issues can be at any level: the entire system, any of the various system elements or enabling system elements, and any or all of the SE processes in use across the program. This insight enables the Program Manager and others in leadership positions to make informed decisions.

Analysis of technical measures and metrics, in terms of progress against established plans, can reveal trends and provide indicators of future results. The Program Manager and Systems Engineer can use these trends and indicators to assess risk and make appropriate changes to program planning to mitigate potentially unfavorable outcomes.

Activities and Products

Programs document their strategy for identifying, prioritizing, and selecting the set of metrics for monitoring and tracking SE activities and performance in the Systems Engineering Plan (SEP). The measures/metrics strategy should include:

- An overview of the measurement planning and metrics selection process appropriate for the life-cycle phase
- The approach to monitor execution to the established plan

- Identification of roles, responsibilities, and authorities

The SEP requires two types of defined metrics:

- Technical Performance Measures (TPM) derived from Key Performance Parameters (KPPs) and Key System Attributes (KSAs) aid in assessing product maturity (see DAG section 4.3.4.2. Technical Performance Measures)
- Technical progress (at both the system and system element levels) should address product knowledge and therefore vary by phase throughout the life cycle

In addition to TPMs and product measures, the Program Manager and the Systems Engineer should ensure that technical planning identifies measures, metrics, and leading indicators to assess the effectiveness of SE process execution within both the Government program office and the developer's SE organization. TPMs should be managed by the cognizant Integrated Product Team (IPT).

Areas in which measures and metrics should be monitored include but are not limited to:

- Software metrics (e.g., size, complexity, reuse, defects, productivity)
- Hardware metrics (space, weight and power (SWaP), processing margin, axle loading, available RAM, etc.)
- Technical staffing
- Technology maturity
- Affordability
- Risk Mitigation
- Schedule
- Quality / manufacturing / production measures (e.g., defects, first pass yields, process escapes)
- Infrastructure measures (e.g., capacity, availability, utilization of facilities and equipment)
- Design/development process measures (e.g., drawing releases, software modules, subsystem integration tasks, defined/documented interfaces, deviations, waivers, etc.)

4.3.4.2. Technical Performance Measures

4.3.4.2. Technical Performance Measures

Technical Performance Measures (TPMs) are a subset of metrics and measures that evaluate technical progress (i.e., product maturity). TPM data support evidence-based decisions at key knowledge points such as technical reviews and audits or milestone decisions. TPMs compare the actual versus planned technical development and design. They report progress in the degree to which system performance requirements are met. Systems engineering (SE) uses TPMs to balance cost, schedule, and performance throughout the life cycle when integrated with other management methods such as the

Work Breakdown Structure (WBS) and Earned Value Management System (EVMS).

Effective TPMs support assessment of design and integration progress toward achieving Key Performance Parameters (KPPs) and Key System Attributes (KSAs). Subjective items such as improved quality, management responsiveness, or timeliness are difficult to measure and are not suitable as TPMs. Regular progress assessments toward meeting TPMs should occur in management reviews with formal documentation in technical reports and test data.

The program's Systems Engineering Plan (SEP) includes a minimum set of TPMs and the plan to achieve them. The planning should show TPM values as a function of time, aligned with key points in the program schedule (e.g., technical reviews). Decision makers can see progress toward achieving the KPPs and KSAs by reviewing actual values (achieved through analysis, test, demonstration, or other measurement) against planned values.

Each parameter selected as a TPM should:

- Have a time-phased profile with tolerance bands that can be predicted and substantiated during design, development, and test
- Be directly measurable during testing or readily derivable from analysis
- Be derived from the functional baseline and/or allocated baseline
- Provide an indication of risk associated with the system's ability to meet specified performance requirements
- Be written using statistical criteria whenever possible

Activities and Products

Systems Engineers from both the Government and the developer, in consultation with the end user, identify a limited number of parameters for consideration as TPMs. This generally occurs as part of the Architecture Design process (see DAG section 4.3.12. Architecture Design Process), in conjunction with development of the physical architecture and allocation of requirements to system elements. As the program matures, the Technical Assessment and Risk Management processes (see DAG sections 4.3.4. Technical Assessment Process and 4.3.6. Risk Management Process, respectively) should inform the Program Manager and the Systems Engineer of progress on risk mitigation actions, as well as emerging risks that could warrant adding attributes that map to a medium or high risk on the list of TPMs.

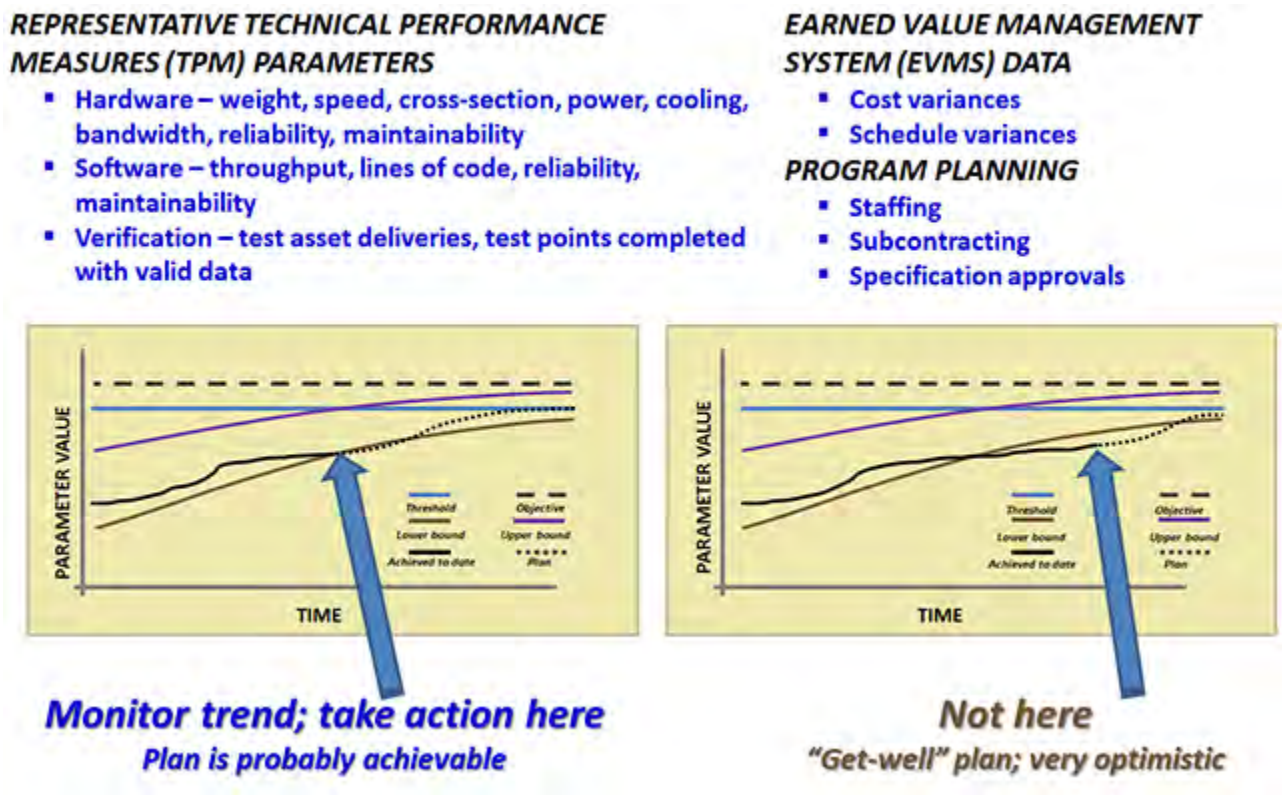
The Program Manager, in coordination with the Systems Engineer and developer, approves selected TPMs. The Program Manager should appropriately delegate responsibility for management and reporting TPMs. The Systems Engineer defines, collects, and analyzes performance measurement data for all TPMs to assess performance over time against threshold and objective values. The Systems Engineer should assess all TPMs at each technical review and audit.

The technical effort documented in the SEP should reflect the events and measurement activities needed for TPM reporting. TPM tracking should be an integral part of the developer's technical planning, and contractors should capture TPM tracking in their Systems Engineering Management Plan (SEMP).

TPM reporting should be in terms of actual versus planned progress, plotted as a function of time and aligned with key points in the program schedule (e.g., technical reviews). A continuous (historical) plot of planned and actual values for each TPM, Earned Value Management System (EVMS) data, and program planning information enables assessment of performance trends (i.e., progress-to-plan relationships with respect to both objective and threshold values).

Figure 4.3.4.2.F1 depicts how leading indicators can influence risk mitigation activities.

Figure 4.3.4.2.F1. Leading Indicators Influence Risk Mitigation Planning



4.3.4.3. Program Support Review

4.3.4.3. Program Support Review

The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) conducts PSRs on ACAT ID and IAM programs to help shape the program's technical planning and management approaches. Like any independent

review, the PSR is a technical assessment tool intended to prevent problems by early recognition of risks and identification of proposed mitigation activities. PSR requirements appear in DoDI 5000.02.

Early conduct of PSRs should help the Program Manager identify and resolve any program planning or execution issues well before major program decisions. Table 4.3.4.3.T1 lists important PSR attributes.

Table 4.3.4.3.T1 PSR Attributes

Cross-functional	• No "stovepipes" • All reviewers look at multiple areas • All observations and comments are adjudicated with the entire team and program office
Multidisciplinary	• Wide range of functional representation (internal ODASD(SE), AT&L, consultants) • Wide range of reviewer expertise • Multiple reviews look at each area
Independent	• Minimize "program experts" • No Government or contractor competitors • No program advocates or antagonists
Consistent	• Essential to identify and understand common issues • Ensure all potential risks are considered • Treat all programs equally and fairly
Tailorable	• Adapt to type of review • Adapt focus on identified issues

Activities and Products

When practical, the initial PSR occurs nine to twelve months before a milestone decision review; a follow-up review (two to three months prior to the milestone) assesses the implementation of key recommendations and mitigation of risks in order to improve program planning and execution. The PSR typically consists of two- to three-day visits to the program office (and developer(s) as applicable).

PSRs focus on all SE processes appropriate to the life-cycle phase but are broader in scope to consider all aspects of acquisition management, including resource planning, management methods and tools, earned value management, logistics, and other areas. The Defense Acquisition Program Support (DAPS) Methodology is a source for tailorable criteria and review questions and helps ensure consistency in reviews. The DAPS Methodology includes:

- Mission capabilities / requirements generation
- Resources
- Management
- Technical planning and process
- Program performance

Insights from PSRs aid the development of the Systems Engineering Plan (SEP) (see DAG section 4.1.2. Systems Engineering Plan) and the Request for Proposals (RFPs), and ensure that the program has adequately addressed SE equities in these documents. After its engagement with the program in preparation for the pre-Milestone A PSR, the ODASD(SE) staff maintains continuous engagement with the program to monitor its execution of the planning reflected in the SEP. PSRs prior to Milestones B, C, and the Full-Rate Production decision can make use of information already vetted during SE WIPT meetings, various technical reviews (see DAG sections 4.2.8. through 4.2.14.), and program management reviews in order to help reduce the PSR burden on the program office and developer staff. PSR action items are documented in the milestone review's Acquisition Decision Memorandum.

4.3.5. Requirements Management Process

4.3.5. Requirements Management Process

Programs should maintain a current and approved set of requirements over the entire acquisition life cycle. The Requirements Management process helps ensure delivery of capability that meets intended mission performance to the operational end user.

The end-user needs are usually identified in operational terms at the system level during implementation of the Stakeholder Requirements Definition and Requirements Analysis processes; see DAG section 4.3.10. Stakeholder Requirements Definition Process and 4.3.11. Requirements Analysis, respectively. Through the Requirements Management process, the Systems Engineer tracks requirements changes and maintains traceability of end-user needs to the system performance specification and ultimately the delivered capability. As the system design evolves to lower levels of detail, the Systems Engineer traces the high-level requirements down to the system elements through the lowest level of the design. Requirements Management provides bottom-up traceability from any derived lower-level requirement up to the applicable source (system-level requirement) from which it originates. This bidirectional traceability is the key to effective management of system requirements. It enables the development of an analytical understanding of any system-wide effects of changes to requirements for a given system element, updating requirements documentation with rationale and impacts for approved changes. At the same time, bi-directional traceability ensures that approved changes do not create any "orphaned" lower-level requirements (i.e., that all bottom-up relationships to applicable system-level requirements remain valid after the change). Bidirectional traceability also ensures that higher-level requirements are properly flowed to lower-level requirements and system element designs so that there are no "childless parent" higher-level requirements (i.e., each high-level requirement is

ultimately being addressed by lower-level requirements and system element designs).

Robust Requirements Management, implemented in synchronization with the program's Configuration Management process (see DAG section 4.3.7. Configuration Management Process), can help the program to avoid or mitigate unintended or unanticipated consequences of changes through rigorous documentation of the system performance specification. Thoughtful analysis and management of requirements can help the lay foundation for system affordability.

Activities and Products

The Program Manager should keep leadership and all stakeholders informed of cost, schedule, and performance impacts associated with requirement changes and requirements growth.

The Systems Engineer establishes and maintains a Requirements Traceability Matrix (RTM) that captures all requirements in the system performance specification, their decomposition/derivation and allocation history, and rationale for all entries and changes. The requirements should be:

- Traceable to and from the stated user needs
- Correctly allocated, with potential effects of proposed changes fully investigated, understood, and communicated to the Program Manager
- Feasibly allocated, i.e., lower-level system elements cannot have the same or wider tolerance bands as those of the higher-level system elements into which they are incorporated

All affected stakeholders and decision makers should fully understand the effects of proposed changes to requirements at the system or system element level before they accept any changes for incorporation into the design. The RTM provides significant benefits during trade-off analysis activities since it captures the system-wide effects of proposed changes to established requirements.

DAG section 4.3.19. Tools and Techniques contains information about SE tools generally employed in the Requirements Management process. There are many commercial software packages specifically designed for the traceability aspect of Requirements Management, from top-level operational requirements down to the lowest-level system elements in the Work Breakdown Structure.

4.3.6. Risk Management Process

4.3.6. Risk Management Process

The Risk Management process is the overarching process that encompasses identification, analysis, mitigation planning, mitigation plan implementation, and tracking of program risks. Risk management is the primary method of mitigating program

uncertainties and is therefore critical to achieving cost, schedule, and performance goals at every stage of the life cycle. Effectively managing risks helps the Program Manager and Systems Engineer develop and maintain a system's technical performance, and ensure realistic life-cycle cost and schedule estimates.

DoDI 5000.02 requires that technical and programmatic risks be managed in all life cycle phases. A program's Technology Development Strategy (TDS) or Acquisition Strategy (AS), and Systems Engineering Plan (SEP) should address risks and should describe the program's risk management process. DAG section 4.3.18.9. Environment, Safety, and Occupational Health contains information regarding ESOH related risk management.

Risk Management is most effective when fully integrated with the program's SE and management processes. Identification of risk drivers, dependencies, root causes, and corrective action, as well as consequence management are key elements of this integration.

By definition, a risk is an unwanted event that may or may not occur in the future. A risk has three components:

- A future (yet-to-happen) root cause that, if corrected or eliminated, would be prevented along with its potential consequences
- A probability (or likelihood), assessed at the present time, of that future root cause occurring
- The consequence (or impact) of that future occurrence

A "Condition-If-Then" construct expresses risk as a function of its root cause, probability, and consequence. This construct generally reveals opportunities to not only mitigate the potential consequences of the risk occurring but also eliminate its root cause(s). As a best practice, risk mitigation plans should focus more on the causal factors that enable the risk's existence rather than on consequence management. Eliminating the root cause of a risk avoids its consequences.

A risk is an unwanted future event that may or may not occur, meaning it has a probability of occurrence of less than one. An issue is an unwanted event that has occurred or is certain to occur in the future (in other words, a probability equal to one). Thus, an issue differs from a risk only in that it is not a probabilistic event. While Program Managers and Systems Engineers can use Risk Management approaches to deal with issues, they should remember that issue management applies resources to current issues or problems. In contrast, risk management proactively applies resources to identify and mitigate future potential root causes and their consequences. Risk management includes the condition when mitigation attempts fail and the risk is realized. The challenge for the Program Manager and Systems Engineer is to balance how they choose to deal with issues and risks, since they encounter both over the life of the program. The Program Manager and Systems Engineer should clearly define, assess, and consider technical and programmatic off ramps if the program cannot be

adequately advanced given schedule and budget.

Activities and Products

Because risks can occur in any aspect of a program, it is important to recognize that all program team members and stakeholders have a responsibility to identify risks and report them to the Program Manager and Systems Engineer. Stakeholders also should be invited to participate in risk analysis and mitigation activities as requested or directed.

The Systems Engineer is responsible for prioritizing identified technical risks and developing mitigation actions. The Program Manager reviews and approves the risk priorities and mitigation plans and ensures required resources are available to implement the mitigation plans.

Risk Management encompasses several significant activities as outlined in Table 4.3.6.T1.

Table 4.3.6.T1. Risk Management Process Activities

Activity	Intent is to answer the question
Risk Identification	What can go wrong? What is the root cause?
Risk Analysis	How big is the risk? What is the probability of occurrence? What is the consequence of occurrence?
Risk Mitigation Planning	What is the program approach (cost, schedule, and technical) for addressing this potential root cause or unfavorable consequence?
Mitigation Plan Implementation	How can the planned risk mitigation be implemented? How do we ensure successful risk mitigation occurs?
Risk Tracking	How are risk mitigation plans going?

Early identification of affordability risk drivers is critical to program success. The investigation of both budgetary (long-term) and cost (near-term) aspects of affordability should continue throughout the acquisition life cycle. The Program Manager and Systems Engineer should carefully examine the technical trade space around budget and cost drivers for opportunities to eliminate or manage affordability concerns before they materialize. See DAG section 4.3.18.2. Affordability - Systems Engineering Trade-Off Analyses for more information on SE trades related to affordability.

Additional information on Risk Management is available in:

- Risk Management Guide for DoD Acquisition (Also see DAG Chapter 11 Program Management Activities for more information on the Program Manager's role in Risk Management)

- MIL-STD-882E, "DoD Standard Practice for System Safety", May 11, 2012
- Joint Capabilities Integration and Development System (JCIDS) Manual (requires Common Access Card (CAC) to access website), January 19, 2012

Table 4.3.6.T2 provides insights into the emphasis of Risk Management throughout the acquisition life cycle. Regardless of phase, several best practices may apply to a program's Risk Management process:

- As designs mature, understanding of schedule alignment, integration challenges, and programmatic functions increase, allowing the decision makers to better assess the risks associated with a given approach.
- Trade studies at various levels (e.g., technology maturation approaches, contracting strategy, material selections, etc.) provide decision support information in the context of risk and affordability throughout the life cycle. See DAG sections 4.3.3. Decision Analysis Process and 4.3.18.2. Affordability - Systems Engineering Trade-Off Analyses for additional information.
- Supply chain risk management (SCRM) should occur throughout the acquisition life cycle. SCRM includes working with appropriate DoD and Office of the Director of National Intelligence (ODNI) organizations on program threats (foreign and counterintelligence), technology vulnerabilities, contractor threat assessments, counterintelligence vulnerabilities, and global distribution risks.
- Quality risks throughout the supply chain can have a drastic impact on performance, cost, and schedule, as well as overall customer satisfaction. Robust quality management systems and processes focused on continuous improvement are essential to the delivery of safe, reliable, and affordable products.

Table 4.3.6.T2. Focus of Risk Management Process by Phase

Phase	Focus	Products / Outputs (Risk Considerations)	Measures / Metrics
Pre-MDD	Risk assessment of the effort/approach, early assessments of complexity, technical maturity, ability to close or reduce gaps Mitigation measures include resourcing teams for further detailed evaluation		Identify operational risks associated with capability gaps, measured in terms of probability and consequence Estimate resources to implement recommendations to close or mitigate capability gaps and reduce operational risk Identify dependencies and constraints (e.g., capability integration and interoperability with other systems or materiel solutions) associated with closing or mitigating capability gaps
MSA	Risk identification as an element of the Analysis of Alternatives (AoA), other technical analysis, and Milestone A entrance criteria Risk assessments to support selection of the preferred materiel solution and appropriate acquisition strategy Vendor viability, contract strategy, acquisition strategy, technology maturity, resource availability, user expectations Acquisition strategy evaluations include risk considerations of contractor availability, technical maturity, environmental, and operational dimensions Mitigation approaches include contract approach, prototype, and parallel development	SE contributions to AoA Report SEP and SE contributions to TDS that highlight how risk areas identified in the AoA are managed or mitigated in the TD phase Selection of alternative solutions to include overall risk of achieving desired capabilities within cost and schedule estimates Risk input to AoA; overall risk assessment and its integration into cost and schedule estimates	A quantitative analytical comparison of the operational effectiveness, suitability, and life-cycle cost of candidate materiel solutions A list of critical technologies (CT) associated with each candidate materiel solution, including measures of technology maturity, integration risk, manufacturing feasibility, CT supply chain risk Quantification of performance, cost, and schedule risks associated with each alternative

Phase	Focus	Products / Outputs (Risk Considerations)	Measures / Metrics
TD	Risk Management as a driver for technology readiness, preliminary design, and Milestone B entrance criteria	Technology maturity and risk reduction Validation of CT maturity for a materiel solution from prototypes, experimentation, or other form of demonstration Validation of CT supplier/vendor trustworthiness from a supply chain integrity risk perspective Risk reduction through competitive prototyping: • Broadens the opportunity for technology maturation by engaging multiple parties to compete for technology prototypes • Can help the program identify the nature of risk at the subsystem/ system level (functionality, performance, or affordability) Risks associated with preliminary design	Measures that demonstrate reduced technology maturity risks with respect to CT developers and producers • Vendor viability in terms of business health, market position, industry outlook stability • Assessments of the CT competitive environment to assess reliance risk on a single vendor/supplier Technology Readiness Levels (TRL) as the metric to assess CT maturity Affordability monitoring Continuous should cost estimation Assessment that preliminary design has high likelihood of satisfying the need within cost and schedule constraints

Phase	Focus	Products / Outputs (Risk Considerations)	Measures / Metrics
EMD	Risk Management as an element of development, full system integration, and Milestone C entrance criteria	EMD Risk Management processes, procedures, and plan Risk mitigation for establishment of qualification requirements throughout the supply chain Special emphasis: • Requirements • Risk management • Affordability risk management • Supply chain risk management Should cost assessments EMD risk management plan that includes addressing the above focus areas; include a sustainment risk management plan as part of the program's overall EMD risk management plan (Life-Cycle Sustainment Plan (LCSP)) At the Critical Design Review (CDR), identify risks and mitigation plans for achieving a fully verified functional baseline in a timely fashion	PM's Risk Management Dashboard focused on EMD: • KPP risk management • TPM analyses and monitoring • Risk burn-down and closure rates • Cost growth monitoring EMD schedule monitoring (e.g., IMS model measurements for schedule slips) Affordability monitoring Continuous should cost estimation
P&D	Risk Management as an element of operational test and evaluation, production, and IOC	P&D Risk Management processes, procedures, and plan Special emphasis: P&D SCRM P&D risk management plan that includes addressing the above focus areas; include updates or refinements to the LCSP/ sustainment risk management, initially created as part of the program's overall EMD risk management plan	PM's Risk Management Dashboard focused on P&D • Funding streams • Continuity of production levels and frequency of breaks • Production failure rate, supplier quality non-conformances, and cost impact metrics • Impact of supplier and design changes to the qualified baseline Deployment and fielding schedules

Phase	Focus	Products / Outputs (Risk Considerations)	Measures / Metrics
O&S	Risk Management as an element of operational readiness and FOC	O&S Risk Management processes, procedures, and plan Special Emphasis: O&S SCRM O&S risk management plan that includes addressing the above focus areas	PM's Risk Management Dashboard focused on O&S: • O&S funding streams • Management and burn-down of technology obsolescence risks • Technology insertion upgrade schedules and refresh rate • Qualification and product verification of spares suppliers, field failure rates, and depot failure rates O&S contract monitoring

4.3.7. Configuration Management Process

4.3.7. Configuration Management Process

The Configuration Management process allows technical insight into all levels of the system design and is the principal methodology for establishing and maintaining consistency of a system's functional, performance, and physical attributes with its requirements, design, and operational information throughout the system's life cycle. Effective configuration management supports the establishment and maintenance of the product baseline, which enables the successful production, delivery, and sustainment of the needed capability to the end user.

Configuration Management activities support:

- Traceability of designs to requirements
- Proper identification and documentation of system elements, interfaces, and interdependencies
- Timely and thorough vetting and disposition
- Control and documentation of approved changes to baselines
- Proper and timely incorporation of verified changes in all affected items and documentation
- Consistent and appropriate provisions in the Engineering Change Proposal (ECP) and related contract actions
- Consistency between the product and its supporting documentation
- A complete audit trail of design decisions and modifications
- Continued assurance of system supportability and interoperability, consistent

with approved acquisition and life-cycle sustainment strategies

Configuration Management facilitates the orderly development of a system through establishment of the technical baseline (including the functional, allocated, and product baselines), and their assessment and approval at various technical reviews and audits. A baseline is an agreed upon description of the attributes of a product at a point in time, which serves as a basis for change. Upon approval, the baseline is placed under formal configuration control. Through Configuration Management, the program identifies, controls, and tracks changes to system baselines, ensuring changes occur only after thorough assessments of performance, cost, and schedule impacts and associated risks.

The following baselines are critical to executing Configuration Management:

- Functional Baseline: Describes the system's performance (functional, interoperability, and interface characteristics) and the verification required to demonstrate the achievement of those specified characteristics. It is directly traceable to the operational requirements contained in the Initial Capabilities Document (ICD). The Program Manager establishes Government control of the functional baseline at the System Functional Review (SFR) and verifies it through Functional Configuration Audits (FCA) leading up to the system-level FCA or the System Verification Review (SVR). Attributes of the functional baseline include:
    - Assessed to be achievable within cost and schedule constraints
    - Documentation of established interfaces between functional segments
    - Documented performance requirements traced to (draft) CDD requirements
    - Reflects design considerations and clear linkage in the systems of systems (SoS) context
    - Documented verification requirements
- Allocated Baseline: Describes the functional and interface characteristics for all system elements (allocated and derived from the higher-level product structure hierarchy) and the verification required to demonstrate achievement of those specified characteristics. The allocated baseline for each lower-level system element (hardware and software) is usually established and put under configuration control at the system element Preliminary Design Review (PDR). This process is repeated for each system element and culminates in the complete allocated baseline at the system-level PDR. The Program Manager then verifies the allocated baseline at the FCA and/or SVR. Attributes of the allocated baseline include:
    - All system-level functional performance requirements decomposed (or directly allocated) to lower-level specifications (configuration items (CI) for system elements)
    - Uniquely identified CIs for all system elements at the lowest level of the specification tree
    - All interfaces, both internal (between element CIs) and external (between the system under development and other systems), documented in

interface control documents
    - Verification requirements to demonstrate achievement of all specified functional performance characteristics (element CI to element CI level and at the system level) documented
    - Design constraints documented and incorporated into the design
- Product Baseline: Describes the detailed design for production, fielding/deployment, and operations and support. The product baseline prescribes all necessary physical (form, fit, and function) characteristics and selected functional characteristics designated for production acceptance testing and production test requirements. It is traceable to the system performance requirements contained in the Capability Development Document (CDD). The initial product baseline includes "build-to" specifications for hardware (product, process, material specifications, engineering drawings, and other related data) and software (software module design - "code-to" specifications). The initial system element product baseline is established and placed under configuration control at the system element Critical Design Review (CDR) and verified later at the Physical Configuration Audit. In accordance with DoDI 5000.02, the Program Manager assumes control of the initial product baseline for all Class I configuration changes at the completion of the system-level CDR to the extent that the competitive environment permits. This does not necessarily mean that the Program Manager takes delivery and acceptance of the Technical Data Package. Attributes of the product baseline include:
    - Requirements Traceability Matrix (RTM) is complete
    - The detailed design (hardware and software), including interface descriptions, satisfies the CDD or any available draft Capability Production Document (CPD), and pertinent design considerations
    - Hardware, software and interface documentation are complete
    - Key product characteristics having the most impact on system performance, assembly, cost, reliability, ESOH, and sustainment have been identified
    - Traceability from design documentation to system and system element verification requirements and methods is complete
    - Manufacturing processes that affect the key characteristics have been identified, and capability to meet design tolerances has been determined

Activities and Products

The program office and developer share responsibility for planning, implementing, and overseeing the Configuration Management process and its supporting activities. The distribution of responsibilities between the program office and the developer varies based on the acquisition strategy and the life-cycle phase.

The Program Manager approves the Configuration Management Plan and should ensure adequate resources are allocated for implementing Configuration Management throughout the life cycle. The Program Manager approves the system baselines, and approves Class I changes to the product baseline after CDR, usually through a

Configuration Control Board (CCB). MIL-HDBK-61A, "Configuration Management Guidance" defines Class I and II changes:

- Class I changes impact the form, fit, function, or interface characteristics of the configuration item
- Class II changes are changes to a Government approved technical baseline that do not meet the definition of a Class I change

In performance-based acquisition, these terms apply only to changes that affect Government-approved (baselined) configuration documentation.

The Systems Engineer ensures Configuration Management planning is complete, and should document details and activities in the program's Systems Engineering Plan (SEP) and the supporting Configuration Management Plan (CMP) (as appropriate). The CM process described in the DoD-adopted standard, ANSI/EIA-649-B-2011 "Configuration Management Standard," consists of five interrelated functions that, when collectively applied, allow the program to maintain consistency between product configuration information and the product throughout its life cycle. The five CM functions are:

- Configuration Management Planning and Management
- Configuration Identification
- Configuration Change Management
- Configuration Status Accounting
- Configuration Verification and Audit

4.3.8. Technical Data Management Process

4.3.8. Technical Data Management Process

Through the Technical Data Management process, the program identifies, acquires, manages, maintains, and ensures access to the technical data and computer software required to manage and support a system throughout the acquisition life cycle. Key Technical Data Management considerations include understanding and protecting Government intellectual property and data rights, achieving competition goals, maximizing options for product support, and enabling performance of downstream life-cycle functions. DoDI 5000.02 contains Technical Data Management requirements for Acquisition Category (ACAT) I and II programs.

Effective acquisition, upgrades, and management of product data provide:

- Information necessary to understand and evaluate system designs throughout the life cycle
- Ability to operate and sustain weapon systems under a variety of changing technical, operational, and programmatic environments
- Ability to re-compete item acquisition, upgrades, and sustainment activities in the

interest of achieving cost savings; the lack of product data and/or data rights often makes it difficult or impossible to award contracts to anyone other than the original manufacturer, thereby taking away much or all of the Government's ability to reduce total ownership costs (TOC)

Activities and Products

The Program Manager and Systems Engineer, in conjunction with the Product Support Manager, should ensure that life-cycle requirements for weapon system-related data products and data rights are identified early and that appropriate contract provisions are put in place to enable deliveries of these products. Figure 4.3.8.F1 shows the activities associated with Technical Data Management, including:

- Identify Data Requirements

- Formulate the program's Technical Data Rights Strategy (TDRS) and technical data management approach, with emphasis on technical and product data needed to support the product throughout its life cycle. (see DAG Chapter 2 Program Strategies for more information about Data Rights).
- Ensure that data requirements are documented in the TDRS; summarized in the Technology Development Strategy (TDS), Acquisition Strategy (AS), and Life-Cycle Sustainment Plan (LCSP) ; and submitted at each milestone prior to award of the contract for the next life-cycle phase.
- Consider not only the immediate, short-term costs of acquiring the needed technical data and data rights but also the long-term cost savings resulting from the ability to compete production and logistics support activities and reduce TOC. Understand that the Government can possess either Government Purpose or Unlimited Rights to use many types of technical data and data rights, at no additional cost, based on the type of technical data and the source of funding used to generate the data (see DoD Open Systems Architecture Contract Guidebook for Program Managers for more information about data rights).

- Acquire Data

- Use explicit contract Statement of Work tasks to require the developer to perform the work that generates the required data. The content, format, and quality requirements should be specified in the contract.
- Use current, approved Data Item Descriptions (DID) and Contract Data Requirements Lists (CDRL) in each contract to order the delivery of the required technical data and computer software.

- Receive, Verify, and Accept Data

- Ensure verification of content, format, and quality of all required product-related data received from originators.
- Inspect contractually ordered data deliverables to ensure markings are in

accordance with the relevant data rights agreements and DFARS clauses, and contain appropriate distribution statements and/or export control statements.

Caution: *Acceptance of delivered data not marked consistent with the contract can result in the Government "losing" legitimate rights to technical data and can incur significant legal liability on the Government and the individual Government employees. Regaining those rights generally requires costly and time-consuming legal actions.*

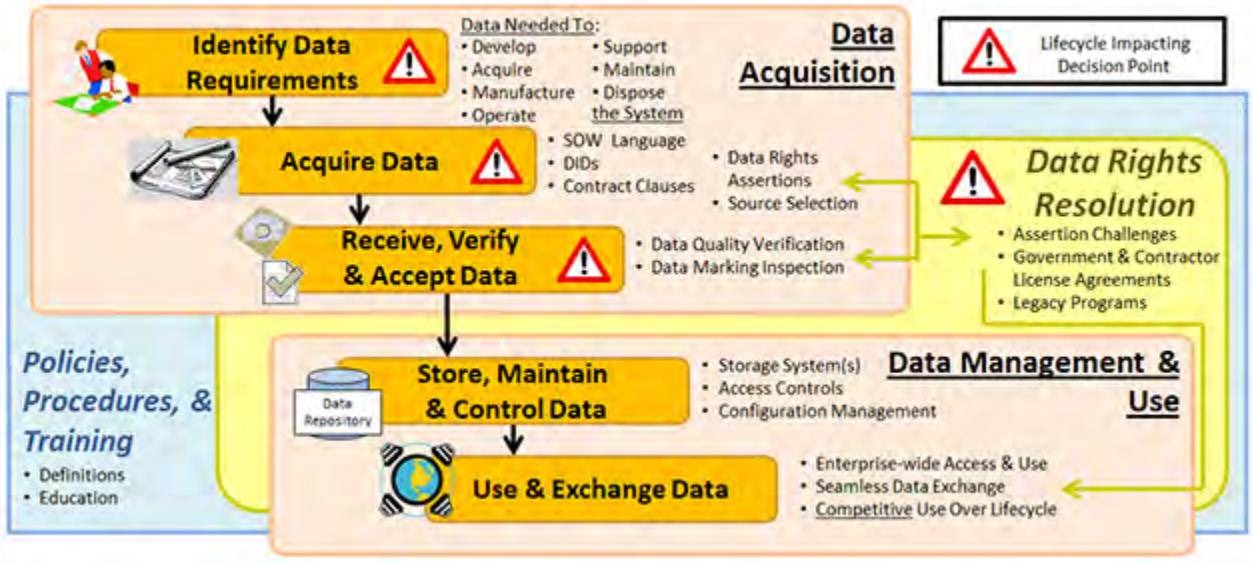
- Store, Maintain, and Control Data

- Budget for and fund the maintenance and upkeep of product data throughout the life cycle.
- An Integrated Data Environment (IDE) or Product Life-cycle Management (PLM) system allows every activity involved with the program to create, store, access, manipulate, and exchange digital data.
- To the greatest extent practical, programs should use existing IDE/PLM infrastructure such as repositories operated by Commodity Commands and other organizations. (Program-unique IDEs are discouraged because the high infrastructure cost; further, multiple IDEs inhibit access, sharing, and reuse of data across programs.)
- Ensure all changes to the data are made in a timely manner and are documented in the program IDE or PLM system.

- Use and Exchange Data

Plan for and establish methods for access and reuse of product data by all personnel and organizations that perform life-cycle support activities.

Figure 4.3.8.F1. Data Management Activities



In support of the Government's requirement for a Technical Data Package (TDP), the Program Manager should also consider all product related data (e.g., technical manuals, repair instructions, and design/analysis data) to:

- Allow logistics support activities
- Better enable sustainment engineering
- Apply, implement and manage product upgrades

Contractually deliverable data should be identified and ordered at the specific "data product" level, e.g., two-dimensional drawings, three-dimensional Computer-Aided Design (CAD) models, technical manuals, etc. Figure 4.3.8.F2 provides a notional representation of different types of product-related data.

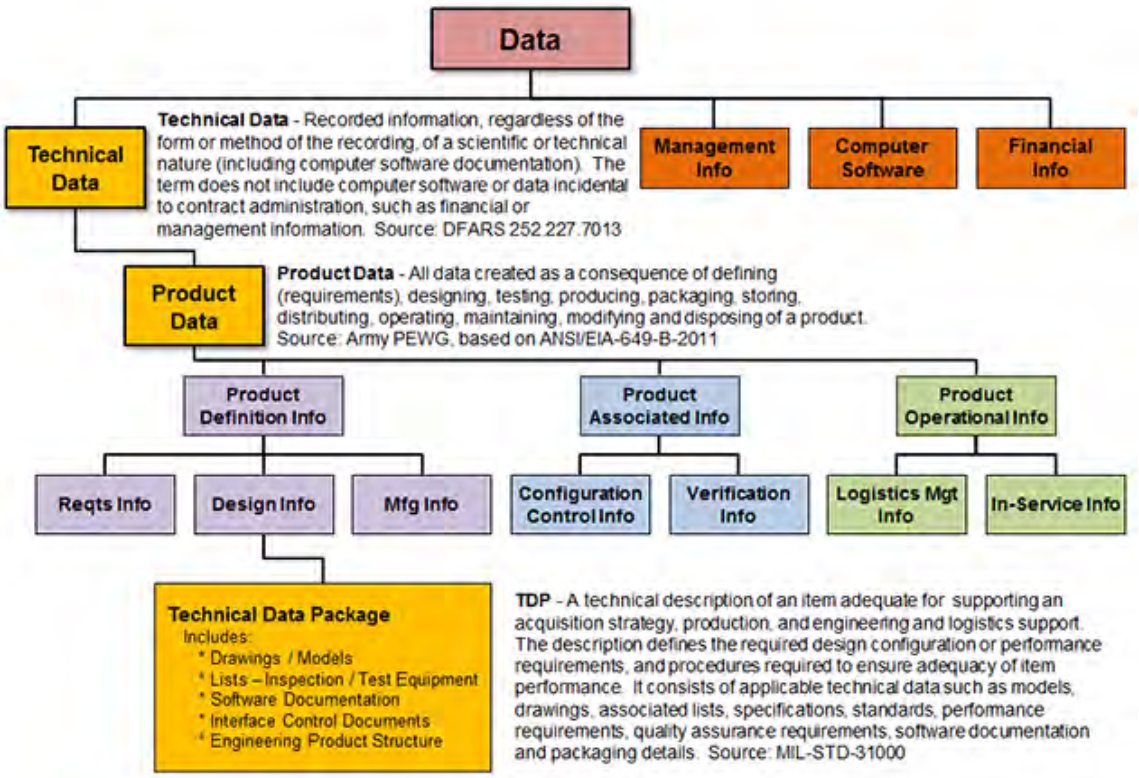
Caution: *Program Managers and Systems Engineers should be aware that terms such as "technical data," "product data," and "TDP" are imprecise, not equivalent, and often incorrectly used interchangeably.*

Resources for establishing and conducting Technical Data Management activities include but are not limited to:

- DoD 5010.12-M, Procedures for the Acquisition and Management of Technical Data
- Army Data Management Strategy (DMS) Guide and Addendum
- Air Force Product Data Acquisition (PDAQ) guidance
- Air Force Technical Data and Computer Software Rights Handbook
- Navy Technical Manual SL150-AA-PRO-010/DMP - Data Management Program
- MIL-HDBK-245, Handbook for the Preparation of Statement of Work

- MIL-STD-963, Data Item Descriptions
- MIL-STD-31000, Technical Data Packages

Figure 4.3.8.F2. Data Taxonomy



- **Data Protection**

The Program Manager is responsible for protecting system data, whether the data is stored and managed by the Government or by contractors. The DoD policy with regard to data protection, marking, and release can be found in:

- DoDD 5230.25
- DoDI 5230.24
- DoD 5400.7-R
- DoD 5200.1-M

Data containing information subject to restrictions are protected in accordance with the appropriate guidance, contract, or agreement. Guidance on distribution statements, restrictive markings, and restrictions on use, release, or disclosure, of data can be found in the DFARS Part 252.227-7013 and 7014, and DoDI 5230.24.

When digital data is used, the data should display applicable restriction markings, legends, and distribution statements clearly visible when the data is first opened or

accessed. These safeguards not only ensure Government compliance regarding the use of data but also guarantee and safeguard contractor data delivered to the Government, and extend responsibilities of data handling and use to parties who subsequently use the data.

Section 208 of Public Law 107-347 and DoD Privacy Impact Assessment (PIA) guidance requires that PIA be conducted prior to developing or purchasing any DoD information system that collect, maintain, use, or disseminate personally identifiable information about members of the public, federal personnel, DoD contractors and, in some cases, foreign nationals. Available PIA guidance provides procedures for completing and approving PIAs. For further information, see DAG Chapter 7 Acquiring Information Technology, Including National Security Systems.

All data deliverables should include distribution statements. Processes should be established to protect all data that contain critical technology information, as well as ensure that limited distribution data, intellectual property data, or proprietary data is properly handled throughout the life cycle, whether the data are in hard-copy or digital format.

4.3.9. Interface Management Process

4.3.9. Interface Management Process

The Interface Management process assists the Program Manager ensure interface definition and compliance among the system elements, as well as with other systems. The Interface Management process helps ensure that developers document all internal and external interface requirements and requirements changes in accordance with the program's Configuration Management Plan. Developers also should communicate interface information to their counterparts responsible for affected systems and system elements, and should plan for coherent testing to verify expected performance and ultimately operational performance.

Systems are composed of system elements, and may operate as part of larger systems of systems (SoS). The design, definition and management of the physical and logical interfaces, both internal (communications between system elements) and external (communications between the system and other systems), are critical to program success. Both types of interfaces have become increasingly important as system complexity has increased, along with demands for systems to operate in highly interdependent SoS environments (see DAG section 4.2.1.2. Systems of Systems). Interfaces play a critical role in all systems and systems of systems that interact to deliver a collective capability. Complex systems consist of numerous interfaces of various types. In the absence of effective governance, interface sprawl can result in degraded system performance, sustainability, and maintainability.

Explicit management of the definition, development, implementation, and test of internal and external interfaces, including any associated dependencies, helps ensure that

systems operate as designed and meet stakeholder expectations throughout the life cycle. Interface management should consider programmatic issues (e.g., roles and responsibilities, funding, scheduling) in addition to the technical aspects of systems engineering (SE) and integration.

Activities and Products

Interface management is an iterative process: as knowledge of the system and system elements increases during design activities, verifiable lower-level requirements and interfaces are defined and refined. Developers should assess impacts of the originally defined capabilities and interfaces, performance parameter thresholds and objectives, and the overall system when defining and modifying interfaces.

The Program Manager and Systems Engineer should ensure that the program's interface management plan:

- Documents the system's internal and external interfaces and their requirement specifications
- Identifies preferred and discretionary interface standards and their profiles
- Provides justification for selection and procedure for upgrading interface standards
- Describes the certifications and tests applicable to each interface or standard
- Is consistent with the program's configuration management plan

The Program Manager and Systems Engineer should ensure that the developer documents all system interface requirements (see DAG section 4.3.5. Requirements Management Process), places them under appropriate levels of configuration management, and makes them available to the appropriate stakeholders. These documented interface requirements serve critical functions at all levels of the system throughout the life cycle, including:

- Developing functional and physical architectures
- Facilitating competitive bids
- Enabling integration of systems and lower-level system elements
- Supporting system maintenance, future enhancements, and upgrades
- Providing input data for continuous risk management efforts

The Systems Engineer responsible for interface management has numerous key tasks throughout the life cycle, including:

- Defining and establishing interface specifications
- Assessing compliance of interfaces among configuration items composing systems or SoS
- Monitoring the viability and integrity of interfaces within a system
- Establishing an interface management plan to assess existing and emerging interface standards and profiles, to update interfaces, and to abandon obsolete

architectures

The Program Manager should establish an Interface Control Working Group (ICWG) composed of appropriate technical representatives from the interfacing activities and other interested participating organizations. The ICWG serves as a forum to develop and provide interface requirements, as well as to focus on detail interface definition and timely resolution of issues. In the SoS environment, external program offices and developers collaborate as members of the ICWG.

4.3.10. Stakeholder Requirements Definition Process

4.3.10. Stakeholder Requirements Definition Process

During the Stakeholder Requirements Definition process, the lead Service, Component, or designated program office receives requirements from relevant stakeholders and translates them into a set of technical requirements. The process helps ensure each individual stakeholder's requirements, expectations, and perceived constraints are understood from the acquisition perspective. Failing to perform an exhaustive Stakeholder Requirements Definition process could result in significant requirements creep, rework due to misunderstanding of end-user needs, unexpected contract modifications, cost growth, and schedule slip. The objective of this process is to help ensure that stakeholder requirements are feasible, balanced, and fully integrated as more information is learned through requirements analysis.

Stakeholder Requirements Definition bridges the gap between the identification of a materiel need, described in the Joint Capabilities Integration and Development System (JCIDS) CJCSI 3170.01, and the acquisition of a materiel solution, governed by the Defense Acquisition System, i.e., DoDD 5000.01 and DoDI 5000.02.

The Stakeholder Requirements Definition process complements Requirements Analysis and Architecture Design (see DAG sections 4.3.11 Requirements Analysis Process and 4.3.12 Architecture Design Process, respectively). These three processes are recursively applied at each level of the system's specifications and then iteratively within each level throughout development.

The DoD Architecture Framework (DoDAF) provides an approach for DoD architecture development, presentation, and integration for both warfighting operations and business operations and processes. For the Net Ready Key Performance Parameter (NR-KPP), JCIDS and CJCSI 6212.01 specify the data needed to elaborate, communicate, verify, and validate a system's interoperability requirements and design. System architectural descriptions contain three basic viewpoints: operational, system, and standards (or technical) viewpoints. In the case of the NR-KPP, these viewpoints contain essential architecture data that describe a system's interoperability requirements and design from multiple perspectives. DoDAF provides a standardized approach for capturing and presenting this architectural data. This standardization facilitates improved communication and sharing of technical information among various stakeholders and

across organizational boundaries.

The Program Manager and Systems Engineer are responsible for supporting the Stakeholder Requirements Definition process and should work with the end user to establish and refine operational needs, attributes, performance parameters, and constraints documented in JCIDS documents.

Stakeholder Requirements Definition activities are performed throughout the acquisition life cycle and include the following activities:

- Elicit stakeholder capability objectives
  - Identify stakeholders who have an interest in the system and maintain relationships with the stakeholders and their organizations throughout the system's entire life cycle
  - Elicit capability objectives from the stakeholders about what the system will accomplish and how well
- Define stakeholder requirements
  - Define the perceived constraints on a system solution
  - Define the relevant environment and support scenarios that can be used to analyze the operation of the system
  - Define potential requirements that may not have been formally specified by any of the stakeholders
- Analyze and maintain stakeholder requirements
  - Analyze requirements for specificity, completeness, consistency, measurability, testability, and feasibility
  - Negotiate modifications with stakeholders to resolve requirement discrepancies
  - Validate, record, and maintain stakeholder requirements throughout the system life cycle
  - Support the Requirements Analysis process to establish and maintain a traceability matrix to document how the system requirements are intended to meet the stakeholder objectives and achieve stakeholder agreements

The authoritative source for stakeholder requirements are documents produced via the JCIDS such as the Initial Capabilities Document (ICD), Capability Development Document (CDD), and the Capability Production Document (CPD). JCIDS analyzes gaps in existing and/or future warfighting operations and provides a process that allows the Joint Requirements Oversight Council to balance joint equities and make informed decisions on validation and prioritization of capability needs.

4.3.11. Requirements Analysis Process

4.3.11. Requirements Analysis Process

The Requirements Analysis process involves the decomposition of user needs (usually identified in operational terms at the system level during implementation of the

Stakeholder Requirements Definition process; see DAG section 4.3.10 Stakeholder Requirements Definition Process) into clear, achievable, and verifiable high-level requirements. As the system design evolves, Requirements Analysis activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design. The allocated requirements form the basis of contracting language and the system performance specification. The resultant system requirements are addressed at technical reviews and audits throughout the acquisition life cycle and in applicable program and systems engineering (SE) technical documentation.

The Requirements Analysis process objectives include:

- Define a capability that links the needs of the users to the system, system elements, and enabling system elements to be designed and developed
- Define a system that meets users' operational mission requirements within specified cost and schedule constraints
- Provide insight into the interactions among various functions to achieve a set of balanced requirements based on user objectives

The Requirements Analysis process provides:

- Translation of user needs (usually stated in operational terms) to unambiguous, verifiable, and feasible system performance specification requirements
- Incorporation of design considerations including statutory and regulatory constraints (see DAG section 4.3.18. Design Considerations)
- Documented allocation of requirements from the system-level specification to the lowest-level system elements and enabling system elements
- Rationale for specification requirements and their decomposition / allocation
- A mechanism to support trade-off analyses between related requirements to provide maximized mission assurance within cost and schedule constraints
- A framework for accurate assessment of system performance throughout the life cycle

The process of defining, deriving, and refining requirements proceeds as follows:

- Analyze user requirements
- Translate user needs into basic functions
- Develop a quantifiable set of performance requirements by defining the functional boundaries of the system in terms of the behavior and properties to be provided
- Define each function that the system is required to perform
- Define implementation constraints (stakeholder requirements or solution limitations)
- Translate performance requirements into specific system technical design requirements and functions

The Requirements Analysis process is an iterative activity whereby system requirements are identified, refined, analyzed, and traded to remove deficiencies and

minimize impacts of potential cost drivers to establish an agreed-to set of requirements coordinated with the appropriate stakeholders. Poorly written requirements can lead to significant problems in the areas of schedule, cost, or performance, and can thus increase program risk. A well-crafted set of functional/performance requirements can then be translated into design requirements for the total system over its life cycle and can allow stakeholders to assess system performance during execution of the Verification and Validation processes (see DAG sections 4.3.15. Verification Process and 4.3.16. Validation Process, respectively). Good requirements have the following attributes:

- Necessary
- Unique
- Unambiguous - clear and concise
- Complete
- Consistent
- Technically feasible/achievable/obtainable
- Traceable
- Measurable/quantifiable
- Verifiable (e.g., Testable)
- Able to be validated
- Operationally effective
- Singular

The Requirements Analysis process ensures that requirements derived from user-specified capability needs are analyzed, decomposed, and functionally detailed across the system design. Early development and definition of requirements using the attributes listed above reduces development time, enables achievement of cost and schedule objectives, and increases the quality of the final system. Requirements Analysis encompasses the definition and refinement of the system, system elements, enabling system elements, and associated functional and performance requirements. The development of the functional baseline is largely a product of the Requirements Analysis process. All requirements are placed under configuration control, tracked, and managed as described in the Requirements Management process and Configuration Management process (see DAG sections 4.3.5. Requirements Management Process and 4.3.7. Configuration Management Process, respectively).

4.3.12. Architecture Design Process

4.3.12. Architecture Design Process

Architecture Design is a trade and synthesis process that allows the Program Manager and Systems Engineer to translate the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions and establishes the architectural design of candidate solutions that may be found in a system model. The alternative design solutions may include hardware, software, and human elements; their enabling system elements; and related internal and external

interfaces. The Architecture Design process, combined with Stakeholder Requirements Definition and Requirements Analysis, provides key insights into technical risks early in the acquisition life cycle, allowing for early development of mitigation strategies. Architecture Design is integral to ensuring that multiple well-supported solutions are considered. The Architecture Design process supports analysis of design considerations and enables reasoning about key system aspects and attributes such as reliability, maintainability, survivability, sustainability, performance, and total ownership cost.

Architecture design synthesizes multiple potential solutions from system performance requirements, evaluates those solutions, and eventually describes the system down to the individual system element for implementation. The Architecture Design process is iterative and strives to seek a balance among cost, schedule, performance, and risk that still meets stakeholder needs.

The functional architecture provides the foundation for defining the system architecture through the allocation of functions and sub-functions to hardware/software, databases, facilities, and human operations to achieve its mission. The development of the physical architecture consists of one or more product structures or views of the physical solution. The product structure may consist of conceptual design drawings, schematics, and/or block diagrams that define the system's form and the arrangement of the system elements and associated interfaces. The DoD Architecture Framework (DoDAF) operational and system viewpoints provide one method for developing and describing the system functional architecture. The development of a physical architecture is an iterative and recursive process and evolves together with the functional requirements and functional architecture. Development of the physical architecture is complete when the system has been decomposed to the lowest system element (usually the lowest replaceable unit of the support strategy). It is critical that this process identify the design drivers and driving requirements as early as possible.

The Program Manager may oversee Architecture Design efforts to gain and maintain insights into program schedule and cost drivers for use in evaluation of alternative architectures, excursions, mitigation approaches, etc.

Key activities in the Architecture Design process include:

- Analysis and synthesis of the physical architecture and the appropriate allocation,
- Analysis of the constraint requirements,
- Identify and define physical interfaces and system elements, and
- Identify and define critical attributes of the physical system elements, including design budgets (e.g., weight, reliability) and open system principles.

During this process, derived requirements come from solution decisions. It is essential to identify derived requirements and ensure that they are traceable and part of the allocated requirements. For each given solution alternative, the Decision Analysis

process trades off requirements against given solution alternatives. For each solution alternative, based on programmatic decisions, certain performance requirements may be emphasized over others. The essence of this activity is to achieve a balanced and feasible design with acceptable risk, and that falls within the program design constraints. An integral part of defining and refining the functional and physical architecture is to provide technical support to the market research especially early in the acquisition life cycle. Systems engineers should analyze whether existing products (commercial or non-developmental items) can meet user performance requirements or whether technologies can realistically be matured within the required time frame. When possible, mature technologies should be used to satisfy user needs.

The development of the system architecture should adhere to sound systems engineering (SE) and should conform to industry standards as applicable. The functional architecture should be part of the functional baseline, and the physical architecture should be part of the allocated and product baselines. The system architecture should be placed under configuration control and maintained in a robust repository that maintains the architecture descriptions and its relationships to each of the baselines. This control provides the Systems Engineer with a means of ensuring consistency of the system architecture definition throughout the acquisition life cycle.

The output of this process is the system allocated baseline, which includes the documentation that describes the physical architecture of the system and the specifications that describe the functional and performance requirements for each configuration item along with the interfaces that compose the system. In addition, Work Breakdown Structures (WBS) and other technical planning documentation are updated. The system architecture and the resulting design documentation should be sufficiently detailed to allow the following:

- Confirmation of upward and downward traceability of requirements
- Confirmation of interoperability and open system performance requirements
- Sufficient product and process definition to support implementation, verification, and validation of the system
- Establishment of achievable alternatives to allow key stakeholders to make informed decisions

Confirmation of requirements traceability and the soundness of the selected physical architecture can be accomplished using a cost-effective combination of design modeling and analysis, as applicable.

The result of the Architecture Design process is an architectural design that meets the end-user capability needs shown in the Requirements Management process to have all stated and derived requirements allocated to lower level system elements and to have the possibility of meeting cost, schedule, and performance objectives. The architectural design should be able to be communicated to the customers and to the design engineers. The level of detail of the architectural design depends on the complexity of the system and the support strategy. It should be detailed enough to bound the cost and

schedule of the delivered system, define the interfaces, ensure the customers that the requirements can be met, and control the design process down to the lowest removable unit to support operations and sustainment. This architecture design may be documented and found in a program's system model. Once identified, the system architecture is placed under configuration management.

4.3.13. Implementation Process

4.3.13. Implementation Process

The Implementation process involves two primary efforts: design and realization. The outputs of the Implementation process include the detailed design down to the lowest level system elements in the system architecture, and the fabrication/production procedures of forming, joining, and finishing, or coding for software. Depending on technology maturity, the Implementation process may develop, buy, or reuse system elements to render the system. Implementation is integral to systematically increasing maturity, reducing risk, and ensuring the system is ready for Integration, Verification, and Validation. The Implementation process provides a system that satisfies specified design and stakeholder performance requirements. As a best practice, the Systems Engineer should develop an implementation plan including implementation procedures, fabrication processes, tools and equipment, implementation tolerances, and verification uncertainties.

Design

Implementation begins in the Materiel Solution Analysis phase, where the Analysis of Alternatives informs whether the preferred materiel solution can be developed, bought, or reused. This analysis takes many forms, such as modeling and simulation, experiments, and prototypes through which competing systems can be assessed. Careful decisions regarding the design of system elements can enable the use of open (non-proprietary) standards and an open systems or modular approach that may allow for resiliency as well as reduce costs and promote competition during development, production, technology refresh, and life-cycle extension. Design activities may include:

- Identify and analyze the constraints that the technology and design and realization techniques impose on the design solution
- Develop design and implementation prototypes and solutions for the system elements
- Analyze candidate system element design and implementation solutions and conduct variability studies to identify conflicts and resolution alternatives to ensure system integrity
- Identify fabrication and quality procedures, and document design assumptions and decisions in the final system elements drawings or technical data package

Realization

Realization is the process of building the system elements using specified materials and fabrication and production tools/procedures identified during design. Early fabrication and production planning is critical for successful realization and delivery of the needed capability. System elements are built to the product baseline and should meet quality standards. Realization activities may include:

- Obtain or acquire access to materials and tools required to build system elements
- Obtain external system elements as applicable
- Build system elements in accordance with implementation procedures, tolerances, and applicable ESOH, security, and privacy
- Determine system elements functionality against specified product quality characteristics
- Document fabrication and production issues and associated corrective actions
- Deliver implemented system elements for integration and subsequent verification

The output of the Implementation process is the physical system elements as identified in the product baseline, including fabrication and production methods.

4.3.14. Integration Process

4.3.14. Integration Process

The program uses the Integration process to systematically assemble lower-level system elements into successively higher-level system elements, iterative with verification until the system itself emerges. Integration is essential to increasing system maturity, reducing risk, and preparing the system for transition to the warfighter.

The Interface Management process is critical to the success of the Integration process. Interface control specifications should be confirmed early on and placed under strict configuration control. All of the program's external interfaces and dependencies should be documented in the program's Systems Engineering Plan (SEP). The SEP Outline requires that all programs with external dependencies and/or interfaces establish Memoranda of Agreement (MOA) in order to formally establish commitments and management procedures. A current table showing the status of all MOAs is a mandated as part of the program SEP, which is updated in each phase.

The Program Manager and Systems Engineer are responsible for planning, managing, and executing the Integration process. Experience has shown that programs that develop an integration plan are more successful. This plan defines the stages of integration during which system elements are successively integrated to form higher level elements and eventually the finished product. Alternative integration paths should be considered. The integration plan should include a description of the required Systems Integration Laboratories or other facilities, personnel, test stands, harnesses,

testing software, and integration schedule.

Integration activities support the Interface Management process by verifying that accurate and effective interface specifications are documented. In parallel, the verification methods for each integration level are developed and included in the allocated baseline. The successive integration phases follow the sequence defined in the program's integration plan and lead to the final product ready for verification and validation.

4.3.15. Verification Process

4.3.15. Verification Process

Verification provides evidence that the system or system element performs its intended functions and meets all performance requirements listed in the system performance specification and functional and allocated baselines. Verification answers the question, "Did you build the system correctly?" Verification is a key risk-reduction activity in the implementation and integration of a system and enables the program to catch defects in system elements before integration at the next level, thereby preventing costly troubleshooting and rework.

The Program Manager and Systems Engineer manage verification activities and methods as defined in the functional and allocated baselines, and review the results of verification. Guidance for managing and coordinating integrated testing activities can be found in DAG Chapter 9 Test and Evaluation and in DoDI 5000.02.

Verification begins during Requirements Analysis, when top-level stakeholder performance requirements are decomposed and eventually allocated to system elements in the initial system performance specification and interface control specifications. During this process, the program determines how and when each requirement should be verified, the tasks required to do so, as well as the necessary resources (i.e., test equipment, range time, personnel, etc.). The resulting verification matrix and supporting documentation become part of the program's functional and allocated baselines.

Verification may be accomplished by any combination of the following methods:

- **Demonstration.** Demonstration is the performance of operations at the system or system element level where visual observations are the primary means of verification. Demonstration is used when quantitative assurance is not required for verification of the requirements.
- **Examination.** Visual inspection of equipment and evaluation of drawings and other pertinent design data and processes should be used to verify conformance with characteristics such as physical, material, part, and product marking and workmanship.
- **Analysis.** Analysis is the use of recognized analytic techniques (including

computer models) to interpret or explain the behavior/performance of the system element. Analysis of test data or review and analysis of design data should be used as appropriate to verify requirements.
- **Test.** Test is an activity designed to provide data on functional features and equipment operation under fully controlled and traceable conditions. The data are subsequently used to evaluate quantitative characteristics.

Designs are verified at all levels of the physical architecture through a cost-effective combination of these methods, all of which can be aided by modeling and simulation.

Verification activities and results are documented among the artifacts for Functional Configuration Audits (FCA) and the System Verification Review (SVR) (see DAG section 4.2.14. Functional Configuration Audits/System Verification Review). When possible, verification should stress the system, or system elements, under realistic conditions representative of its intended use.

The individual system elements provided by the Implementation process are verified through developmental test and evaluation (DT&E), acceptance testing, or qualification testing. During the Integration process, the successively higher level system elements may be verified before they move on to the next level of integration. Verification of the system as a whole occurs when integration is complete. As design changes occur, each change should be assessed for potential impact to the qualified baseline. This may include a need to repeat portions of verification in order to mitigate risk of performance degradation.

The output of the Verification process is a verified production-representative article with documentation to support Initial Operational Test and Evaluation (IOT&E). The SVR provides a determination of the extent to which the system meets the system performance specification.

4.3.16. Validation Process

4.3.16. Validation Process

Validation provides objective evidence that the capability provided by the system complies with stakeholder performance requirements, achieving its use in its intended operational environment. Validation answers the question, "Is it the right solution to the problem?" Validation consists of evaluating the operational effectiveness, operational suitability, sustainability, and survivability of the system or system elements under operationally realistic conditions.

The Program Manager and Systems Engineer are responsible for supporting the Validation process. The execution of the Validation process is typically conducted by independent testers as documented in the Test and Evaluation Master Plan (TEMP). System end users and other stakeholders are typically involved in validation activities. Guidance for managing and coordinating integrated testing activities can be found in

DAG Chapter 9 Test and Evaluation and DoDI 5000.02. Using and engaging integrated test teams, composed of knowledgeable and experienced Government and industry developmental and operational testers, bring different perspectives and allow for an efficient use of resources.

Validation activities can be conducted in the intended operational environment or on an approved simulated environment. Early program-validation activities assist in the production of validated concept of operations (CONOPS), system performance specifications, use cases, functional and physical system architectures, and test cases. Validation is applied to the initial product baseline to ensure the emerging design meets the end-user needs. Models, simulations, mockups, and prototypes may be used in these early activities. They are often combined with the verification activities (see DAG section 4.3.15. Verification Process). Aggressive early validation significantly mitigates the risk to the program by identifying operational issues up front when they are easier and less costly to fix. This ultimately improves system performance during the final validation activity (e.g., operational test and evaluation (OT&E)).

Final validation involves operational testing on a production-representative system in an operationally realistic environment. The product of the Validation process is a validated system and enabling system elements, leading to approval for Full-Rate Production (FRP) and/or a Full Deployment (FD) Decision Review (DR).

4.3.17. Transition Process

4.3.17. Transition Process

Transition is the process applied to move any system element to the next level in the physical architecture. For the end-item system, it is the process to install and field the system to the user in the operational environment. The end-item system may need to be integrated with other systems in the operational environment honoring the defined external interfaces. In this case, the transition process needs to be performed in conjunction with the integration process and interface management process for a smooth transition.

Early planning for system transition reduces risk and supports smooth delivery and rapid acceptance by the system’s end user. Transition considerations should include, as appropriate, user and maintainer requirements, training, deployability, support tasks, support equipment, and packaging, handling, storage, and transportation (PHS&T). Part of the Transition process is ensuring that each site is properly prepared for the receipt, acceptance, and/or installation of the system.

The Transition process includes maintenance and supportability activities for the deployed system and its enabling system elements, as well as a process for reporting and resolving deficiencies. The OUSD(AT&L) memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)" requires that sustainment and support planning be documented in the LCSP, which is required for all Major Defense Acquisition Programs

and reviewed prior to Milestones A, B, and C, as well as the Full-Rate Production Decision Review (FRP DR).

The Program Manager, Systems Engineer, and Product Support Manager oversee all transition plans and activities required to install or deploy the end-item system and enabling system elements to its operational environment. The Systems Engineer conducts In-Service Reviews (see DAG section 4.2.17. In-Service Review) and leads all engineering efforts to correct deficiencies found during transition. Program Managers should ensure all deliverables, particularly documentation (i.e. drawings, tech manuals, etc.), have been received from the contractor.

Transition activities vary based on life-cycle phase, program scale, and system complexity. The end-item system may need to be integrated with other systems in the operational environment based on the defined external interfaces. In this case, the Transition process is performed in conjunction with the Integration process and Interface Management process for a smooth transition.

4.3.18. Design Considerations

4.3.18. Design Considerations

The program should review the requirements to determine conformance with Government policy and legal compliance and to identify potential integration and interoperability challenges. The Program Manager and Systems Engineer should consider and document all statutory and regulatory as well as other design considerations in order to:

- Satisfy the unique needs of the program or system (user capabilities, and operational performance requirements) while balancing cost and schedule constraints, through trade-offs, by addressing the design considerations (as mandated in the Systems Engineering Plan (SEP) and DoDI 5000.02) and management tools listed in Table 4.3.18.T1 Design Considerations
- Translate the end user desired capabilities into a structured system of interrelated design specifications
- Enable trade-offs among the design considerations in support of achieving desired mission effectiveness within cost and schedule constraints
- Translate the end-user desired capabilities into a structured system of interrelated design specifications that support delivery of required operational capability
- Incorporate mandated design considerations into the requirements since some design considerations are mandated by laws, regulations, or treaties, while others are mandated by the domain or Service / Component; these mandates should be incorporated during the Requirements Analysis process to achieve balance across all of the system requirements

Some design considerations are concepts that assist trade-offs and ought to be accommodated or applied to each system/program/project. Others are constraints, boundaries, or limitations, with values that sometimes can be tailored or negotiated, but which in general represent fairly immovable parts of the trade space. The Program Managers and Systems Engineers should show evidence of critical thinking in addressing the design considerations, as documented in the program SEP. The mandated SEP Outline Table 4.6-1 identifies design considerations critical to achieving the program's technical requirements and demonstrates that the mandated design considerations are an integral part of the design decision process, including trade study criteria.

With the understanding that each design consideration is a discrete item to investigate during the design process, the Program Manager and Systems Engineer also need to view design considerations as an integrated set of variables. These variables influence one another, and stakeholders should consider them in conjunction with one another, as early as the Analysis of Alternatives, to achieve better mission performance and to preclude a stove pipe view during design.

The design considerations listed in Table 4.3.18.T1 need to be assessed for applicability to the system since they may not all be appropriate. Table 4.3.18.T1 is not all inclusive and does not include any additional design considerations levied by the Service, Center, platform, or domain. Not all design considerations are equally important or critical to a given program, but all should be examined for relevancy.

Table 4.3.18.T1. Design Considerations

Design Consideration	DAG Section Number	Statutory Requirement	Policy & Guidance
Accessibility (Section 508 Compliance)	**4.3.18.1.**	• Section 508 of the Rehabilitation Act of 1973 (as amended 36 CFR Part 1194)	• DoDD 8000.01 • DoD 8400.01-M • FAR 39.204
Affordability - SE Trade-Off Analysis	**4.3.18.2.**		• USD(AT&L) memorandum, "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending," November 13, 2012 • USD(AT&L) memorandum, "Implementation Directive for Better Buying Power-Restoring Affordability and Productivity in Defense Spending," November 3, 2010 • USD(AT&L) memorandum, "Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending," September 14, 2010

Design Consideration	DAG Section Number	Statutory Requirement	Policy & Guidance
Anti-Counterfeiting	**4.3.18.3.**	• FY2012 National Defense Authorization Act (NDAA)	• USD(AT&L) memorandum, "Overarching DoD Counterfeit Prevention Guidance," March 16, 2012
Commercial-Off-the-Shelf (COTS)	**4.3.18.4.**	• Sections 403 and 431 of title 41, United States Code • Public Law 103-355 • Public Law 104-106	• DoDI 5000.02, Enclosure 2
Corrosion Prevention and Control (CPC)	**4.3.18.5.**	• Section 2228 of title 10, United States Code	• DoDD 5000.01, Enclosure 1, paragraph E1.1.17 • DoDI 5000.02, Enclosure 12, paragraph 7 • DoDI 5000.67 • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • DoD Corrosion Prevention and Control Planning Guidebook • DFARS 223.73
Critical Safety Item (CSI)	**4.3.18.6.**	• Section 802 of Public Law 108-136 • Section 130 of Public Law 109-364 • Section 2319 of title 10, United States Code	• DoD 4140.1-R • JACG Aviation CSI Management Handbook • SECNAVINST 4140.2 • AFI 20-106 • DA Pam 95-9 • DLAI 3200.4 • DCMA INST CSI (AV) Management of Aviation Critical Safety Items • DFARS 209.270, 246.407, 246.504, 246.371 and 252.246-7003
Demilitarization and Disposal	**4.3.18.7.**		• DoDI 4160.28, Volume 1 • DoDI 5000.02, Enclosure 2, paragraph 8.c.(2) • DoD 4140.1-R • DoD 4160.21-M • MIL-STD-882E
Diminishing Manufacturing Sources and Material Shortages (DMSMS)	**4.3.18.8.**		• SD-22

Design Consideration	DAG Section Number	Statutory Requirement	Policy & Guidance
Environment, Safety, and Occupational Health (ESOH)	**4.3.18.9.**	• National Environmental Policy Act (NEPA) • Section 4321-4347 of title 42, United States Code • Executive Order 12114, Environmental Effects Abroad of Major Federal Actions	• DoDI 4715.9 • DoDI 5000.02, Enclosure 12 • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • MIL-STD-882E • DFARS 223.73 • FAR 23.2, 23.4, 23.7 and 23.8
Human Systems Integration (HSI)	**4.3.18.10.**		• DoDD 5000.01, Enclosure 1, paragraph E1.1.29 • DoDI 5000.02, Enclosure 8
Insensitive Munitions	**4.3.18.11.**	• Section 2389 of title 10, United States Code	• DoDD 6055.9 • Secretary of Defense Memorandum, "DoD Policy on Submunition Reliability," January 10, 2001 • USD(AT&L) Memorandum, "Joint Insensitive Munitions Test Standards and Compliance Assessment," February 10, 2010 • USD(AT&L) Memorandum, "Insensitive Munitions Strategic Plans," July 21, 2004 • DoD Acquisition Manager's Handbook for Insensitive Munitions, Revision 02, November 2008
Intelligence (Life-cycle Mission Data Plan (LMDP))	**3.3.18.12.**		• DoDD 5250.01
Interoperability and Dependency (I&D)	**4.3.18.13.**	• Public Law 104-106 • Section 3506 of title 44, United States Code	• DoDD 4630.05 • DoDD 5000.01 • DoDI 2010.06 • DoDI 4630.8 • DoDI 5000.02 • CJCSI 3170.01 • CJCSI 6212.01 • JCIDS Manual

Design Consideration	DAG Section Number	Statutory Requirement	Policy & Guidance
Item Unique Identification (IUID)	**4.3.18.14.**		• DoDD 8320.03 • DoDI 4151.19 • DoDI 4140.01 • DoDI 5000.02, Enclosure 12, paragraph 10 • DoDI 5000.64 • DoDI 8320.04 • PDUSD(AT&L) Memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • DoD Guide to Uniquely Identifying Items, Version 2.5, September 15, 2012 • DoD Guidelines for Engineering, Manufacturing and Maintenance Documentation Requirements, April 20, 2007 • DFARS 211.274-2, 252.211-7003, 252.211-7007
Open Systems Architecture (OSA)	**4.3.18.15.**	• Section 2430 of title 10, United States Code	• DoDI 5000.02, Enclosure 12, paragraph 8 • DoD 5010.12-M • USD(AT&L) Memorandum, "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending," November 13, 2012
Operational Energy	**4.3.18.16.**	• Section 138c of title 10, United States Code	• CJCSI 3170.01 • JCIDS Manual
Packaging, Handling, Storage and Transportation (PHS&T)	**4.3.18.17.**	• Title 49 of the Code of Federal Regulations (49 CFR)	• DoDI 4540.07 • DoD 4145.19-R • DoD 4140.27-M • DTR 4500.9-R
Producibility, Quality & Manufacturing (PQM)	**4.3.18.18.**	• Section 812 of National Defense Authorization Act FY2011	• DoDI 5000.02, Enclosure 2 • DFARS 207.105, 215.304

Design Consideration	DAG Section Number	Statutory Requirement	Policy & Guidance
Reliability & Maintainability (R&M) Engineering	**4.3.18.19.**	• Public Law 111-23, Weapon System Acquisition Reform Act 2009	• DoDI 5000.02, Enclosure 12 • DTM 11-003 • PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011 • DoD Reliability, Availability, Maintainability, and Cost Rationale (RAM-C) Report Manual
Spectrum Management	**4.3.18.20.**	• Sections 305 and 901 - 904 of title 47, United States Code • Section 104 of Public Law 102-538	• DoDD 3222.3 • DoDI 4650.01 • DoDI 5000.02, Enclosure 12, paragraph 11 • AR 5-12 • AFI 33-118 • OPNAVINST 2400.1 and 2400.2 • OPNAVINST 2400.20F
Standardization	**4.3.18.21.**	• Sections 2451-2457 of title 10, United States Code • Public Law 82-436	• DoDI 4120.24 • DoD 4120.24-M • SD-19
Supportability	**4.3.18.22.**		• DoDD 5000.01, Enclosure 1, paragraphs E1.1.17, E1.1.29 • DoDI 4151.22 • PDUSD(AT&L) Memorandum, "Document Streamlining - Life-Cycle Sustainment Plan (LCSP)," September 14, 2011 • DoD 4140.1-R • DoD 4151.22-M • SD-19 • MIL-HDBK-502
Survivability (including CBRN) & Susceptibility	**4.3.18.23.**		• DoDI 3150.09 • DoDI 5000.02, Enclosures 6 and 8
System Security Engineering (SSE)	**4.3.18.24.**	• Section 2358 of title 10, United States Code	• DoDI 5000.02, Enclosure 4 • DoDI 5200.39 • DoDI 5200.44 • DODI 8500 Series • PDUSD(AT&L) memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011 • Program Protection Plan Outline and Guidance, Version 1.0, July 2011

4.3.18.1. Accessibility (Section 508 Compliance)

4.3.18.1. Accessibility (Section 508 Compliance)

All Electronic and Information Technology (E&IT) systems comply with Section 508 of the Rehabilitation Act (as amended 36 CFR Part 1194), unless exempt under FAR 39.204 as a military system or National Security System. Compliance with Section 508 provides access by Federal employees with disabilities and the public to information and data that able-bodied persons can access through E&IT systems. Section 508 should be considered as a design requirement, addressed at each technical review, and clearly stated in the Acquisition Strategy and Systems Engineering Plan.

Program Managers should ensure Section 508 compliance, unless exempt, while Systems Engineers are responsible for implementation through use of standards and compliant tools and products.

Resources to aid programs in complying are in Table 4.3.18.1.T1. Additional information on accessibility is found in DAG Chapter 6 Human Systems Integration and Chapter 7 Acquiring Information Technology, Including National Security Systems.

Table 4.3.18.1.T1. Links to Section 508 Government Resources

Description of Link	Active Link
Section 508 technical standards	http://www.access-board.gov/508.htm
Federal rules for Section 508 implementation hosted by GSA has: • Roles and responsibilities of procurement officials and engineers • 508 best practices • Products and techniques	http://www.section508.gov/index.cfm
The "Buy Accessible System" GSA site has free tools and guides for conduct of Section 508-compliant acquisitions as well as on-line training and help desk	http://www.buyaccessible.gov/ and section.508@gsa.gov help desk
Department of Health and Human Services has: • Check lists • Code library • Test tools	http://www.hhs.gov/ found by searching on "section 508"
Department of Justice home page for ADA has federal laws and pending legislation	http://www.ada.gov/
Department of Veteran Affairs reports on Section 508 products and tools and tracks user comments	http://www.section508.va.gov/

4.3.18.2. Affordability - Systems Engineering Trade-Off Analyses

4.3.18.2. Affordability - Systems Engineering Trade-Off Analyses

Affordability is the degree to which the capability benefits are worth the system's total life-cycle cost and support DoD strategic goals. Systems engineering (SE) trade-off analyses for affordability, a special application of the Decision Analysis process (see DAG section 4.3.3. Decision Analysis Process), supports the establishment of a realistic affordability target, serves as inputs for the will cost and should cost estimates, and enables continuous monitoring of affordability estimates across the system life cycle. SE trade-off analyses should always practice continuous improvement, value engineering and Lean Six Sigma.

Although not a mandated Key Performance Parameter (KPP), the affordability target is managed throughout the system life cycle as a system KPP and cannot be changed without Milestone Decision Authority (MDA) approval. The USD(AT&L) memorandum "Implementation Directive for Better Buying Power Restoring Affordability and Productivity in Defense Spending" requires the program to establish an affordability target at Milestone A. This affordability target forms the basis for the SE trade-offs and sensitivity analyses that is conducted in support of Milestone B, and subsequent reviews. The affordability target is nominally the average unit acquisition cost and average annual operations and support cost per unit. For indefinite quantity of production units, the affordability target may be the total acquisition cost (see DAG Chapter 3 Affordability and Life-Cycle Resource Estimates for more information regarding the affordability target).

The independently generated will cost estimate is used to defend the system budget but does not account for potential efficiencies. The should cost estimate is based on efficient use of resources and effective implementation of processes, and is the focus of SE activities and program management decisions across the life cycle.

The SE trade-offs are conducted among cost, schedule, and performance objectives to ensure the program is affordable. The Program Manager should identify the design performance points that are the focus of trade-off analyses to establish cost and schedule trade space. The Program Manager presents the results of the trade-off analyses at program milestone/technical reviews, showing how the affordability target varies as design performance and schedules are varied (affordability drivers) and demonstrating how the cost-effective design point is established for the program.

The Program Manager and Systems Engineer use the results of SE trade-off analyses for affordability to inform system requirements and ensure that, when taken collectively, the requirements are compelling, affordable, and achievable within the time frame available to the program. These requirements are normally characterized by creative alternatives, reliable information and models, well-reasoned aggregation techniques, and a sound recommendation and action plan.

The trade-off analyses are executed by a resourced team that consists of a decision maker with full responsibility, authority, and accountability for the trade at hand, a trade-off analyst with a suite of reasoning tools, subject matter experts with performance models, and a representative set of end users and other stakeholders.

Throughout the system life cycle, the Systems Engineer continuously monitors affordability drivers, identifies opportunities to reduce life-cycle costs, and conducts trade-off analyses as needed to meet program cost, schedule, and performance requirements.

4.3.18.3. Anti-Counterfeiting

4.3.18.3. Anti-Counterfeiting

An increasing threat of counterfeit (and fraudulent) parts in the global marketplace affects every component of the program from commercial-off-the-shelf (COTS) assemblies to military-unique systems. Preventing counterfeit parts from entering the supply chain reduces cost and negative impacts to program schedule and system performance. "Overarching DoD Counterfeit Prevention Guidance" policy memorandum was signed by USD(AT&L) on March 16, 2012.

Counterfeit parts are becoming pervasive in various supply chains and therefore have become a significant threat to the Defense supply chain. Counterfeiters motives are primarily greed (profit) and/or malicious intent. Counterfeits may appear at all phases of the life cycle, making it necessary for the Program Manager, Systems Engineer, and Product Support Manager to plan for prevention, detection, remediation, reporting, and restitution activities from the beginning of the life cycle to disposal and demilitarization.

Anti-counterfeit activities have relations, as describe in Table 4.3.18.3.T1, with many of the other design considerations outlined in DAG section 4.3.18. Design Considerations, such as:

Table 4.3.18.3.T1. Anti-Counterfeit Design Consideration Relationships

Design Consideration	Relationship
Commercial-Off-the-Shelf (COTS)	The Government and its industry agents have little to no visibility into the supply chains that create COTS products. Implications of this lack of visibility into the supply chain include counterfeit vulnerabilities and counterfeit parts being more readily available.
Corrosion Prevention and Control (CPC)	Counterfeits, by their nature, may have been falsely certified. In addition, if the counterfeit is a compound/material or component (e.g., gaskets, ground wires) intended to prevent or reduce corrosion, then effects of wear may appear sooner than predicted and the impacts to the system may be worse than expected or catastrophic.

Design Consideration	Relationship
Critical Safety Items (CSI)	From an anti-counterfeiting risk-based approach, CSI should be more carefully scrutinized to ensure no counterfeits infiltrate the supply chain.
Demilitarization and Disposal	An excellent source for counterfeiters to obtain parts that can be turned into "used sold as new" parts (fraudulently certified as new).
Diminishing Manufacturing Sources and Material Shortages (DMSMS)	As systems age and the trustworthy sources for the piece parts dry up, counterfeiters increasingly take advantage of the situation by offering a source for hard-to-find-parts.
Environment, Safety, and Occupational Health (ESOH)	Several examples of counterfeit materials that can increase ESOH risks include: false R-134, a refrigerant which produces explosive by-products; fire extinguishers compressed with air; and faulty smoke detectors. Furthermore, Restriction of Hazardous Substances (RoHS) (2002/95/EC) has led to increased numbers of counterfeits, where a lead-free (Pb-free) microcircuit is sold as having tin-lead (SnPb) leads.
Item Unique Identification (IUID)	Successful implementation of IUID could reduce the ability of counterfeiters to introduce parts into supply. Conversely, IUID may provide a false sense of security if it can be duplicated by counterfeiters.
Open Systems Architecture (OSA)	OSA could provide a means to quickly certify a newer, more available part for use in weapon systems, thus reducing the impact of DMSMS. Conversely, it could also result in more part numbers (equivalents) being introduced into supply thus increasing the likelihood of counterfeit intrusion.
Producibility, Quality, and Manufacturing (PQM)	PQM can be severely degraded if supply is contaminated with counterfeits.
Reliability and Maintainability Engineering	Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the "honest" part.
Supportability	Increased failure rates due to counterfeits can have a negative impact on supportability and might drive the wrong problem-resolution behaviors and increase sustainment costs.
System Security Engineering (SSE)	SSE implements anti-counterfeit protection measures as part of a comprehensive plan to protect CPI and mission-critical functions and components.

During development of the Systems Engineering Plan (SEP), the Program Manager, Systems Engineer, and Product Support Manager should consider these relationships and develop plans to address the threat.

4.3.18.4. Commercial-Off-the-Shelf

4.3.18.4. Commercial-Off-the-Shelf

The use of commercial-off-the-shelf (COTS) items, including Non-Developmental Items, can provide significant opportunities for efficiencies during system development but also can introduce certain issues that should be considered and mitigated if the program is to realize the expected benefits. Investigation of COTS product use is required by DoDI 5000.02, Enclosure 2.

The primary benefits of using COTS components in system design are to:

- Reduce development time
- Allow faster insertion of new technology
- Lower life-cycle costs by taking advantage of the more readily available and up-to-date commercial industrial base

However, regardless of the extent to which a system is made up of commercial items, the Program Manager still engineers, develops, integrates, tests, evaluates, delivers, sustains, and manages the overall system.

Among concerns with using COTS products are:

- Subtle differences in product use can significantly affect system effectiveness, ESOH, reliability, and durability
- If integration requires a "modified COTS product," meaning that a COTS product may not be designed for many military environments (which, by definition, is not a COTS product under section 403 of title 41, United States Code, but is allowed under section 431 of title 41, United States Code), then the program may lose the ability to use the vendor's subsequent product upgrades or to find a suitable replacement for the product from other commercial sources
- The vendors can embed proprietary functions into COTS, limiting supply sources
- Vendors do not have to provide design information and often restrict purchasers from reverse engineering their intellectual property
- Licensing agreements vary and can be very restrictive while limiting the vendors liability for merchantability for intended purposes
- Supply chain risk management of COTS items is limited by the vendor, who is under no obligation to the purchaser to provide such information
- Incorporating COTS products places constraints on the rest of the design and reduces trade space; functionality, interfaces, and reliability and maintainability characteristics are embedded in the choice of a COTS system element
- Difficulty in finding suitable replacements and/or alternate items if the COTS vendor stops manufacturing the product or changes the configuration drastically, requiring the need to maintain different configurations of a single product
- The program needs to understand the "pedigree" or the qualified vendors for the COTS product

- The graphical user interface (GUI) design may not completely support user tasks, which can cause inefficient workarounds and improper use of the system by the user

The marketplace drives COTS product definition, application, and evolution. COTS products presume a flexible architecture and often depend on product releases that are designed to be used "as is" to meet general business needs and not a specific organization's needs. The commercial product life cycle is usually much shorter than the equivalent military product life cycle. Programs should consider the potential availability of suitable replacement and/or alternative items throughout the longer, military life cycle, and should monitor the commercial marketplace through market research activities and ongoing alignment of business and technical processes. This necessary activity imposes additional cost, schedule, and performance risks that the acquisition community should plan for. COTS products should be evaluated to meet all performance and reliability requirements during all environmental conditions and service life requirements specified by the intended application requirements documents.

The Federal Acquisition Streamlining Act (FASA) of 1994 (Public Law 103-355) and the Clinger-Cohen Act (Public Law 104-106) both endorse the use of COTS products by the Federal Government but have slightly different definitions, with the latter allowing for modifications to COTS.

The Systems Engineer should ensure open system design, identification and mitigation of Environment, Safety, and Occupational Health (ESOH) and security risks, survivable technology insertion, or refresh throughout the projected system life cycle.

The Program Manager and Systems Engineer should consider the following when evaluating use of COTS products:

- The intended product use environment and the extent to which this environment differs from (or is similar to) the commercial use environment
- Integration, documentation, security, Human System Integration, ESOH, hardware/software integrity, reliability risk, operational environment, and corrosion susceptibility/risk, etc.
- Planning for life-cycle activities (including sustainment, supply chain risks, obsolescence, and disposal)
- Developing relationships with vendors, Foreign Ownership Control, and Influence (FOCI) (see Defense Security Service for the latest policy regarding COTS from FOCI sources)
- Supportability, if vendor or marketplace changes occur
- Test and evaluation of COTS items (including early identification of screening, functionality testing and usability assessments) (See DAG Chapter 9 Test and Evaluation, Chief Development Tester)
- Protecting intellectual property rights by being aware of pertinent intellectual property right issues associated with commercial items acquisitions, especially with the acquisition of commercial software products. When acquiring Intellectual

Property (IP) license rights, the acquisition community should consider the core principles described in the DoD guide: "Intellectual Property: Navigating through Commercial Waters."
- Ability to modify or interface COTS software with other software even if Government generated or owned
- Ability to have insight into configuration management, and the features and functions of upgrades and changes
- Ability to instrument and/or test aspects of COTS products

4.3.18.5. Corrosion Prevention and Control

4.3.18.5. Corrosion Prevention and Control

The corrosion of military equipment and infrastructure within the DoD has been documented to cost approximately $23 billion annually. In addition to its significant financial impact, corrosion can also adversely affect system availability and ESOH. Therefore, it is extremely important to plan for and implement corrosion prevention and mitigation as early as possible in the acquisition life cycle (even prior to Milestone A) to minimize the life-cycle impact.

The execution of a program's Corrosion Prevention and Control (CPC) planning should contribute to reduced corrosion vulnerability with lower life-cycle costs; and improved ESOH, maintainability, and availability.

Section 2228 of title 10, United States Code requires planning and execution of corrosion prevention and mitigation in DoD systems. Accordingly DoDI 5000.02 and 5000.67 require corrosion prevention and control planning for all acquisition programs across the life cycle. Elements of good CPC engineering include, but are not limited to, the following:

- Examination of legacy systems for possible corrosion design improvements
- Open and transparent assessment of alternative materials and processes that offer increased protection against corrosion
- Inclusion of CPC as a consideration in trade studies involving cost, useful service life, and effectiveness
- Incorporation of CPC criteria into relevant contractual documentation
- Identification, planning, resourcing, and acquisition of corrosion-related features for longevity, lowest total ownership cost (TOC), and maximum of effectiveness in support of the program

In the PDUSD(AT&L) memorandum, "Document Streamlining - Program Strategies and Systems Engineering Plan," April 20, 2011, Program Managers are directed to capture all design considerations relating to CPC planning within the Systems Engineering Plan (SEP) with "hotlinks" to the program's CPC Plan.

The Program Manager is responsible for ensuring resources, including corrosion

engineering expertise, are available throughout the program and that corrosion performance is considered appropriately during design trades. The Systems Engineer, supported by CPC subject matter experts, is responsible for identifying corrosion concerns and developing mitigation strategies within the whole system design and operational construct.

All designated Acquisition Category (ACAT) programs are required to accomplish CPC planning across their life cycle, with ACAT I programs required to formally document this planning in an approved CPC Plan delivered at Milestones B and C. In addition, the DoD has developed the Corrosion Prevention and Control Planning Guidebook as a resource to assist the Program Manager, Systems Engineers, and other program staff in the development of a robust CPC program.

For all ACAT programs, CPC engineering should be reflected in various program documents, including, but not limited to:

- Technology Development Strategy/Acquisition Strategy (TDS/AS)
- SEP
- Test and Evaluation Master Plan (TEMP)
- Life-Cycle Sustainment Plan (LCSP)
- Contract/Request for Proposal (RFP)
- Program schedule - Integrated Master Plan/Integrated Master Schedule (IMP/IMS)
- Funding/budget
- Programmatic ESOH Evaluation (i.e., DFARS Subpart 223.73, Minimizing the Use of Hexavalent Chromium)
- System finish/process specification (add as a Data Item Description (DID) to Contract Data Requirements List (CDRL))
- System Performance Specification design, build, and testing requirements

In the contract and RFP, CPC planning should be addressed in some fashion in the technical content of each contract/RFP Section and subsection, including, but not limited to the Statement of Work (SOW), IMP/IMS, CDRL, and system performance specification (see DAG section 4.1.6. SE Role in Contracting).

4.3.18.6. Critical Safety Item

4.3.18.6. Critical Safety Item

Critical Safety Item (CSI) is a part, assembly, or support equipment whose failure could cause loss of life, permanent disability or major injury, loss of a system, or significant equipment damage. Special attention should be placed on CSIs to prevent the potential catastrophic or critical consequences of failure. Significant problems occurred when DoD purchased CSIs from suppliers with limited knowledge of the item's design intent, application, failure modes, failure effects, or failure implications. The definition of CSI is not to be confused with the MIL-STD-882E definition of a Safety Critical Item (SCI). A

SCI is "a hardware or software item that has been determined through analysis to potentially contribute to a hazard with catastrophic or critical mishap potential, or that may be implemented to mitigate a hazard with catastrophic or critical mishap potential."

The purpose of CSI analysis is to ensure that Program Managers for DoD acquisition programs who enter into contracts involving CSIs do so only with resources approved by the Design Control Activity (DCA). The DCA is defined by law as the systems command of a military department. The DCA is responsible for the airworthiness or seaworthiness certification of the system in which a CSI is used.

The intent of CSI laws, policies, regulations, and guidance is to avoid hazards through mitigating receipt of defective, suspect, improperly documented, unapproved, and fraudulent parts having catastrophic potential. These statutory requirements are contained in section 802 of Public Law 108-136, enacted to address aviation CSIs, and section 130 of Public Law 109-364, enacted to address ship CSIs, embedded in section 2319 of title 10, United States Code. The statute addresses three specific areas:

- Establish that the DCA is responsible for processes concerning the management and identification of CSIs used in procurement, modification, repair, and overhaul of aviation and ship systems.
- Require that DoD work only with sources approved by the DCA for contracts involving CSIs.
- Require that CSI deliveries and services performed meet all technical and quality requirements established by the DCA.

CSI policies and guidance ensure that items of supply that are most critical to operational safety are rigorously managed and controlled in terms of:

- Supplier capability
- Conformance to technical requirements
- Controls on changes or deviations
- Inspection, installation, maintenance, and repair requirements

DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation establishes top-level procedures for the management of aviation CSIs. The Joint Aeronautical Commanders Group issued the Aviation Critical Safety Items (CSIs) Management Handbook. This guidance establishes standard user-level operating practices for aviation CSIs across the Services, the Defense Logistics Agency (DLA), the Defense Contract Management Agency (DCMA), and other Federal agencies. Appendix I of the Aviation CSI Management Handbook is a joint Military Service/Defense Agency instruction on "Management of Aviation Critical Safety Items" issued on January 25, 2006. This instruction (SECNAVINST 4140.2, AFI 20-106, DA Pam 95-9, DLAI 3200.4, and DCMA INST CSI (AV)) addresses requirements for identifying, acquiring, ensuring quality, managing, and disposing of aviation CSIs. Similar policies and guidance are being developed and/or revised to address ship CSIs as defined by public law.

The Defense Federal Acquisition Regulation Supplement (DFARS) was amended to implement the contractual aspects regarding aviation CSIs. Comparable DFARS amendments are being developed to address ship CSIs. DFARS 209.270 states that the DCA is responsible to:

- Identify items that meet aviation CSI criteria
- Approve qualification requirements
- Qualify suppliers

This supplement states that the contracting activity contracts for aviation CSIs only with suppliers approved by the DCA. Program Managers should coordinate with the contracting activity to ensure that they contract for aviation CSIs only with suppliers approved by the DCA and that nonconforming aviation CSIs are to be accepted only with the DCA's approval, as required by DFARS 246.407. DFARS 246.407 was amended to state that DCA authority can be delegated for minor nonconformance. DFARS 246.504 requires DCA concurrence before certificates of conformance are issued to accept aviation CSIs.

Because the system developer may uncover problems with products after items are delivered, DFARS 246.371 and 252.246-7003 require the developer to notify the procuring and contracting officers within 72 hours after discovering or obtaining credible information that a delivered CSI may have discrepancies that affect safety. Program Managers should coordinate with the contracting authority to be kept aware of materiel recalls and shortfalls that may impact production rates and sustainment.

The CSI list evolves as the design, production processes, and supportability analyses mature. Program Managers identify and document CSIs during design and development to influence critical down-stream processes such as initial provisioning, supply support, and manufacturing planning to ensure adequate management of CSIs throughout a system's Operations and Support (O&S) phase. The Program Manager should make provisions for developers including original equipment manufacturer (OEM) contractors to deliver an initial allocated baseline at the Preliminary Design Review (PDR), to include an initial list of proposed CSIs and a proposed process for selecting and approving CSIs as well as addressing the critical characteristics of those items. Prior to the Critical Design Review (CDR), the program office, with support from the DCA and developer/OEM contractors, should ensure there is a clear understanding of CSI processes, terms, and criteria. The initial product baseline is delivered at CDR and at that time the program should have 100% of drawings completed for the CSIs. Throughout Low-Rate Initial Production (LRIP) (if applicable), conduct of the Physical Configuration Audit (PCA), and establishment of the final product baseline, the program should update the CSI list and review it to ensure the list reflects the delivered system. Before the Full-Rate Production / Full Deployment Decision Review (FRP/FD DR), a final CSI list should be documented and approved by the DCA.

4.3.18.7. Demilitarization and Disposal

4.3.18.7. Demilitarization and Disposal

The incorporation of demilitarization (DEMIL) and disposal requirements into the initial system design is critical to ensure compliance with:

- All DoD DEMIL and disposal policies.
- All legal and regulatory requirements and policies relating to safety (including explosive safety), security, and the environment.

Program Managers and Program Support Managers should ensure, as an essential part of systems engineering, that DEMIL and disposal requirements are incorporated in system design to minimize DoD's liabilities, reduce costs, and protect critical program information and technology. This includes integrating DEMIL and disposal into the allocated baseline approved at the Preliminary Design Review (PDR) and refining DEMIL and disposal requirements in the initial product baseline at the Critical Design Review (CDR). DEMIL and disposal requirements are included in the program's Systems Engineering Plan (SEP), the Life-Cycle Sustainment Plan (LCSP), and the contract(s). For munitions programs, DEMIL and disposal documentation need to be in place before the start of Developmental Test and Evaluation.

DEMIL renders safe and eliminates functional capabilities and inherent military design features from both serviceable and unserviceable DoD materiel. It is the act of destroying the military offensive or defensive advantages inherent in certain types of equipment or material. DEMIL may include mutilation, scrapping, melting, burning or alteration designed to prevent the further use of this equipment and material for its originally intended military or lethal purpose. Systems Engineers integrate DEMIL considerations into system design to recover critical materials and protect assets, information, and technologies, from uncontrolled or unwanted release and disruption or reverse engineering. Program Managers should ensure the DEMIL of materiel is accomplished in accordance with DoDI 4160.28, DoD Demilitarization (DEMIL) Program.

Disposal is the process of reusing, transferring, donating, selling, destroying, or other ultimate disposal of excess surplus and foreign excess property. Disposal first ensures adequate screening is accomplished to satisfy that all valid DoD and other United States Government agency needs are met. After assurances that Government needs for surplus DoD property are met, the materiel disposition process:

- Permits authorized transfer or donation to Government or non-Government entities
- Obligates DoD to obtain the best available monetary return to the Government for property sold

Program Managers ensure disposal is accomplished in accordance with DoD 4140.1-R,

Supply Chain Materiel Management Regulation and DoD 4160.21-M, Defense Materiel Disposition Manual.

The program's plan for demilitarization and disposal of DoD excess and surplus property protects the environment and personnel and minimizes the need for abandonment or destruction. During systems design, the Systems Engineer supports the Program Manager's plans for the system's demilitarization and disposal, through the identification and documentation of hazards and hazardous materials related to the system, using MIL-STD-882E, DoD Standard Practice for System Safety. Early, balanced analyses of ESOH hazards relative to the system's design, enable the Program Manager to make informed decisions based on alternatives and provide a clear understanding of trade-offs and consequences, both near term and over the systems life cycle.

4.3.18.8. Diminishing Manufacturing Sources and Material Shortages

4.3.18.8. Diminishing Manufacturing Sources and Material Shortages

Diminishing Manufacturing Sources and Material Shortages (DMSMS) is the loss, or impending loss, of manufacturers or suppliers of items, raw materials, or software. DMSMS-generated shortages in the ongoing production capability or life-cycle support of a weapon system or shortages in any training, support, or test equipment already in the field can endanger mission effectiveness. While DMSMS issues can be caused by many factors, their occurrence is inevitable.

The Program Manager should incorporate a technology management strategy into design activities as a best practice to reduce DMSMS cost and readiness impacts throughout the life cycle. The Program Manager and Systems Engineer should develop a technology management strategy for maintaining insight into technology trends, and internal product changes by the manufacturer and testing the effects of those changes on the system when necessary. This insight into technology trends could potentially:

- Result in seamless upgrade paths for technologies and system elements
- Provide a timetable for replacing system elements even if they are not obsolete

The Systems Engineer should be aware of and consider DMSMS management during system design. Following are several practices that the program should consider to minimize DMSMS risk throughout the life cycle of the system:

- Avoid selecting technology and components that are near the end of their functional life
- During the design process, proactively assess the risk of parts obsolescence while selecting parts
- When feasible, use an Open Systems Architecture (OSA) to enable technology insertion/refreshment more easily than with design-specific approaches
- Proactively monitor supplier bases to prevent designing in obsolescence;

participate in cooperative reporting forums, such as the Government-Industry Data Exchange Program (GIDEP), to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment
- Proactively monitor potential availability problems to resolve them before they cause an impact in performance readiness or spending

A useful resource for additional guidance is SD-22, "Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook."

4.3.18.9. Environment, Safety, and Occupational Health

4.3.18.9. Environment, Safety, and Occupational Health

Environment, Safety, and Occupational Health (ESOH) analyses are an integral, ongoing part of the systems engineering (SE) process throughout the life cycle. The benefits of early integration of ESOH considerations include:

- Mitigation of program cost and schedule risks from actions that cause damage to people, equipment, or the environment
- Reduction of Operations and Support and disposal costs
- Provision of a safe, suitable, supportable, and sustainable capability able to operate world-wide

Throughout each acquisition phase, programs conduct the ESOH analyses to:

- Identify and mitigate potential risks to the system and its associated personnel
- Manage ESOH design considerations from the beginning of the SE effort
- Plan for compliance with the National Environmental Policy Act (NEPA) and Executive Order (EO) 12114, Environmental Effects Abroad of Major Federal Actions
- Ensure compliance with statutory ESOH requirements

Efforts to identify and analyze hazards, and mitigate ESOH risks provide information needed for informed design decisions and development of ESOH-related documentation for milestone decisions.

DoD defines ESOH in MIL-STD-882E, DoD Standard Practice for System Safety as *"the combination of disciplines that encompass the processes and approaches for addressing laws, regulations, EOs, DoD policies, environmental compliance, and hazards associated with environmental impacts, system safety (e.g., platforms, systems, system-of-systems, weapons, explosives, software, ordnance, combat systems), occupational safety and health, hazardous materials management, and pollution prevention."*

ESOH System Design Requirements

The Systems Engineer identifies the ESOH requirements applicable to the system throughout its life cycle from statutes, regulations, policies, design standards, and capability documents. From these requirements, the Systems Engineer should derive ESOH design requirements and include them in capability documents, technical specifications, solicitations, and contracts.

ESOH in Program Documents

The Acquisition Program Office ESOH-specific documents are the Programmatic ESOH Evaluation (PESHE) and the NEPA/EO 12114 Compliance Schedule. The Systems Engineering Plan (SEP) contains the ESOH management planning information. The SEP, PESHE, and NEPA/EO 12114 Compliance Schedule provide inputs to program documentation that include, but are not limited to: Technology Development Strategy (TDS), Test and Evaluation Strategy (TES), Test and Evaluation Master Plan (TEMP), Life-Cycle Sustainment Plan (LCSP), Corrosion Prevention and Control Plan (CPCP), system specifications, solicitations, and contracts; and capability documents.

The SEP contains ESOH design considerations as an integral part of the requirements analysis process, including trade study criteria. ESOH design considerations are particularly important for Milestone A to ensure SE addresses ESOH during the Technology Development (TD) phase, which includes a significant amount of the design development, testing, and the Preliminary Design Review. SEP Table 4.6-1 includes the information listed in Table 4.3.18.9.T1. Additional ESOH details are provided in SEP Sections 3.4 and 3.6; Tables 2.2-1, 3.4.4-1, 3.4.4-2, and 4.4-1; and Figure 3.4.1-1.

Table 4.3.18.9.T1. ESOH Information in SEP

Column Heading in SEP Table 4.6-1	Expected Information (provided or attached)
Cognizant PMO Organization	Organizational structure for integrating ESOH (or refer to Table 3.4.4-2 if it includes the ESOH team details) and the Program Office ESOH point of contact
Certification	Required ESOH approvals, endorsements, releases, and the designated high and serious risk acceptance user representative(s)
Documentation	PESHE and NEPA/EO 12114 Compliance Schedule
Contractual Requirements (CDRL#)	ESOH contractual language, ESOH Contract Data Requirements List (CDRL) items, and ESOH DFARS clauses
Description / Comments	Description of how design minimizes ESOH risks by summarizing how the program has integrated ESOH considerations into SE processes including the method for tracking hazards and ESOH risks and mitigation plans throughout the life cycle of system

The PESHE documents the ESOH design consideration data produced by executing

the ESOH planning described in the SEP. The PESHE includes, but is not limited to:

- ESOH Risk Matrices (for hardware and software) used by the program with definitions for severity categories, probability levels, risk levels, and risk acceptance and user representative concurrence authorities.
- The following data for each hazard: Hazard Tracking System (HTS) identification number, hazard description, potential mishap, initial Risk Assessment Code (RAC) and risk level, mitigation measure(s) and funding status, target RAC and risk level, current RAC and risk level, and risk acceptance and user concurrence status (**NOTE:** providing an electronic copy of the current data from the HTS would satisfy this requirement).
- The following data for each hazardous material, hazardous waste, and pollutant associated with the system: the specific uses, locations, quantities, and plans for their minimization and/or safe disposal (**NOTE:** providing an electronic copy of the current data from either the HTS (if it includes this information) or the hazardous materials management data would satisfy this requirement).
- Environmental impact information not included in the HTS or hazardous materials tracking system needed to support installation and range analyses.

NOTE: The results of the sustainability analysis (see DAG section 4.3.19.2. Sustainability Analysis) should be used to inform the hazard analysis.

DoDI 5000.02, Enclosure 12 requires that each program maintain a NEPA/EO 12114 compliance schedule. This schedule includes, but is not limited to:

- Each proposed action (e.g., testing or fielding)
- Proponent (as defined in DoDI 4715.9) for each action
- Anticipated start date for each action at each specific location
- Anticipated NEPA/EO 12114 document type
- Anticipated start and completion dates for each document
- The document approval authority

Because actions occurring during the TD phase may require NEPA/EO 12114 compliance, the program should develop a TD Compliance Schedule for inclusion in the SEP. DoDI 5000.02, Enclosure12 also requires programs to support other organizations NEPA/EO 12114 analyses involving their systems.

ESOH Activities by Phase

Table 4.3.18.9.T2. aligns typical ESOH activities by phase.

Table 4.3.18.9.T2. ESOH Activities by Phase

Acquisition Phase	Typical ESOH Activities
Materiel Solution Analysis (MSA)	• Participate in Analysis of Alternatives (AoA) • Provide inputs to the SEP, draft Capability Development Document (CDD), Corrosion Prevention and Control (CPC) Planning, TDS, Test and Evaluation (T&E) Strategy (TES), Life-cycle Sustainment Plan (LCSP), and draft Request for Proposal (RFP)
Technology Development (TD)	• Participate in prototyping and design development through the IPT structure • Prepare initial PESHE and NEPA/EO 12114 Compliance Schedule • Ensure NEPA/EO 12114 compliance, ESOH risk acceptance, Preliminary Design Review (PDR) risk reporting, and safety releases • Inputs to SEP, CPC Planning, final CDD, Test and Evaluation Master Plan (TEMP), LCSP, and draft RFP
Engineering and Manufacturing Development (EMD)	• Participate in trades and design development activities through the IPT structure • Evaluate T&E results, to include assessment of ESOH risk mitigations • Update NEPA/EO 12114 Compliance Schedule and PESHE; support NEPA/EO 12114 compliance activities, ESOH risk acceptance • Obtain required ESOH approvals, endorsements, and releases; provide inputs to the SEP, CPC Planning, LCSP, Capability Production Document (CPD), and draft RFP
Production and Deployment (P&D)	• Participate in initial Configuration Control Board (CCB) process • Evaluate T&E results, to include assessment of ESOH risk mitigations • Analyze deficiency reports • Review Physical Configuration Audit (PCA) • Update NEPA/EO 12114 Compliance Schedule and PESHE • Support NEPA/EO 12114 compliance activities and ESOH risk mitigations • Obtain required ESOH approvals, endorsements, and releases • Support Initial Operational Capability (IOC) and Full Operational Capability (FOC) • Provide inputs to the LCSP, CPC Planning, and product support package
Operations and Support (O&S)	• Participate in mishap investigations and the CCB process • Analyze deficiency reports • Keep the PESHE data current; support NEPA/EO 12114 compliance activities and ESOH risk acceptance • Provide inputs to draft Joint Capabilities Integration and Development System (JCIDS) documents and CPC Planning

ESOH Risk Management

The Systems Engineer uses the MIL-STD-882E process to identify and assess hazards

(to include software safety), eliminate hazards where possible, and manage ESOH risks where hazards cannot be eliminated. MIL-STD-882E provides a matrix and defines probability and severity criteria to categorize ESOH risks. Prior to exposing people, equipment, or the environment to known system-related hazards, the Systems Engineer ensures ESOH risks are formally accepted, which includes formal concurrence on high and serious risks by the designated user representative as defined in MIL-STD-882E (or by each participating Service user representative in a Joint program). DoDI 5000.02 identifies the appropriate management level authorized to accept ESOH risks.

For Joint programs, the Component Acquisition Executive of the Lead Executive Component should be the acceptance authority for high-level risks. The program documents formal risk acceptances as part of the program record (e.g., Hazard Tracking System (HTS)). If a risk level increases for a hazard, a new risk acceptance is required prior to exposing people, equipment, or the environment to the increased risk. The program also participates in system-related mishap investigations to assess contributing hazards, risks, and mitigations.

DoDI 5000.02, Enclosure 12 requires programs to report the status of current high and serious ESOH risks at program reviews and fielding decisions and the status of all ESOH risks at technical reviews. The purpose of this reporting is to inform the Milestone Decision Authority (MDA), Program Executive Office (PEO), Program Manager, and end user about trades being made and ESOH risks that need to be accepted. Each ESOH risk report includes the following: the hazard, potential mishap, initial Risk Assessment Code (RAC) and risk level, mitigation measure(s) and funding status, target RAC and risk level, current RAC and risk level, and risk acceptance / user representative concurrence status.

Hazardous Materials (HAZMAT) Management

When Hazardous Materials (HAZMAT) and chemicals/materials of evolving regulatory concern are designed into the system or used for system operation and maintenance, the Systems Engineer assesses and documents the ESOH risks for each combination of HAZMAT and application. The Systems Engineer also documents:

- The locations, quantities, and usage of each HAZMAT
- Safe demilitarization and disposal requirements
- Energetic qualification information, as applicable
- Reasonably anticipated quantities of hazardous waste generated during normal operation and maintenance
- Hazardous emissions/discharges including those anticipated in emergency situations
- Special training, handling, and storage requirements

The Systems Engineer manages hexavalent chromium usage in systems to balance the requirements for corrosion control and prevention and the procedures in DFARS Subpart 223.73 - Minimizing the Use of Hexavalent Chromium. For more information on

chemicals/materials of evolving regulatory concern, refer to the DENIX website.

Safety Release for Testing

The Program Manager, in concert with the user and the T&E community, provides safety releases (to include formal ESOH risk acceptance in accordance with DoDI 5000.02, Enclosure 12, Section 6), to the developmental and operational testers before any test using personnel. The safety release addresses each system hazard present during the test and include formal risk acceptance for each hazard. The program's safety release is in addition to any test range safety release requirements, but it should support test range analyses required for a range-generated test release. The program documents safety releases as part of the Program Record.

The Program Manager should provide a transmittal letter to the involved test organization with a detailed listing of the system hazards germane to the test that includes the current risk level and documented risk acceptance along with information on all implemented mitigations.

Green Procurement Program (GPP)

In an effort to enhance and sustain mission readiness over the system life cycle, reduce reliance on resources, as well as reduce the DoD footprint, programs should follow the policy and procedures identified in the DoD Green Procurement Program (GPP). GPP benefits include:

- Reducing resource consumption
- Ensuring availability of chemicals and materials
- Reducing waste generation
- Contributing to regulatory compliance

Program Managers should implement the applicable GPP procedures in Federal Acquisition Regulation (FAR) Subparts 23.2, 23.4, 23.7 and 23.8 to select materials and products that are energy-efficient, water conserving, and environmentally preferable. More information on GPP is available on the DENIX website.

Key Resources

- Acquisition Community Connection/ESOH
- Defense Acquisition University Continuous Learning Modules "CLE 009 -- ESOH in Systems Engineering" and "CLR 030 - ESOH in JCIDS"
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Federal Acquisition Regulation (FAR)
- Joint Software System Safety Engineering Handbook, August 27, 2010
- MIL-STD-882E with 25 optional Tasks

4.3.18.10. Human Systems Integration

4.3.18.10. Human Systems Integration

Systems engineering (SE) addresses the three major elements of each system: hardware, software, and human. SE integrates human capability considerations with the other specialty engineering disciplines to achieve total system performance requirements by factoring into the system design the limitations of the human users.

During system design, Systems Engineer should apply Human Systems Integration (HSI) and Human Factors Engineering (HFE) design criteria, principles, and practices described in MIL-STD-1472, Human Engineering and MIL-STD-46855A, Human Engineering Requirements for Military Systems, Equipment and Facilities.

The HSI effort minimizes ownership costs and ensures the system is built to accommodate the human performance characteristics of users who operate, maintain, and support the total system. The total system includes not only the mission equipment but also the users, the training and training devices, and the operational and support infrastructure.

The Program Manager has overall responsibility for integrating the HSI effort into the system program. These responsibilities are described in DAG Chapter 6 Human Systems Integration.

The Systems Engineer supports the Program Manager and is responsible for HSI. The Systems Engineer should work with the manpower, personnel, training, safety, health, habitability, personnel survivability, and HFE stakeholders to develop the HSI effort. The Systems Engineer translates and integrates those human capability considerations, as contained in the capabilities documents, into quantifiable system requirements. Requirements for conducting HSI efforts should be specified for inclusion in the Statement of Work and contract and included in the Systems Engineering Plan (SEP), specifications, the Test and Evaluation Master Plan (TEMP), the Life-Cycle Sustainment Plan (LCSP), and other appropriate program documentation. The SEP Outline requires that HSI be addressed as a mandatory design consideration in Table 4.6-1.

Elements of an effective HFE effort, described in DAG Chapter 6 Human Systems Integration, should:

- Provide a better operational solution to the warfighters
- Lead to the development or improvement of all human interfaces of the system
- Achieve required effectiveness of human performance during system testing, operation, maintenance, support, transport, demilitarization and disposal
- Make for more economical demands upon personnel resources, skills, training, and costs

4.3.18.11. Insensitive Munitions

4.3.18.11. Insensitive Munitions

Insensitive Munitions minimize the probability of inadvertent initiation and the severity of subsequent collateral damage to weapon platforms, logistic systems, and personnel when munitions are subjected to unanticipated stimuli during manufacture, handling, storage, transport, deployment, or disposal, or due to accidents or action by an adversary.

Insensitive Munitions is a component of explosive ordnance safety described in section 2389 of title 10, United States Code, which specifies that it is the responsibility of DoD to ensure insensitive munitions under development or procurement are safe, to the extent practicable, throughout development and fielding when subjected to unplanned stimuli, e.g., electro-magnetic interference, vibration, or shock. The Program Manager and the Systems Engineer for munitions programs such as: ordnance, warheads, bombs, and rocket motors and munitions handling, storage, and transport programs have an overriding responsibility to address safety aspects of their programs in trade studies, design reviews, milestone reviews, and in JCIDS documents.

The Program Manager and Systems Engineer for munitions acquisition programs, regardless of the ACAT level, should have safety as a top consideration when performing trade studies or making program decisions. The term "Insensitive Munitions" implies that unanticipated stimuli will not produce an explosive yield, in accordance with MIL-STD-2105D, Hazard Assessment Tests for Non-Nuclear Munitions. The Program Manager and cognizant technical staff should coordinate harmonized Insensitive Munitions/Hazard Classification (HC) test plans with the Service Insensitive Munitions/Hazard Classification (HC) review organizations. The Service organizations should coordinate the Insensitive Munitions/Hazard Classification (HC) with the Joint Services Insensitive Munitions Panel (JSIMTP), Joint Service Hazard classifiers, and the DoD Explosives Safety Board (DDESB), is chartered by DoDD 6055.9E, Explosives Safety Management and the DDESB. Aspects of Insensitive Munitions also apply to nuclear weapons but are not addressed herein.

The primary document to address Insensitive Munitions is the Insensitive Munitions Strategic Plan (IMSP), as required by USD(AT&L) memorandum, "Insensitive Munitions Strategic Plans," July 21, 2004, which establishes Department of Defense Policy for the annual submission of Insensitive Munitions Strategic Plans to the Joint Requirements Oversight Council (JROC) and Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (OUSD(AT&L)), by the Program Executive Officer (PEO) for munitions programs. USD(AT&L) memorandum, "Joint Insensitive Munitions Test Standards and Compliance Assessment." February 10, 2010, provides for oversight and compliance assessment. The DoD Standard Operating Procedure (SOP) for IMSP and the Plan of Action and Milestones (POA&M), defined by Joint Business Rules, March 2011, define the content of the IMSP, which spans the Future Years Defense Plan (FYDP) and includes currently funded as well as unfunded requirements. The DoD

Acquisition Manager's Handbook for Insensitive Munitions contains the above-referenced documents and appendices for each Service's policy and review board process.

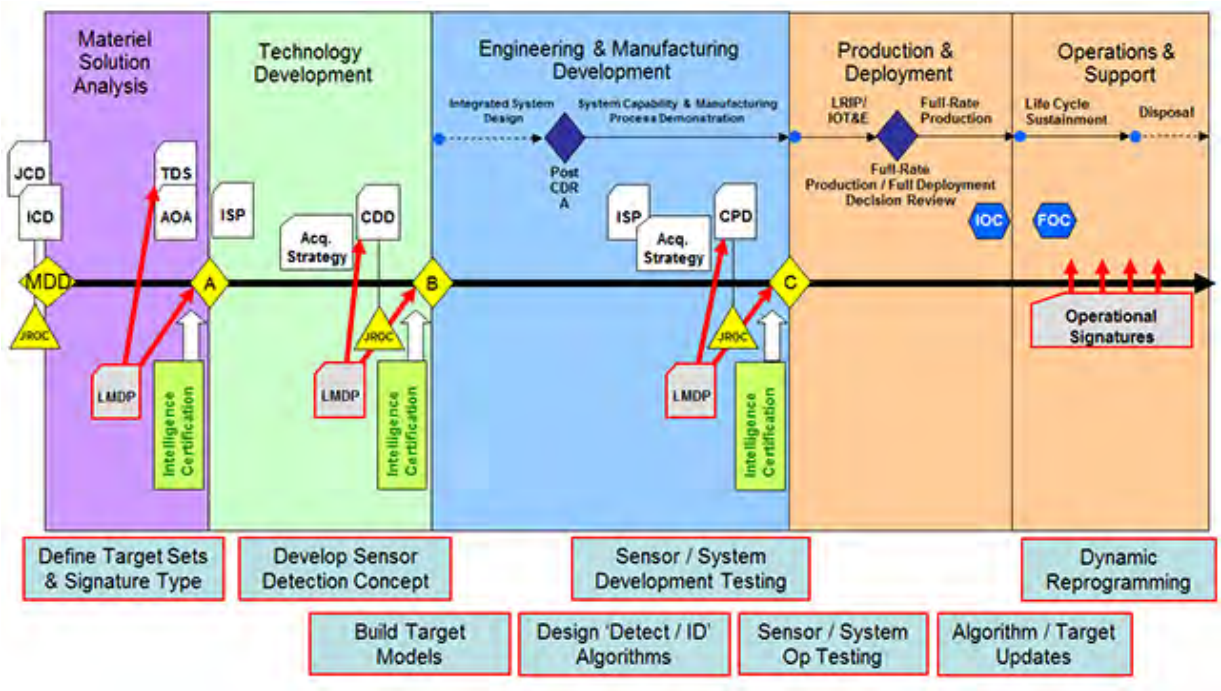
The IMSP is the primary program output required by USD(AT&L) and the Joint Staff to provide evidence that the program is in compliance with all applicable laws and regulations. Both the Component-level and DoD-level insensitive munitions review organizations can provide additional guidance and can assess the adequacy of the IMSP. In addition to the IMSP, the Analysis of Alternatives (AOA), Acquisition Strategy (AS), Systems Engineering Plan (SEP), Test and Evaluation Master Plan (TEMP), Risk Management Plan, Corrosion Prevention and Control Plan (CPCP), and other JCIDS documents called for in CJCSI 3170 and the JCIDS Manual (requires Common Access Card (CAC) to access website), address aspects of explosive ordnance safety, including Insensitive Munitions.

4.3.18.12. Intelligence (Life-Cycle Mission Data Plan)

4.3.18.12. Intelligence (Life-Cycle Mission Data Plan)

Modern weapon systems are inherently dependent on a variety of scientific and technical intelligence products throughout every stage of their life cycle. Intelligence Mission Data (IMD) provides essential data for building system models, developing algorithms, optimizing sensor design, system testing and evaluation, and validating sensor functionality. Therefore, it is imperative to ensure IMD is considered, identified, and applied throughout the life cycle of IMD-dependent programs by informing the Analysis of Alternatives (AoA) and continuing through disposal. See Figure 4.3.18.12.F1.

Figure 4.3.18.12.F1. Intelligence Mission Data (IMD) Life Cycle Timeline



The Program Manager, Systems Engineer, and Test and Evaluation Manager are the primary functional program office leads responsible for the identification and programming of unique IMD to support the program beginning at MS A (see DoDD 5250.01).

IMD is necessary to:

- Derive functional baseline requirements and intelligence signature requirements (sensors, algorithms, and other entities that require intelligence data) identified in the Life-Cycle Mission Data Plan (LMDP) (based upon mission and environment) (see LMDP template)
- Allocate the functional baseline necessary to identify sensors, algorithm, and intelligence database
- Design, develop, test, and evaluate IMD dependent sensors, systems, processes, and interfaces
- Conduct trade-off studies, effectiveness analysis, and risk assessments
- Develop technical performance measures to inform test and evaluation
- Inform decision-making and science and technology investments for identifying the intelligence signature, and intelligence mission data, production, and collection requirements
- Assess system capability and limitations
- Ensure system flexibility and agility in response to dynamic threat and environment

DAG Chapter 8 Intelligence Analysis Support to Acquisition provides key linkages to the System Requirements Document (SRD), Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP).

These three products are directly affected by the intelligence signature and mission data requirements.

4.3.18.13. Interoperability and Dependencies

4.3.18.13. Interoperability and Dependencies

Almost all DoD systems operate in a system-of-systems (SoS) context relying upon other systems to provide desired user capabilities, making it vital that interoperability needs and external dependencies are identified early and incorporated into system requirements. When identifying system requirements, it is critical to consider the operational and SoS context (see DAG section 4.2.1.2. Systems of Systems). These include, but are not limited to, physical requirements (e.g., size, power limits, etc.), electronic requirements (e.g., signature, interference, etc.) and information exchange/management (e.g., network, bandwidth, information needs, etc.). These also include interdependencies with other systems. For efficiency, systems often rely on either services provided by other systems during operations or reuse of system elements developed by other programs.

The Program Manager is responsible for ensuring that the operational and SoS context for the system are well understood.

The Systems Engineer has the primary responsibility for ensuring all interoperability and dependency impacts are analyzed and collaborated with the appropriate internal/external stakeholders and are translated into system requirements and design considerations.

Analysis conducted for the SoS contexts for the system -- where the system is dependent on other systems and where the system needs to interact with other systems - enables translation of I&D into system requirements. I&D requirements call for collaborative implementation approaches with external organizations, including identification, management, and control of key interfaces. Areas of dependency and interoperability should be reviewed for risks to the program and plans made to manage and mitigate those risks. This review includes system interdependencies (e.g., weapon may depend on new sensor capabilities provided by another system) and information exchanges with other systems required to support mission capabilities. For efficiency, systems may rely on system elements developed by others for key functionality, either through services (e.g., weather information) provided by other systems or through reuse of system elements (e.g., engines, radios) developed by other programs. These contexts are analyzed to identify system requirements and risks, including actions needed by external parties (e.g., other systems or infrastructure) for the system to meet

user requirements.

Additional DoD policy and guidance regarding I&D, summarized below, are directed at ensuring that systems work effectively with other systems:

- Interoperability of information technology and National Security System (NSS) acquisition programs are required to comply with DoDD 4630.05, DoDI 4630.8, CJCSI 3170.01, the JCIDS Manual (requires Common Access Card (CAC) to access website), CJCSI 6212.01, Public Law 104-106, and section 3506 of title 44, United States Code.
- DoDD 5000.01, Enclosure 1 :
    - Ability of acquired systems to exchange information and services with other systems and to interoperate with other United States forces and coalition partners, and as appropriate with other United States Government departments and agencies
    - Providing systems and systems of systems that are interoperable and able to communicate across a universal infrastructure that includes organizational interactions, other systems, networks, and information exchange capabilities
- DoDI 5000.02, Enclosure 2 : An integrated system design that defines system and system-of-systems functionality and interfaces, and reduces system-level risk
- DoDI 2010.06 : Pursuing opportunities throughout the acquisition life cycle that enhance international cooperation and improve interoperability

4.3.18.14. Item Unique Identification

4.3.18.14. Item Unique Identification

Properly implemented, Item Unique Identification (IUID)-enabled Serialized Item Management (SIM) provides a capability that allows DoD to locate, control, value, and manage its assets throughout the life cycle. A robust SIM program provides tools and processes to assist informed decision making to achieve both better weapon system reliability and readiness at reduced total ownership cost. As a key enabler, IUID is a systematic process to globally and unambiguously distinguish one item from all other items that DoD buys or owns. IUID-enabled SIM provides DoD with a standard methodology to:

- Consistently capture the value of all individual items it buys/owns
- Trace these items during their use
- Combat counterfeiting of parts
- Associate valuable business intelligence to an item throughout its life cycle via automatic identification technology and connections to automated information systems

Program Managers and Product Support Managers should budget, plan for, and

implement IUID-enabled SIM as an integral activity within MIL-STD-130 requisite item identification processes to identify and track applicable major end items and configuration-controlled items. IUID implemented in accordance with DoDI 8320.04 and IUID Implementation Plans are required for all milestone decisions as directed by DoDI 5000.02. IUID-specific design considerations are required in the Systems Engineering Plans (SEP), and SIM planning and implementation required by DoDI 4151.19 are addressed in the Life-Cycle Sustainment Plan (LCSP).

The Systems Engineer considers what to mark and how to incorporate the IUID mark within MIL-STD-130 item marking requirements when formulating design decisions. In addition, the Systems Engineer considers where product and maintenance information reside and how the life-cycle data is used within the configuration management and product support systems - including new and legacy information systems.

The DoD Guide to Uniquely Identifying Items, provides guidance on implementing IUID intended for use by Department of Defense (DoD) contractors and their suppliers who put unique item identifier (UII) marks on new items during production, as directed in the contract.

4.3.18.15. Open Systems Architecture

4.3.18.15. Open Systems Architecture

Open Systems Architecture (OSA) benefits Program Managers by using established and working frameworks that are already crafted with component reuse in mind, such that many common services and applications can be quickly instantiated with small effort from program to program. Adding features to address evolving threats to an already tested, fielded, and working component is far less risky than a "ground up" new development start. OSA is identified as a key tenet of Better Buying Power, under Promoting Effective Competition, because it enhances system interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions of the enterprise. It is also addressed in DoDI 5000.02.

An open architecture is defined as a technical architecture that adopts open standards supporting a modular, loosely coupled, and highly cohesive system structure that includes the publishing of key interfaces within the system and relevant design disclosure. The key enabler for open architecture is the adoption of an open business model that requires doing business in a transparent way that leverages the collaborative innovation of numerous participants across the enterprise, permitting shared risk, maximized reuse of assets, and reduced total ownership costs. The combination of open architecture and an open business model permits the acquisition of OSA that yield modular, interoperable systems allowing components to be added, modified, replaced, removed, and/or supported by different vendors throughout the life cycle in order to afford opportunities for enhanced competition and innovation.

OSA benefits warfighters by:

- Reducing operator learning curves by using systems that have similar functions and are operated in similar ways thereby reducing costs
- Increasing interchangeability
- Reducing support and sustainment costs

The engineering trade analyses conducted prior to MS B help determine which system elements of program architecture can be adapted to OSA in order to reduce program cost and development time lines. Correct application of OSA principles and practices results in modular architecture components having well-defined functions and open standards-based interfaces. Threat analyses, functional criticality analyses, technology opportunities, and evolved capability assessments are examples of assessments against the functional architecture to determine what components should be OSA-enabled. When these architecture components require upgrade, replacement is competitive, faster, and cheaper because the OSA-enabled components are modular. Because system functional architecture maps from the higher-level enterprise architecture, engineering trade analyses and assessments supporting OSA should be completed and OSA-enabled architecture components specified, before contracts are let for technology development of those architecture components. Successful implementation of OSA approaches requires the synchronized acquisition of data rights for OS and interfacing architecture elements. These data rights are initially structured to support acquisition of modular open system designs but also should address life-cycle support.

Acquisition programs adopting OSA benefit from:

- Reduced acquisition and sustainment cost without sacrificing capability
- Reduced reliance on single-source vendors ("Vendor Lock")
- Shortened program acquisition time line
- Enhanced rapid and agile development
- Accelerated transition from science and technology into acquisition due to modular insertion
- Increased ability to retrofit/upgrade system elements for new/evolving capability
- Enhanced incremental approach to capabilities
- Increased competition and innovation
- Enhanced ability to create security structures within a design to reduce security risk

DoDI 5000.02 identifies the use of OSA as a key systems engineering (SE) approach in Enclosure 12, paragraph 8. The USD(AT&L) memorandum, "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending," November 13, 2012, raises the relevance of OSA along with acquisition of data rights for appropriate architecture elements. The overarching business case for DoD is increasing the level of competition by enabling small business. Programs should develop a business model documenting the strategy for use of OSA and associated

data rights. The OSA-DR Charter signed by USD(AT&L) on February 15, 2012, requires programs to issue business case guidance to aid programs in developing their business models.

The DoD Open Systems Architecture Contract Guidebook for Program Managers contains guidance regarding contract language programs should use to acquire data rights in support of a program's OSA strategy. Additional information and supporting details amplifying each aspect of OSA is available on the DASD(SE) website.

The Program Manager should:

- Establish supportive requirements; business practices; and technology development, acquisition, test and evaluation, and product support strategies for effective development of open systems
- Ensure their data deliverables support their Technical Data Rights Strategy (see Acquisition Strategy template) and secure the necessary data rights to support and sustain the system
- Map Open Systems strategy and functional architecture to SOW requirements, Data Item Descriptions (DIDs), and CDRLs consistently across the enterprise
- Ensure compliance
- Consider including OSA as one of the evaluation criteria for contract proposals
- Determine the appropriateness of an OSA approach by considering software constraints, security requirements and procedures, availability and cost of data rights, life-cycle affordability, and reliability of open standards, as well as other relevant factors such as environmental constraints (e.g., temperature, humidity, and environment, safety, and occupational health (ESOH))

The Systems Engineer should:

- Employ an overall plan for and OSA approach that supports program functional architecture and that uses prescribed USD(AT&L) business case analyses
- Ensure the program functional architecture is structured to accommodate OSA where feasible, due to the high potential for reduced risk and cost
- Assess performance
- Balance current implementation of OSA with performance and evolving technology at the physical level; OSA establishes a technical baseline that may support modular architecture, but formally constrains the interfaces between modules, where interfaces close to current performance limits may quickly become obsolete
- Technically evaluate the appropriateness of an OSA approach by considering software constraints, security requirements and procedures, availability and cost of data rights, life-cycle affordability, and reliability of open standards, as well as other relevant factors such as environmental constraints (e.g., temperature, humidity, and ESOH)

Modular open system designs, developed from the system architecture, should be

analyzed at each design review because there is a link between OSA and the level and type of technical data, computer software, and data rights the Government needs for life-cycle support. In many cases weapon systems using OSA system elements can have increased opportunities for competitive sourcing during the life-cycle sustainment, and a correspondingly less need for detailed design data and associated data rights. This benefit enables an incremental approach to capability adaptation in OSA-enabled systems and is a benefit of the modularity originally specified into the functional architecture.

Figure 4.3.18.15.F1. Sample OS and Data Rights Analysis

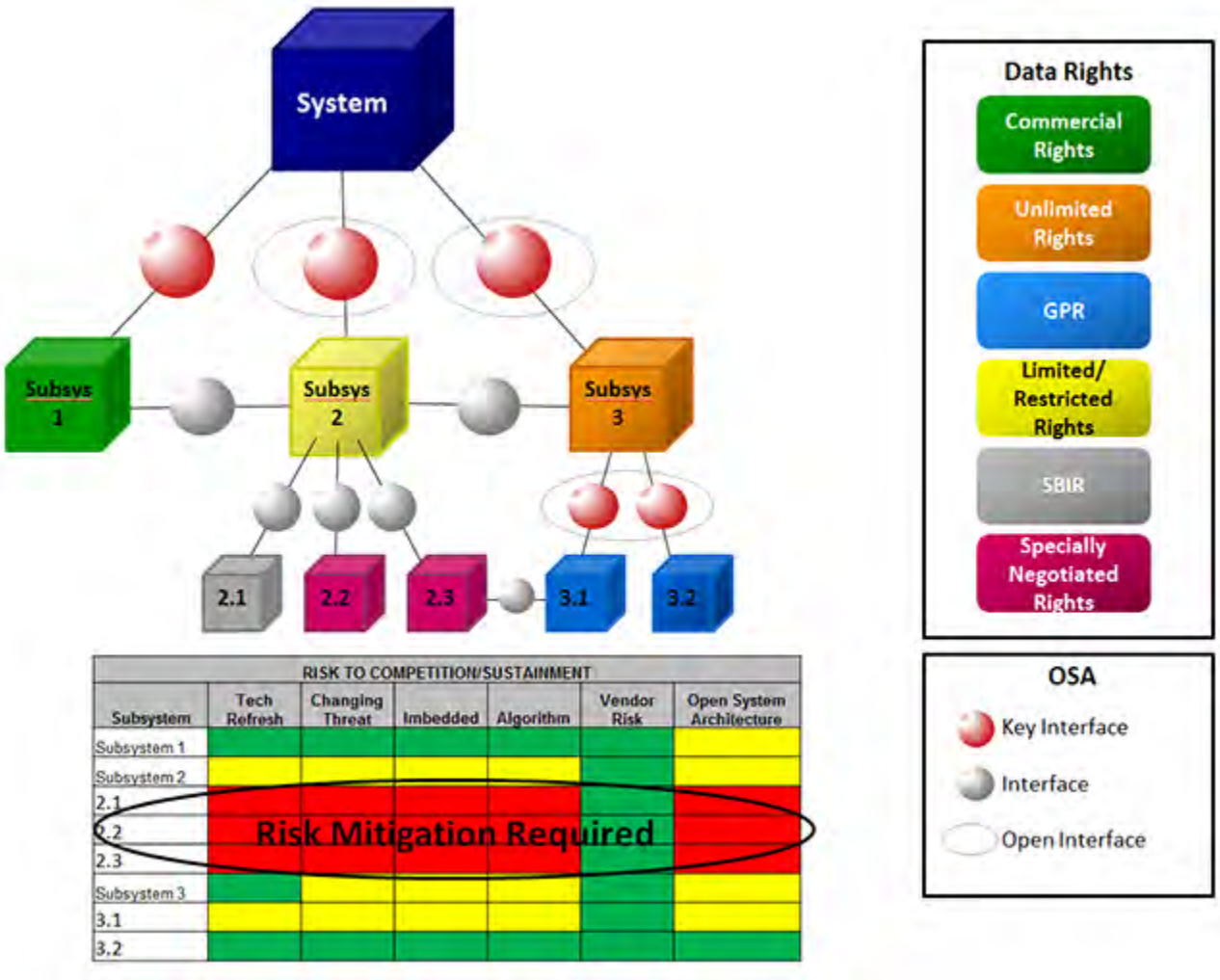


Figure 4.3.18.15.F1 depicts an example architectural approach for mapping and assessing which component interfaces can be open, how associated risk is ascertained, and visualizing the impact to interfaces with other system elements. The figure presents a top-level system view of the OSA characteristics of system architecture components. Not all interfaces need to be open at any one level of the design, only those that are required to meet anticipated incremental capability updates or changes in threat or

technology insertion. A system view such as this one includes a record of the data rights that are required to enable the planned OSA design. This is to initially ensure and, for the life-cycle sustainment, maintain the strong link between the OSA design and the acquired data rights that enable it. The levels of data rights that need to be required for each OSA-enabled architecture component are determined in order to assert the requisite contract requirements to obtain them. The data rights strategy ensures that enterprise-level data rights flow to system architecture components and that they support the system architecture. Levels of data rights are described in DAG Chapter 2 Program Strategies and in Appendix 9 of the OSA Contract Guidebook.

Successfully implementing an OSA strategy results in identification of required technical data and software deliverables that are necessary to field and maintain weapon systems and their logistics support. The Technology Development Strategy and Acquisition Strategy should be updated throughout the system's life cycle to reflect changes in the OSA approach resulting from technology and software evolutionary developments. The Systems Engineering Plan (SEP) also is updated to reflect the OSA-related updates and modifications employed throughout the system and its system elements.

Specific OSA-related data deliverables that should be required to include:

- Software Development Plans (DI-IPSC-81427A)
- Software Development Status Reports (DI-MCCR-80459)
- Software Development Summary Reports (DI-MCCR-80902)
- Software Design Descriptions (DI-IPSC-81435A)

In addition, the Program Manager should maintain an open systems management plan. The plan describes the offeror's approach to:

- OSA, modularity, and open design
- Inter-component dependencies
- Design information documentation
- Technology insertion
- Life-cycle sustainability
- Interface design and management
- Treatment of proprietary or vendor-unique elements
- Reuse of preexisting items including all commercial-off-the-shelf/non-developmental Item (COTS/NDI) components, their functionality and proposed function in the system
- Copies of license agreements related to the use of COTS/NDI components for Government approval

The open system management plan also should include a statement explaining why each COTS/NDI was selected for use.

Program products typically used in making decisions regarding OSA include:

- System Requirements
- Technology Development Strategy (TDS) or Acquisition Strategy (AS)
- Program Protection Plan (PPP)
- Analysis of Alternatives (AoA)
- Enterprise Architecture

OSA approaches and requirements should be addressed at design reviews, e.g., System Readiness Review (SRR), Preliminary Design Review (PDR), and Critical Design Review (CDR).

See DoD ASSIST homepage for more data item deliverables that may be appropriate for each specific program and DoD 5010.12-M for data deliverables.

4.3.18.16. Operational Energy

4.3.18.16. Operational Energy

Emerging threats to the logistic resupply of operational forces, the trend toward ever greater energy demand in the operational forces, and increasing costs to operate and resupply energy-intensive systems have all put increasing focus on lowering system and unit energy demand. Reducing the force's dependence on energy logistics can improve the force's mobility and resilience and increase its control over the timing and conditions of the fight. Focusing on energy as an explicit design consideration and systems engineering (SE) category is a significant change in practice and thinking, to help manage emerging operational challenges.

The Program Manager and Systems Engineer can help lower operational energy by addressing issues associated with the system's energy logistics support and power resupply frequency.

This approach should generate informed choices based on the threshold and objective values of the Energy Key Performance Parameter (KPP) for the system. For liquid energy-consuming systems, the top-level units of measure for the Energy KPP might be gallons of fuel demanded (consumed) over a defined set of duty cycles, or to accomplish a specified mission goal such as a sortie. These measures may be further decomposed into weight, range, electric power demand, and other relevant measures to inform the necessary SE trade analysis. The intended result is a comprehensive set of trade-space choices for industry to consider to deliver solutions that are not only energy efficient but also mission effective and affordable. See Joint Capabilities Integration and Development System (JCIDS) Manual (requires Common Access Card (CAC) to access website) and CJCSI 3170.01H linked at the end of this section.

Energy's relationship to performance arises from the operational context in which the system is used. Accordingly, the scenarios that illustrate how the system is used, as

part of a unit of maneuver, are essential to understanding the energy supply and demand constraints to be managed. This is essentially the same approach as balancing survivability goals against lethality goals in the engineering trade space. Operational energy issues include:

- How the system and combat unit refuel/recharge in the battlespace scenarios, and how often
- How this refueling/recharging requirement might constrain our forces (limit their freedom of action, on-station time, signature, etc.)
- How the adversary depicted in the defining scenarios might delay, disrupt, and/or defeat our forces by interdicting this system's refueling/recharging logistics
- How much force protection could be diverted from combat missions to protecting these refueling/recharging events when and where required

Systems Engineers should consider incorporating energy demand in design, technology, materials, and related issues into the system trade space along with other performance issues, so that oppressive energy resupply needs are not inadvertently introduced in the attempt to achieve other performance goals (e.g., survivability, lethality). In practice, this means requirement developers should factor into the system design the necessity of refueling/recharging using the same scenarios that are used to illustrate other performance requirements, and allowing the adversary a realistic chance to interdict the refueling/recharging effort. Systems Engineers may find it necessary to have a continuing dialogue with the warfighter (the user and requirements developer) to help grasp the operational impact of these issues and depict them in trade space decisions.

Energy-related engineering analysis should begin early enough to support initial Analysis of Alternatives (AoA) planning following the Materiel Development Decision, and should also be routinely updated to inform any AoA performed later in the life cycle (i.e., in support of block upgrades and modifications).

The following documents provide the Program Manager and Systems Engineer with additional insight into the issue of Operational Energy in the acquisition life cycle:

- CJCSI 3170.01H (for the Energy Key Performance Parameter)
- Joint Capabilities Integration and Development System (JCIDS) Manual (requires Common Access Card (CAC) to access website)
- Operational Energy Strategy: Implementation Plan
- Defense Science Board Task Force report on Operational Energy, February 2008
- Defense Science Board Task Force report on Operational Energy, May 2001

NOTE: The results of the sustainability analysis (see DAG section 4.3.19.2. Sustainability Analysis) can be used to inform energy analyses.

4.3.18.17. Packaging, Handling, Storage, and Transportation

4.3.18.17. Packaging, Handling, Storage, and Transportation

The program team employs Packaging, Handling, Storage, and Transportation (PHS&T) principles/methods to ensure the necessary equipment reaches the warfighter while minimizing risk of damage to the equipment during handling, storage, and transportation - frequently in highly challenging and corrosive operational environments.

Thorough PHS&T requirements promote supportability and sustainability of major end items, reparable system elements, and supporting test equipment. PHS&T focuses on transportation, handling, and storage constraints on performance resulting from driving size, weight, parts robustness, and shelf life.

Program Managers and Systems Engineers should ensure PHS&T is addressed during the requirements analysis process, and validated throughout each phase of the systems engineering (SE) development of the weapon system. DoDI 4540.07 identifies specifics regarding PHS&T as related to program management of weapon systems acquisitions. In addition, the following documents address PHS&T:

- MIL-STD-2073-1E, Department of Defense Standard Practice for Military Packaging
- MIL-STD-129P, Military Marking for Shipment and Storage
- ASTM-D3951, Standard Practice for Commercial Packaging
- DOD 4140.27-M, Self-Life Item Management Manual
- DTR 4500.9-R, Defense Transportation Regulation
- Title 49 of the Code of Federal Regulations (49 CFR)

4.3.18.18. Producibility, Quality, and Manufacturing Readiness

4.3.18.18.1. Producibility

4.3.18.18.2. Quality in Design

4.3.18.18.3. Assessing Manufacturing Readiness and Risk

4.3.18.18. Producibility, Quality, and Manufacturing Readiness

4.3.18.18.1. Producibility

Producibility (the relative ease of manufacturing), like manufacturing and other key system design functions, is integral to effectively and efficiently delivering capability to the warfighter. Producible designs are lower risk, more cost-effective, and repeatable, which enhances product reliability and supportability. Producibility should be assessed at both a product and enterprise (i.e., organizational) level. The Program Manager should implement producibility engineering and planning efforts early and should

continuously assess the integrated processes and resources needed to successfully achieve producibility.

To assess producibility on a product level, both the product and its manufacturing processes should be measured. Manufacturing processes should be monitored and controlled, through measurement, to ensure that they can repeatedly produce accurate, high-quality products, which helps the program meet objectives for limiting process variability to a tolerable range.

To assess producibility within a manufacturing enterprise level, the organization should evaluate producibility performance on a product-specific basis. This evaluation allows the organization to better understand the strengths and weaknesses of its producibility approach, so that enhancements can be identified and measures of processes, products, and the producibility system (integrated processes and resources needed for achieving producibility) can be tailored to strive for continuous improvement.

The Program Manager should ensure that the producibility program focuses on the following five elements to build and maintain a successful producibility system:

1. Establish a producibility infrastructure:

- Organize for producibility
- Integrate into the program's risk management program
- Incorporate producibility into the new product strategy
- Employ producibility design guidelines

2. Determine Process Capability:

- Determine Process Capability (Cpk)
- Understand and document company and supplier processes
- Plan for future process capabilities

3. Address producibility during initial design efforts:

- Identify design objectives
- Identify key characteristics of the design
- Perform trade studies on alternative product and process designs
- Develop a manufacturing plan
- Perform complexity analysis

4. Address producibility during detailed design:

- Address producibility measurements at Preliminary Design Review (PDR), Critical Design Review (CDR), Production Readiness Review (PRR), and Full-Rate Production Design Review (FRP DR)

- Optimize manufacturing plans as the design matures

5. Measure producibility processes, products and systems.

Producibility should be a Technical Performance Measure (TPM) for the program, and the program's strategy for producibility should be contained in paragraph 3.6 of the program's Systems Engineering Plan (SEP). Planned producibility engineering activities for previous and subsequent phases also should be summarized in the SEP. As a key design accomplishment, producibility should be included in the SEP, mapping key design considerations into the RFP and subsequently into the contract.

4.3.18.18.2. Quality in Design

Design engineering focuses on concurrent development of the total system using capable manufacturing processes leading to a producible, testable, sustainable and affordable product that meets defined requirements. The design phase is critical because product life-cycle costs are committed at this point. The objectives of quality design efforts are to:

- Achieve effective and efficient manufacturing with necessary process controls to meet system requirements
- Transition to production with no significant manufacturing process and reliability risks that could breach production thresholds for cost and performance

To ensure consistency in applying quality planning and process control, the program should establish Quality Management Systems (QMS) early (Milestone A). The QMS should be defined and documented in paragraph 11.2 of the Technology Development Strategy (TDS) and the Acquisition Strategy (AS). The process should be integrated into these documents as a systems engineering (SE) practice that supports the successful transition of capability development to full-rate production and delivery of systems to support warfighter missions.

The primary focus of the QMS should be to ensure efficiency in processes; when integrated with Statistical Process Control (SPC) (eliminate defects and control variation) the transition from system development to production should help with controlling life-cycle cost and reducing complexities that are often found when quality is not integrated as a function of the design. Therefore, to achieve high-quality (product characteristics meet specification requirements), an end product should be designed so:

- Processes to produce the end product are in statistical control (uniformity in manufacturing and production)
- Design specifications are aligned with manufacturing process capabilities
- Functional design integrates producibility requirements (measure of relative ease of manufacturing) with no significant compromises to quality and performance

The Program Manager and Systems Engineer should take into consideration that

process capability goes beyond machine capability. The process should include the effects of change in workers, materials, fabrication methods, tooling and equipment, setup, and other conditions. Process capability data should be collected throughout process and product development. Data collection efforts should be continuously refined, using test articles, through production.

In addition to QMS and SPC, understanding and improving processes may require common and/or new tools and techniques to eliminate defects and variation in processes.

Another quality management tool available to the program management team is parts management. MIL-STD-3018 provides requirements for the implementation of an effective Parts Management Program (PMP) on Department of Defense (DoD) acquisitions.

Quality should be a TPM for the program, and the program's strategy for managing quality should be included in the SEP. Planned quality engineering and management activities for previous and subsequent phases also should be summarized in the SEP. As a key design accomplishment, quality should be included in the SEP (Table 4.6-1) mapping key design considerations into contracts.

Two valuable tools to assist in creating quality in design are Six Sigma and Quality Function Development (QFD). Six Sigma techniques identify and reduce all sources of product variation - machines, materials, methods, measurement system, the environment, and the people in the process. QFD is a structured approach to understanding customer requirements and translating them into products that satisfy those needs.

4.3.18.18.3. Assessing Manufacturing Readiness and Risk

Manufacturing feasibility, processes, and risk should be assessed early (Materiel Solution Analysis (MSA) phase) and continuously through the Production and Deployment (P&D) phase on all acquisition programs. To ensure integration of manufacturing readiness and risk as part of design activities, the focus should be on system risk reduction, manufacturing process reliability, and producibility.

Program Managers should use existing manufacturing processes whenever practical to support low-risk manufacturing. When the design requires new manufacturing capability, the Program Manager may need to consider new manufacturing technologies or process flexibility (e.g., rate and configuration insensitivity), which introduces risk. DoDI 5000.02, Enclosure 2, defines the requirements for manufacturing processes and manufacturing risks. See DFARS 207.105, Contents of Written Acquisition Plans, for specific guidance on manufacturing actions planned by the Program Manager to execute the approach established in the Acquisition Strategy (AS) and to guide contractual implementation. These include:

- Consideration of requirements for efficient manufacture during the design and production of the system
- The availability of raw materials, special alloys, composite materials, components, tooling, and production test equipment
- The use of advanced manufacturing technology, processes, and systems
- The use of contract solicitations that encourage competing offerors to acquire modern technology, production equipment, and production systems (including hardware and software)
- Methods to encourage investment in advanced manufacturing technology, production equipment, and processes
- During source selection, increased emphasis on the efficiency of production
- Expanded use of commercial manufacturing processes rather than processes specified by DoD

Low-risk manufacturing readiness includes early planning and investments in producibility requirements, manufacturing process capabilities, and quality management to ensure effective and efficient manufacturing and transition to production. It also includes assessments of the industrial base. Manufacturing risk is evaluated through manufacturing readiness assessments, which are integrated with existing program assessments throughout the acquisition life cycle. The Program Manager should assess manufacturing readiness in the program's earliest phase and the assessment should be continuous. The Program Manager should report on the program's manufacturing readiness progress/status during each system's engineering technical review, Program Support Review, or their equivalent, and before each milestone decision.

Successful manufacturing has many dimensions. Industry and Government have identified best practices in the following nine manufacturing risk categories. Program Managers should use the best practices to assess their programs early and should report on these areas during technical reviews and before acquisition milestones. Implementation of these best practices should be tailored according to product domains, complexity and maturity of critical technologies, manufacturing processes, and specific risks that have been identified throughout the assessment process. These categories should help frame the risk assessment and focus mitigation strategies:

- Technology and the Industrial Base: assess the capability of the national technology and industrial base to support the design, development, production, operation, uninterrupted maintenance support, and eventual disposal (environmental impacts) of the system
- Design: assess the maturity and stability of the evolving system design and evaluate any related impact on manufacturing readiness
- Cost and Funding: examine the risk associated with reaching manufacturing cost targets
- Materials: assess the risks associated with materials (including basic/raw materials, components, semi-finished parts, and subassemblies)
- Process Capability and Control: assess the risks that manufacturing processes are able to reflect the design intent (repeatability and affordability) of key

characteristics
- Quality Management: assess the risks and management efforts to control quality and foster continuous improvement
- Manufacturing Workforce (Engineering and Production): assess the required skills, certification requirements, availability, and required number of personnel to support the manufacturing effort
- Facilities: assess the capabilities and capacity of key manufacturing facilities (prime, subcontractor, supplier, vendor, and maintenance/repair)
- Manufacturing Management: assess the orchestration of all elements needed to translate the design into an integrated and fielded system (meeting program goals for affordability and availability)

As part of the manufacturing strategy development effort, the Program Management team needs to understand the contractor/vendor business strategy and the impacts to Government risk identification and mitigation efforts, such as the Make/Buy decisions. Additional guidance on assessing manufacturing risks can be found in the Manufacturing Readiness Guide.

Assessment and mitigation of manufacturing risk should begin as early as possible in a program's acquisition life cycle-including conducting a manufacturing feasibility assessment as part of the AoA.

The Program Manager and Systems Engineer should consider the manufacturing readiness and manufacturing-readiness processes of potential contractors and subcontractors as a part of the source selection for major defense acquisition programs, see DFARS 215.304.

The Program Manager and Systems Engineer should assess manufacturing readiness at a minimum of four key points (events) during the acquisition life cycle, as described in Table 4.3.18.18.3.T1.

Table 4.3.18.18.3.T1. Minimum Points (Events) to Assess Manufacturing Readiness during the Acquisition Life Cycle

Manufacturing Readiness Assessment Points	Considerations
1. Post-AoA assessment during the Materiel Solution Analysis Phase. As part of the AoA, manufacturing risks should have been assessed for each of the competing alternatives (see the MRL Implementation Guide for one source of specific assessment factors). Risks for the preferred system concept should be assessed and identified at this point. The overall assessment should consider whether:	• Program critical technologies are ready for the Technology Development phase • Required investments in manufacturing technology development have been identified • Processes to ensure manufacturability, producibility, and quality are in place and are sufficient to produce prototypes. Manufacturing risks and mitigation plans are in place for building prototypes • Cost objectives have been established and manufacturing cost drivers have been identified; draft Key Performance Parameters have been identified as well as any special tooling, facilities, material handling, and skills required • Producibility assessment of the preferred system concept has been completed, and the industrial base capabilities, current state of critical manufacturing processes, and potential supply chain sources have all been surveyed

Manufacturing Readiness Assessment Points	Considerations
2. Technology Development, Pre-EMD Review. As the program approaches the Pre-EMD Review and the Milestone B decision, critical technologies should have matured sufficiently for 2366b certification and demonstrated in a relevant environment and should consider:	• The program should be nearing acceptance of a preliminary system design • An initial manufacturing approach has been developed • Manufacturing processes have been defined and characterized, but there are still significant engineering and/or design changes in the system itself; manufacturing processes that have not been defined or that may change as the design matures should be identified • Preliminary design, producibility assessments, and trade studies of key technologies and components should have been completed • Prototype manufacturing processes and technologies, materials, tooling and test equipment, as well as personnel skills have been demonstrated on systems and/or subsystems in a production-relevant environment • Cost, yield, and rate analyses have been performed to assess how prototype data compare with target objectives, and the program has in place appropriate risk reduction to achieve cost requirements or establish a new baseline, which should include design trades • Producibility considerations should have shaped system development plans, and the Industrial Base Capabilities assessment (in the Acquisition Strategy (AS) for Milestone B has confirmed the viability of the supplier base
3. Production Readiness Review. A production readiness review identifies the risks of transitioning from development to production. Manufacturing is a function of production; in order to transition to production without significant risk it is important that key processes have been considered and evaluated during the PRR, such as ensuring:	• The detailed system design is complete and stable to support low-rate production • Technologies are mature and proven in a production environment, and manufacturing and quality processes are capable, in control and ready for low-rate production • All materials, manpower, tooling, test equipment, and facilities have been proven on pilot lines and are available to meet the planned low-rate production schedule • Cost and yield and rate analyses are updated with pilot line results • Known producibility risks pose no significant challenges for low-rate production • Supplier qualification testing and first article inspections have been completed • Industrial base capabilities assessment for Milestone C has been completed and shows that the supply chain is adequate to support LRIP

Manufacturing Readiness Assessment Points	Considerations
4. FRP Decision Review. To support FRP, there should be no significant manufacturing process and reliability risks remaining. Manufacturing and production readiness results should be presented that provide objective evidence of manufacturing readiness. The results should include recommendations for mitigating any remaining low (acceptable) risk, based on assessment of manufacturing readiness for FRP which should include (but not be limited to):	• LRIP learning curves that include tested and applied continuous improvements • Meeting all systems engineering (SE)/design requirements • Evidence of a stable system design demonstrated through successful test and evaluation • Evidence that materials, parts, manpower, tooling, test equipment, and facilities are available to meet planned production rates • Evidence that manufacturing processes are capable, in control, and have achieved planned FRP objectives • Plans are in place for mitigating and monitoring production risks • LRIP cost targets data have been met; learning curves have been analyzed and used to develop the FRP cost model

4.3.18.19. Reliability and Maintainability Engineering

4.3.18.19. Reliability and Maintainability Engineering

The purpose of Reliability and Maintainability (R&M) engineering (Maintainability includes Built-In-Test (BIT)) is to influence system design in order to increase mission capability and availability, and decrease logistics burden and cost over a system's life cycle. Properly planned, R&M engineering reduces cost and schedule risks by preventing or identifying R&M deficiencies early in development. This early action results in increased acquisition efficiency and higher success rates during operational testing, and can even occur in the development process as early as the Engineering and Manufacturing Development (EMD) phase.

DoDI 5000.02 requires Major Defense Acquisition Program (MDAP) Program Managers to implement a comprehensive R&M engineering program as an integral part of the systems engineering (SE) process. The Systems Engineer should understand that R&M parameters have an impact on the system's performance, availability, logistics supportability, and total ownership cost. To ensure a successful R&M engineering program, the Systems Engineer should integrate the following activities across the program's engineering organization and processes:

- Providing adequate R&M staffing
- Ensuring R&M engineering is fully integrated into SE activities, Integrated Product Teams, and other stakeholder organizations (i.e., Logistics, Test, and ESOH)
- Ensuring specifications contain realistic quantitative R&M requirements traceable

to the Initial Capabilities Document (ICD)/Capability Development Document (CDD) /Capability Production Document (CPD)
- Ensuring that R&M engineering activities and deliverables in the Request for Proposal are appropriate for the program phase and product type
- Integrating R&M engineering activities and reliability growth planning curve(s) in the Systems Engineering Plan (SEP) at each milestone
- Planning verification methods for each R&M requirement
- Ensuring the verification methods for each R&M requirement are described in the TEMP, along with a reliability growth planning curve beginning at MS B
- Ensuring data from R&M analyses, demonstrations, and tests are properly used to influence life-cycle product support planning, availability assessments, cost estimating, and other related program analyses
- Identifying and tracking R&M risks and Technical Performance Measures.
- Assessing R&M status during program technical reviews
- Including consideration of R&M in all configuration changes and trade-off analyses

As part of the SE process, the R&M engineer should be responsible for the R&M activities by acquisition phase outlined in Table 4.3.18.19.T1.

Table 4.3.18.19.T1. R&M Activities by Acquisition Phase

Acquisition Phase	R&M Activities
Materiel Solution Analysis (MSA) Phase. During the Materiel Solution Analysis Phase, the R&M engineer, as part of the program SE team, should:	• Analyze conceptual design approaches and estimate the feasibility with respect to R&M ICD performance capabilities • Perform AoA trade-off studies among R&M, availability, and other system performance parameters to arrive at a preferred system alternative. The studies should be performed in conjunction with product support, cost, and design personnel, using the DoD RAM-C Rationale Report Manual • Prepare the Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report and attach it to the SEP • Translate ICD performance capabilities and draft CDD thresholds to R&M specification requirements based on system use conditions, mission profile, failure definitions, and utilization rates • Define contractor R&M engineering activities in the RFP and contract Statement of Work for the TD phase, which should include: a. Allocations b. Block diagrams and modeling c. Predictions d. Failure Mode, Effects, and Criticality Analysis (FMECA) e. Subsystem and system-level reliability growth planning activities f. R&M tests and demonstrations g. Failure Reporting, Analysis, and Corrective Action System (FRACAS)
Technology Development (TD) Phase. During the Technology Development phase, the R&M engineer, as part of the program SE team, should:	• Participate in trade studies during requirements analysis and architecture design • Review results of R&M engineering analyses, verification tests, design approach, availability assessments, and maintenance concept optimization to verify conformance to requirements, and to identify potential R&M problem areas • Contribute to integrated test planning to avoid duplication and afford a more complete utilization of all test data for R&M assessment. Comprehensive test planning should include subsystem reliability growth and maintainability and Built-In Test (BIT) demonstrations as appropriate • Verify that plans have been established for the selection and application criteria of parts, materials, and processes to limit reliability risks • Define contractor R&M engineering activities in the RFP and contract Statement of Work for the EMD phase, during which R&M quantitative requirements and verification methods are incorporated

Acquisition Phase	R&M Activities
Engineering and Manufacturing Development (EMD) Phase. During the EMD phase, the R&M engineer, as part of the program SE team, should:	• Perform evaluations to assess R&M status and problems • Ensure that the product baseline design and required testing can meet the R&M requirements • Ensure the final FMECA identifies failure modes, and their detection methods, that could result in personnel injury and/or mission loss, and ensure they are mitigated in the design • Ensure that the detailed R&M prediction to assess system potential to meet design requirements is complete • Verify through appropriate subsystem/equipment-level tests the readiness to enter system-level testing at or above the initial reliability established in the reliability growth-planning curve in both the SEP and the TEMP • Verify system conformance to specified R&M requirements through appropriate demonstration and test • Implement a FRACAS to ensure feedback of failure data during test and to apply and track corrective actions • Coordinate with the Chief Developmental Tester (T&E Lead) and Operational Test Agencies (OTA) to ensure that the program office and OTA data collection agree on R&M monitoring and failure definitions, and that R&M and BIT scoring processes are consistent in verification of requirements through all levels of testing • Define contractor R&M engineering activities in the RFP and contract Statement of Work (SOW) for the P&D phase to ensure adequate R&M engineering activities take place during P&D, and to ensure the RFP and contract SOW provide adequate consideration of R&M in re-procurements, spares, and repair parts • Verify that parts, materials, and processes meet system requirements through the use of a management plan detailing reliability risk considerations and evaluation strategies for the intended service life. Include flow of requirements to subcontractors and suppliers. See MIL-STD-1546, Parts, Materials, and Processes Control Program for Space and Launch Vehicles, and MIL-STD-1547, Electronic Parts, Materials, and Processes for Space and Launch Vehicles

Acquisition Phase	R&M Activities
Production and Deployment (P&D) Phase. During the P&D phase, the R&M engineer, as part of the programs SE team should:	• Verify initial production control of R&M degradation factors by test and inspection, production data analysis, and supplemental tests • Verify R&M characteristics, maintenance concept, repair policies, Government technical evaluation, and maintenance procedures by T&E • Identify R&M and production-related BIT improvement opportunities via FRACAS and field data assessment • Review Engineering Change Proposals (ECP), operational mission/deployment changes, and variations for impact on R&M • Update R&M predictions and FMECAs based on field results and apply them to the models previously developed to assess impacts on spares, manpower, missions, and availability • Verify that parts, materials, and processes management requirements for limiting reliability risk and "lessons learned" are utilized during all design change efforts including change proposals, variations, substitutions, product improvement efforts, or any other hardware change effort
Operations and Support (O&S) Phase. During the O&S phase, the R&M engineer, as part of the program SE team should:	• Assess operational data to determine the adequacy of R&M and BIT characteristics performance, maintenance features and procedures, and provisioning plans • Identify problem areas for correction through ongoing closed-loop FRACAS and field data assessment • Monitor availability rates and respond to negative trends and data anomalies

[4.3.18.20. Spectrum Management](#)

4.3.18.20. Spectrum Management

Warfighters use spectrum-dependent systems for communications, sensors (i.e., radar), navigation beacons, jammers, homing devices, anti-Improvised Explosive Devices (IED), and other purposes. Often emitters are in close physical proximity to each other and to civilian devices that should not be disrupted by military signals. Spectrum-dependent system developers should be aware of the enemy electronic order of battle and countermeasures, and plan accordingly. Devices (including commercial items) that do not account for countermeasures may have vulnerabilities in hostile environments.

Spectrum management requirements are needed for all spectrum-dependent systems. Any system that uses an antenna or a platform that mounts such systems is a spectrum-dependent system. If a platform obtains a spectrum-dependent system as Government-furnished equipment (GFE), the platform Program Manager is responsible for ensuring that the GFE Program Manager has obtained the needed permissions. Both programs are required to submit a Spectrum Supportability Risk Assessment (SSRA). The platform SSRA can reference the GFE SSRA, but may have to expand upon it regarding host nation features or other information not contained in the GFE-

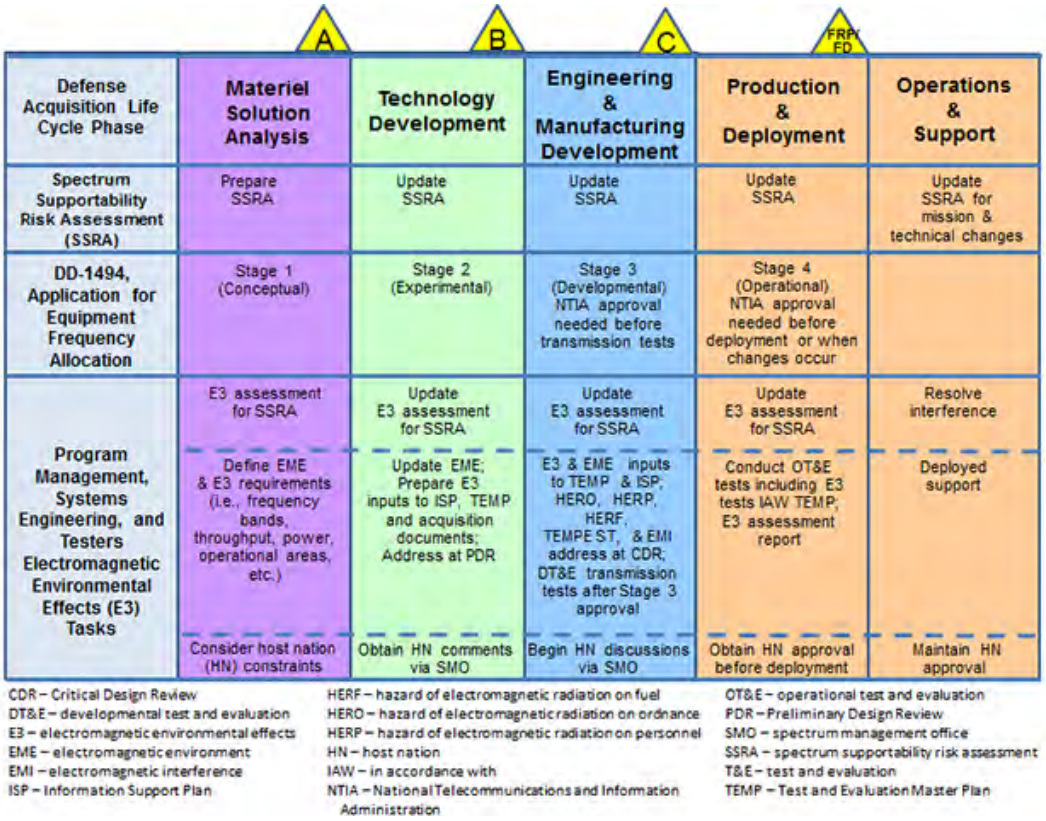
level SSRA. The Systems Engineer should be aware of the worldwide rules for spectrum management and the need to obtain host nation permission for each transmitter and frequency assignment.

Program Managers need to ensure that spectrum access is adequate and that it is granted in the Continental United States (CONUS) and wherever else the equipment is deployed. The Pre-Milestone A Analysis of Alternatives (AoA) should address spectrum needs as part of concept formulation. Both the SSRA and DD-1494 are required for each milestone (see DoDI 4650.01). The SSRA is used within the DoD as the basis for assessing the feasibility of building and fielding equipment that operate within assigned frequency bands and to identify potential de-confliction situations. The DD-1494, Application for Equipment Frequency Allocation, has four stages, which reflect the increasing maturity of available spectrum information during development. The DD-1494 form is submitted to National Telecommunications and Information Administration (NTIA) for approval of spectrum allocation without which emitters cannot operate within CONUS, and to the International Telecommunications Union (ITU) for satellites. The NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook) chapter 3 addresses international treaty aspects of the spectrum and chapter 4 addresses frequency allocations.

The Systems Engineer has a lead role in defining spectrum needs, throughput and power requirements, and other attributes of the signals in space (outside the antenna - not in the transmission device) and the antenna characteristics and platform mounting details, as well as the safety aspects of emitters with regard to the Hazards of Electromagnetic Radiation to Ordnance (HERO), Personnel (HERP), and Fuel (HERF). The SE should be aware that portions of the spectrum previously assigned to DoD or other Federal users are being sold for commercial use. Thus, previously approved DD-1494 can be revoked, requiring modifications to designs, and even to fielded equipment. Similarly, host nations can alter prior agreements as commercial applications encroach upon previously available spectrum.

Each nation reserves the right to control emitters operating within its territory, thus host nation agreements are essential in support of deployment. Program Managers and Systems Engineers of platforms that mount multiple emitters and receivers need to obtain spectrum access for each emitter and ensure that those emitters and receivers do not produce mutual interference, or interact with ordnance (see DoDD 3222.3, MIL-STD-461, MIL STD-464, and MIL-HDBK-235-1, 237,and 240A, and "Joint Services Guide for Development of a Spectrum Supportability Risk Assessment"). The Defense Information Systems Agency (DISA), Defense Spectrum Organization provides spectrum support and planning for DoD and can be reached at http://www.disa.mil/Services/Spectrum. See Figure 4.3.18.20.F1 for spectrum activities by acquisition phase. This figure summarizes the requirements of DoDI 4650.01.

Figure 4.3.18.20.F1. Spectrum-Related Activities by Life-Cycle Phase



4.3.18.21. Standardization

4.3.18.21. Standardization

Standardization supports the achievement of commonality and interoperability of parts and processes with United States forces and our allies, promote safety, provide for life-cycle sustainment, and allow for rapid, cost-effective technology insertion through use of standard interfaces and open systems. Standardization is an enabling tool to provide the warfighter with systems and equipment that are interoperable, reliable, sustainable and affordable. Standardization plays a key role in defining systems engineering (SE) best practices and processes.

The Program Manager balances the decision to use standardized agreements, practices, products, parts, processes, interfaces, and methods with required capabilities, operational environment, technology feasibility and growth, and cost-effectiveness.

DoD 4120.24-M, Chapter 3, Standardization in the Acquisition Process, provides policies on when to standardize, how to document standardization decisions, and a discussion of the tailoring of standardization documents through rewriting, extracting, or

eliminating requirements.

Parts management is a standardization design strategy available to Program Managers. Benefits of parts standardization include:

- Reducing the number of unique or specialized parts used in a system (or across systems)
- Reducing the logistics footprint
- Lowering life-cycle costs

In addition, parts management can enhance the reliability of the system and mitigate part obsolescence due to Diminishing Manufacturing Sources and Material Shortages (DMSMS). MIL-STD-3018, Parts Management, dictates that program offices should apply standardization processes to:

- Improve parts commonality
- Reduce total ownership costs
- Reduce proliferation of parts
- Promote the use of parts with acceptable performance, quality, and reliability

The Systems Engineer is responsible for:

- Implementing parts management contractual requirements
- Approving contractor submitted plans
- Ensuring parts management objectives are met

Additional guidance on parts management may be found in SD-19, Parts Management Guide.

4.3.18.22. Supportability

4.3.18.22. Supportability

Supportability refers to the inherent characteristics of the system and the enabling system elements that allow effective and efficient sustainment (including maintenance and other support functions) throughout the system's life cycle. By addressing supportability as part of the system design, the Program Manager through the Systems Engineer and Product Support Manager ensures the system reaches Initial Operational Capability (IOC) with the required enabling system elements in place. The benefits to the program are:

- Cost savings
- Fielding of a more affordable logistics infrastructure
- Improving Materiel and Operational Availability
- Reducing footprint

Early consideration of supportability needs during Requirements Analysis, Architecture Design, and Implementation processes are critical to ensure the delivered capability is operationally suitable, effective, sustainable, and affordable. The system baseline should incorporate inherent supportability characteristics and should include the design of the enabling support infrastructure. Details can be found in DAG Chapter 5 Life-Cycle Logistics, but typical product support infrastructure considerations are listed in Table 4.3.18.22.T1.

Table 4.3.18.22.T1. Product Support Infrastructure Considerations

Infrastructure Elements	Typical Considerations
Manpower and Personnel	Specifically support personnel for installation, checkout, sustaining support and maintenance
Training and Training Support	For the system operators and for system maintenance personnel
Supply Support	Including repairable and non-repairable spares, consumables, and special supplies
Support Equipment	Including tools, condition and state monitoring, diagnostic and checkout, special test and calibration equipment
Computer Resources	Operating systems and software supporting logistics functions and associated infrastructure
Packaging, Handling, Storage, and Transportation	Special provisions, containers and transportation needs
Facilities and Infrastructure	Including facilities to support logistics and sustainment actions at all levels
Technical Data	Including system installation and checkout procedures; operating and maintenance instructions and records; alteration and modification instructions, etc.

The Program Manager is responsible for approving life-cycle cost trades throughout the acquisition process. It is critical that the design of a program focused on life-cycle supportability involve the logisticians alongside the end users early in the Stakeholder Requirements Definition process to support the Reliability Centered Maintenance (RCM) analysis and to develop the overall performance based product support strategy. Reference DoD 4151.22-M, Conditioned Based Maintenance Plus (CBM+), an important support concept and a specific initiative, can be useful to perform maintenance based on evidence of need as provided by RCM analysis and other enabling processes and technologies.

RCM analysis is a systematic approach analyzing the functions and potential failures to identify and define preventive or scheduled maintenance tasks for an equipment end item. Tasks may be preventive, predictive, or proactive in nature. RCM results provide operational availability with an acceptable level of risk in an efficient and cost-effective

manner.

Additionally, the Product Support Manager and Systems Engineer should ensure that supportability activities are documented in the Systems Engineering Plan (SEP) and the Life-Cycle Support Plan (LCSP), and that the supportability design requirements are documented in the program's functional baseline.

The Systems Engineer working with the Product Support Manager should identify and mitigate the supportability life-cycle cost drivers to ensure a system is affordable across the life cycle. The streamlined LCSP outline calls out specific phase and milestone expectations. These expectations include determining supportability design alternatives along with their associated cost and establishing both the Operational Availability (A_O) and Materiel Availability (A_M) drivers. The derived supportability requirements should be based on trade studies along with their associated cost and operational and materiel availability drivers (see DAG Chapter 5 Life-Cycle Logistics). The Cost-Benefit Analyses, jointly conducted by the Systems Engineer and Product Support Manager in the supportability analysis, provides insight into supportability drivers and includes the impact of resources on readiness supported by engineering analyses required for product support (i.e., FMECA, predictions, and diagnostics architecture).

Supportability analysis is an iterative activity conducted during the system's development, and is used by the Program Manager and Product Support Manager to define the system's support and document the support in the program's LCSP. Supportability analysis begins in stakeholder requirements definition, as part of the Analysis of Alternatives (AoA), and continues through the design, test and evaluation, production and deployment activities/phases of the system. The supportability analysis and the resultant product support package mature in parallel with the maturity and evolution of the design, and should be documented in an integrated data/decision environment.

4.3.18.23. Survivability and Susceptibility

4.3.18.23. Survivability and Susceptibility

A system with a balanced survivability and susceptibility approach ensures operational crew and personnel safety while satisfying mission effectiveness and operational readiness requirements.

Survivability is the capability of a system and its crew to avoid or withstand a hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Susceptibility is the degree to which a device, piece of equipment, or weapon system is open to effective attack as a result of one or more inherent weaknesses. Man-made and natural environmental conditions, described in MIL-STD-810 (sand, vibration, shock, immersion, fog, etc.), and electromagnetic environment, described in MIL-STD-461/464, also should be considered in system design.

Susceptibility is a function of operational tactics, countermeasures, probability of an enemy threat, etc. Susceptibility is considered a subset of survivability. Vulnerability is the characteristics of a system that cause it to suffer a definite degradation (loss or reduction of capability to perform the designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (man-made) or natural (e.g., lightning, solar storms) hostile environment. Vulnerability is also considered a subset of survivability.

Design and testing ensure that the system and crew can withstand man-made hostile environments without the crew suffering acute chronic illness, disability, or death. The Program Manager, supported by the Systems Engineer, should fully assess system and crew survivability against all anticipated threats, at all levels of conflict, throughout the system life cycle. The goal of survivability and susceptibility is to:

- Provide mission assurance while maximizing warfighter safety (or minimizing their exposure to threats)
- Incorporate balanced survivability, with consideration to the use of signature reduction with countermeasures
- Incorporate susceptibility reduction features that prevent or reduce engagement of threat weapons
- Provide mission planning and dynamic situational awareness features

The mandatory Survivability Key Performance Parameter (KPP) is applicable to all capability documents for manned systems and may be applicable to unmanned systems. The intent of the Survivability KPP includes:

- Reducing a system's likelihood of being engaged by hostile fire, through attributes such as speed, maneuverability, detectability, and countermeasures
- Reducing the system's vulnerability if hit by hostile fire, through attributes such as armor and redundancy of critical components
- Allowing the system to survive and continue to operate in a chemical, biological, radiological, and nuclear (CBRN) environment, if required

If the system or program has been designated by the Director, Operational Test and Evaluation (DOT&E), for live-fire test and evaluation (LFT&E) oversight, the Program Manager should integrate test and evaluation (T&E) to address crew survivability issues into the LFT&E program supporting the Secretary of Defense LFT&E Report to Congress.

If the system or program has been designated a CBRN mission-critical system, the Program Manager should address CBRN survivability, in accordance with DoDI 3150.09, The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy. The Program Manager should ensure that progress toward CBRN survivability requirements is documented in the applicable Service CBRN mission-critical report.

Unless waived by the Milestone Decision Authority (MDA), mission-critical systems,

including crew, regardless of acquisition category, should be survivable to the threat levels anticipated in their projected operating environment as portrayed in their platform-specific System Threat Assessment Report (STAR) (see DoDI 5000.02, Enclosures 6 and 8), or in lieu of a STAR, the appropriate capstone threat document.

The Systems Engineer should describe in the Systems Engineering Plan:

- How the design incorporates susceptibility and vulnerability reduction and CBRN survivability requirements
- How progress toward these are tracked over the acquisition life cycle

Additional techniques include rapid reconstruction (reparability) to maximize wartime availability and sortie rates and incorporating damage tolerance in the system design.

4.3.18.24. System Security Engineering

4.3.18.24. System Security Engineering

System Security Engineering (SSE) activities allow for identification and incorporation of security design and process requirements into risk identification and management in the requirements trade space.

SSE is the integrating process for mitigating and managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, battlefield loss, and unauthorized or inadvertent disclosure throughout the acquisition life cycle. The SSE process captures SSE analysis in the system requirements and design documents, and SSE verification in the test plans, procedures, and results documents. The Program Protection Plan (see DAG Chapter 13 Program Protection) documents the comprehensive approach to system security engineering analysis and the associated results.

SSE is the functional discipline within systems engineering that ensures security requirements are included in the engineering analysis with the results being captured in the Program Protection Plan (PPP), provided at each Systems Engineering (SE) technical review (SETR) event (see DAG Chapter 13 Program Protection) and incorporated into the SETR-related SE requirements and the functional, allocated, and product baselines. The PPP is approved by the Milestone Decision Authority (MDA) at each milestone decision review and at the Full-Rate Production/Full-Deployment (FRP/FD) decision, with an approvable draft at the pre-Engineering and Manufacturing Development (EMD) review. The analysis should be used to update the SE baselines prior to each SETR and key knowledge point throughout the life cycle.

The Program Manager is responsible for developing a PPP that ensures the program complies with program protection policy and system requirements. The Systems Engineer and/or System Security Engineer is responsible for ensuring a balanced set of security requirements, designs, testing, and risk management are incorporated and

addressed in the their respective trade spaces.

The Systems Engineer and/or System Security Engineer is responsible for facilitating cross-discipline system security working groups and is typically responsible for leading the SSE analysis necessary for development of the PPP. The cross-discipline interactions reach beyond the SSE community to the test and logistics communities. The Test Lead is responsible for incorporating sufficient system security test requirements into the Test and Evaluation Strategy (TES) and Test and Evaluation Master Plan (TEMP). The logistics community is responsible for continuing the protections and risk management activities initiated in acquisition throughout the Operations and Support (O&S) phase.

SSE processes inform the development and release of each request for proposal (RFP) (see DAG Chapter 13 Program Protection) by incorporating SSE process requirements into the Statement of Work (SOW) and the system security requirements into the Requests for Proposal (RFP) requirements document. Contractor responsibilities include developing plans to ensure that the system security protections are implemented in the development environments, system designs, and supply chains. The early and frequent consideration of SSE principles reduces rework and expense resulting from late-to-need security requirements (e.g., anti-tamper, exportability features, supply chain risk management, secure design, defense-in-depth, and information assurance implementation).

4.3.19. Tools, Techniques, and Lessons Learned

4.3.19. Tools, Techniques, and Lessons Learned

Systems engineering (SE) tools support the performance of activities and the development of products. SE techniques use tools and methods to complete specific tasks. SE tools and techniques support the Program Manager and Systems Engineer in performing and managing the SE activities and processes to improve productivity and system cost, schedule, capabilities, and adaptability. The program should begin applying SE tools and techniques during the early stages of program definition to improve efficiency and traceability and to provide a technical framework for managing the weapon system development.

Collaboration tools allow the program office and developer to exchange data and analyses easily. Analytical tools and techniques also can assist in the development and validation of system designs. It is critical that the Systems Engineer understand the constraints and limitations of any particular analysis tool or technique, and apply this understanding when making assessments or recommendations based on its output.

Before selecting and implementing a SE tool or technique, the Systems Engineer should consider:

- Needs and constraints of the program (e.g., complexity, size, and funding)

- Applicability to required tasks and desired products
- Computer system requirements, including peripheral equipment
- Licensing and maintenance costs
- Technical data management (see DAG section 4.3.8. Technical Data Management Process)
- Integration with other SE tools in use within the program, by the developer, and by externally interfacing programs
- Cost to train the user to apply the tool or technique
- Number and level of expertise of Government and contractor staff (both users of the tool and users of the tool outputs)
- Feasibility of implementing the tool or technique throughout the acquisition life cycle

Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs should clearly identify tools in use, define tool interfaces when the Government and developer select different tools to use for the same purpose, and describe how the tools support the program's SE approach. This information is documented in the program's Systems Engineering Plan (SEP) Table 4.7-1 Engineering Tools.

Table 4.3.19.T1 lists general capabilities and features of SE tools and the SE processes they might support.

Table 4.3.19.T1. SE Process-Related Tools

SE Process	Tool Capabilities / Features
Technical Planning	• Assists in planning and scheduling activities • Assists in resource planning, tracking, and allocation • Facilitates cost estimation
Decision Analysis	• Assists in trade-off analysis • Provides optimization and sensitivity analysis capability • Assists in recording, tracking, evaluating, and reporting decision outcomes
Technical Assessment	• Assists in tracking, measuring, and assessing metrics • Assists in metric collection
Requirements Management	• Provides requirements bidirectional traceability capability • Provides requirements flow-down capability • Tracks requirements changes
Risk Management	• Assists in risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking

SE Process	Tool Capabilities / Features
Configuration Management	• Assists in the identification of configuration items • Assists in baseline/version control of all configuration items • Assists in ensuring configuration baselines and changes are identified, recorded, evaluated, approved, incorporated and verified
Technical Data Management	• Assists in identification of data requirements • Assists in storage, maintenance, control, use, and exchange of data • Assists in document preparation, update, and analysis
Interface Management	• Assists in capturing system internal and external interfaces and their requirement specifications • Assists in assessing compliance of interfaces among system elements of the system or systems of systems • Produces a view of interface connectivity
Stakeholder Requirements Definition	• Assists in capturing and identifying stakeholder requirements • Assists in analyzing and maintaining stakeholder requirements
Requirements Analysis	• Assists in requirements definition and decomposition • Interfaces with architecting tools • Supports Requirements Validation
Architecture Design	• Assists in development of functional and physical architectures • Provides traceability among architectural components • Supports multiple views
Implementation	• Assists in development of the system design, prototypes, and alternate solutions • Assists in realization of the system, system elements, and enabling system elements
Integration	• Assists in integration-planning activities • Assists in assembling lower-level system elements into successively higher-level system elements • Provides analysis and simulation capability
Verification	• Assists in determining the system and system elements performance as designed through demonstration, examination, analysis, and test
Validation	• Assists in determining, the effectiveness, suitability and survivability of the system in meeting end-user needs

SE Process	Tool Capabilities / Features
Transition	• Assists in planning and executing delivery and deploying of the system to the end user for use in operational environment

4.3.19.1. Modeling and Simulation

4.3.19.1. Modeling and Simulation

Models and simulations are SE tools used by multiple functional area disciplines during all life-cycle phases. Modeling is essential to aid in understanding complex systems and system interdependencies, and to communicate among team members and stakeholders. Simulation provides a means to explore concepts, system characteristics, and alternatives; open up the trade space; facilitate informed decisions and assess overall system performance.

Modeling and simulation provide:

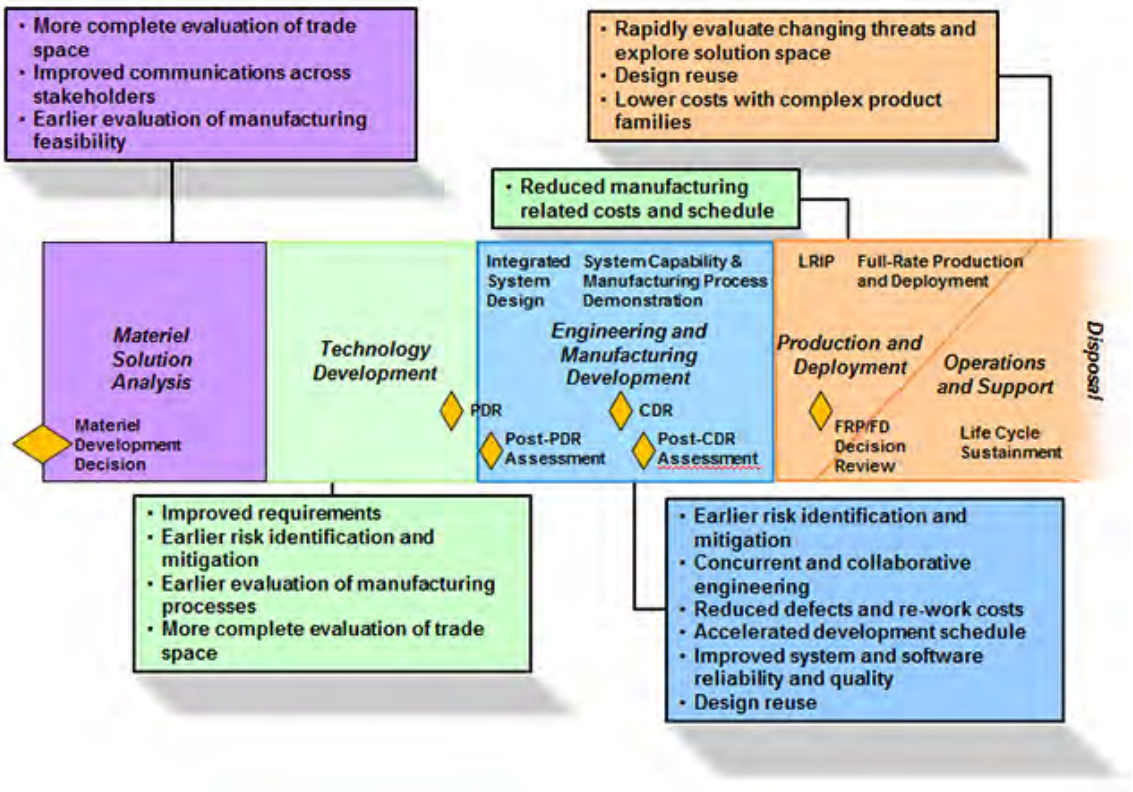
- Insight into program cost, schedule, performance, and supportability risk
- Understanding of capabilities and the requirements set
- Data to inform program and technical decisions
- Efficient communication and shared understanding among stakeholders about relationships between system requirements and the system being developed, through precise engineering artifacts and traceability of designs to requirements
- Better analysis and understanding of system designs (including system elements and enabling system elements), therefore providing a greater understanding of the reasons for defects and failures at all levels
- Greater efficiencies in design and manufacturing by reducing the time and cost of iterative build/test/fix cycles
- Timely understanding of program impacts of proposed changes

The DoD Acquisition Modeling and Simulation Working Group Systems Engineering Modeling, Simulation, and Analysis Fundamentals (located on the DASD(SE) website) recommends that all programs identify and maintain "a collection of related information, representing all necessary viewpoints on the design, and capturing all relevant system interactions." The Program Manager and Systems Engineer should consider directing the use of such a collection when planning for the development, use, and application of models, simulations, and analyses on their program. This collected information can help drive consistency and integration among SE and analytical tools, and provide the program with a capability to assess potential design changes as well as system upgrades throughout the life cycle. Figure 4.3.19.1.F1. shows some benefits of using modeling and simulation throughout the acquisition life cycle. This figure is adapted from a 2010 National Defense Industrial Association (NDIA) Systems Engineering

Division "Model-Based Engineering (MBE)" study and is used with permission.

Modeling and simulation should take advantage of opportunities for reuse (see DoD Modeling and Simulation Catalog). Models and simulations developed in early acquisition phases may be repurposed for other activities during later phases (e.g., engineering models can be used in training simulations).

Figure 4.3.19.1.F1. Benefits of Using Modeling and Simulation throughout the Acquisition Life Cycle



SE requires use of models and simulations from many disciplines and across a hierarchy of perspectives that range from an engineering/technical level up to the campaign/strategic level in order to effectively analyze requirements, design, cost, schedule, performance, and risk. These models and simulations often exist, but sometimes need to be newly developed, which can be costly. An option for new development is to consider federating existing models and simulations, using any of various interoperability standards, in order to create needed capability. Program Managers and Systems Engineers should consider how to leverage M&S interoperability as they plan for M&S use throughout a program's life cycle. Modeling and simulation is also used to support developmental test and evaluation (DT&E) and operational test and evaluation (OT&E).

Roles, Responsibilities, and Activities

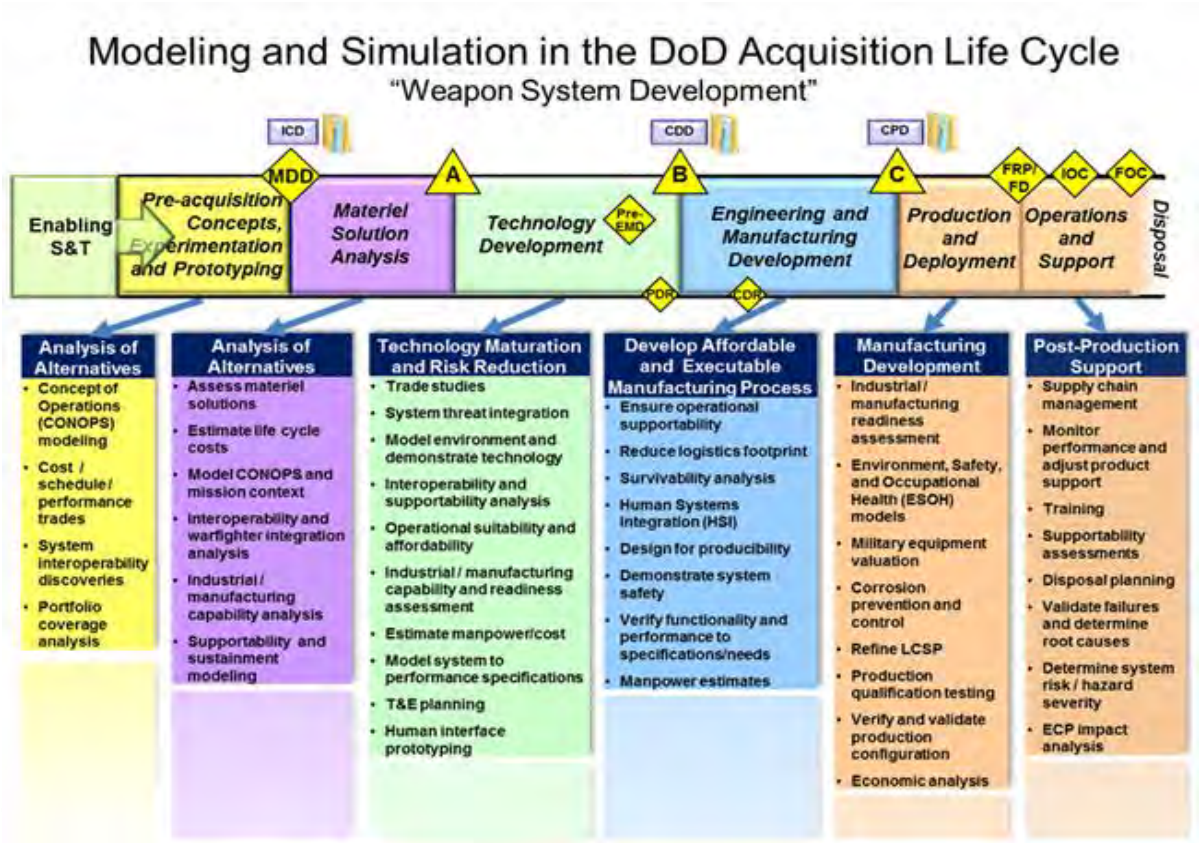
To make effective and appropriate use of modeling and simulation, the Program Manager and Systems Engineer should ensure that planned modeling and simulation activities are:

- Complete and comprehensive, including all efforts anticipated throughout the life cycle, to include planning, development, and acceptance through proper verification, validation, and accreditation (VV&A); (see DAG Chapter 9 Test and Evaluation)
- Reflected in the program's technical planning (Work Breakdown Structure (WBS), schedules, budgets, Systems Engineering Plan (SEP), and other program documentation; see DAG section 4.3.2. Technical Planning Process)
- Appropriately resourced, including a properly skilled workforce

The Program Manager and Systems Engineer should establish and maintain a repository of all relevant modeling and simulation data products that describe what the system is and does. This repository also should contain descriptive system information that could be used to feed other modeling and simulation efforts. They should ensure that all modeling and simulation products are established, maintained, controlled, and resourced to achieve an efficient and effective acquisition program.

Figure 4.3.19.1.F2 shows some applications of modeling, simulation, and analysis throughout the life cycle.

Figure 4.3.19.1.F2. Various Applications of Modeling and Simulation



The Program Manager and Systems Engineer should ensure that the program's modeling and simulation activities are coordinated, managed, and controlled such that products are consistent with the system and architecture design at all levels. Modeling and simulation planning should be part of the overall program plan; and should be integrated with it. The program may choose to integrate the modeling and simulation planning details into the program plan or create a separate modeling and simulation planning document. If the documents are separate, the program must ensure the modeling and simulation planning is kept up to date as the program plan adjusts. Program Managers should follow their local modeling and simulation organizations standards for planning managing and controlling such activities.

Models and simulations should be:

- Developed and matured through the life of the program
- Properly managed and controlled as part of the program's technical baseline
- Developed and documented, to include metadata (see Modeling and Simulation Community of Interest Discovery Metadata Specification (MSC-DMS)) and open systems standards, to maximize opportunity for reuse and repurposing (both within the program and in support of other acquisition efforts)
- Included as part of the technical data package to be transitioned into the next phase of the life cycle or into other efforts

Modeling and modeling artifacts should be evident in the contents of the required program technical reviews and in the baselined technical data needed to support major program reviews and program decisions.

4.3.19.2. Sustainability Analysis

4.3.19.2. Sustainability Analysis

The sustainability analysis, using a Life Cycle Assessment (LCA) method, is a tool to assist the Systems Engineer in designing more sustainable systems - those which use fewer resources over the life cycle, have fewer impacts on human health and the environment, and thus have a lower total ownership cost (TOC). The Program Manager should make sustainability considerations an integral part of both a robust trade space analysis and a comprehensive supportability analysis. These sustainability analyses can help reduce system TOC by uncovering previously hidden or ignored life-cycle costs, leading to more informed decisions earlier in the acquisition life cycle. They can also help make systems more affordable and improve the accuracy of life-cycle cost estimates.

Large military systems and platforms can have a life cycle of 30 years or more. To meet evolving mission needs far into the future, the system design should incorporate long-term sustainability considerations in order to reduce life-cycle costs. Without a full understanding of life-cycle impacts, significant costs may be unintentionally inserted

during acquisition and later exposed by the logistics and operational communities.

"Sustainability" differs from "sustainment" in that it relates to the use of resources, and the associated impacts and costs over the system's life cycle. In contrast, sustainment is more concerned with the end user's ability to operate and maintain a system once it is in inventory and deployed. Both aspects need to be addressed in the design process.

Executive Order (E.O.) 13514, "Federal Leadership in Environmental, Energy and Economic Performance" dated October 5, 2009, establishes an integrated Federal Government strategy for sustainability. As required by the E.O., DoD generated a Strategic Sustainability Performance Plan (SSPP) that is updated annually. The SSPP identifies DoD goals for efficiency and reductions in energy, water, solid waste, and use of hazardous chemicals and materials.

A sustainability analysis examines and compares various system attributes associated with energy, water, solid waste, chemicals, materials, and land use. Outputs include decision diagrams (i.e., Kivat/spider-web diagrams) that compare alternatives according to their relative sustainability indicators and related costs. These diagrams can be used to develop system life-cycle cost estimates.

A sustainability analysis can support numerous acquisition activities, including:

- Analysis of Alternatives to compare conceptual alternatives
- Trade space analysis to compare how sustainability attributes (e.g., chemical or material choices, water or solid waste) affect life-cycle cost, TOC, performance, human health, and the environment
- Business Case Analysis using the LCA method to include sustainability as one of the elements in the analysis
- Preliminary design to select the most sustainable system that meets performance requirements and end-user needs
- Supportability analysis to help ensure the use of resources throughout the life cycle is considered and the system is supportable
- Detailed design to select the most sustainable components

The Streamlined Life Cycle Assessment Process for Sustainability in DoD Acquisitions is specifically for use in the DoD acquisition process. It combines LCA with multi-attribute analysis. It integrates a number of trade space and design considerations and provides a procedure to compare conceptual or detailed design alternatives. The streamlined LCA can be applied in a qualitative mode even when data are lacking, and can be accomplished with minimal resources. It is intended to ensure consideration of important downstream impacts and costs in trade-off and design decisions. The method is consistent, without duplication, with other considerations such as operational energy, supportability, and environment, safety, and occupational health (ESOH).

4.3.19.3. Value Engineering

4.3.19.3. Value Engineering

Value Engineering (VE) is an organized, systematic technique that analyzes the functions of systems, equipment, facilities, services, and supplies to ensure they achieve their essential functions at the lowest life-cycle cost consistent with required performance, reliability, quality, and safety. In today's environment, many systems remain in inventory for a longer time than initially envisioned. Budgetary realities (i.e., affordability) often dictate extending a system's operational life through major modifications or upgrades (e.g., block changes or preplanned product improvements), rather than acquiring a new system. Therefore, opportunities for large VE savings extend well into sustainment.

A VE analysis is a type of process improvement. Key steps include:

- Scoping the issue, improvement targets, and evaluation factors
- Identifying specific areas/functions for evaluation
- Collecting and analyzing data
- Exploring alternative approaches
- Developing and presenting specific recommendations
- Implementing directed changes

By following this process, the Program Manager can analyze the functions of an item or process to determine best value, identify and reduce unnecessary costs, increase productivity, enhance quality, and improve system and program performance. VE supports most aspects of the Better Buying Power initiative:

- Affordability and cost growth: VE critically compares the cost and value of every requirement to focus the program on providing only necessary functions at a minimum overall cost. This represents a systematic approach for attaining return on investment.
- Promote competition: Program Managers can employ VE to identify technical data describing required functions of system elements, enabling multiple suppliers to bid.
- Provide incentives for productivity and innovation: VE provides industry with an incentive to reduce costs; the developer receives a share in the savings if the Government implements a VE change.

Federal Acquisition Regulation (FAR) Parts 48 and 52 mandate inclusion of a VE clause in many Government contracts. This clause allows the developer to receive a share of the cost savings generated from Value Engineering Change Proposals (VECP). (See SD-24 Value Engineering: A Guidebook of Best Practices and Tools for additional details.)

Roles, Responsibilities, and Activities

Program Managers and Systems Engineers should encourage both in-house VE and VECP-based studies and trade-offs on every activity or contract with a value exceeding the simplified acquisition threshold. While a common misconception is that VE applies only to production, successful introduction of VE may occur at any point in the life cycle. The most opportune time to apply VE is early in the life cycle, before production begins, before preparation of field or technical manuals, and before finalizing logistics support plans.

Program Managers and Systems Engineers should consider applying VE principles throughout their program. They should investigate VE saving for:

- Hardware, software, or human components
- Development, production, test, or manufacturing
- Specifications and standards
- Facilities design and construction
- Contract requirements
- Other program documentation

The following examples are potential areas in which the application of VE and VECP may provide a benefit:

- The Analysis of Alternatives and associated cost-effectiveness studies can use VE to evaluate functions and essential requirements, and develop possible alternatives offering improved value
- VE analyses can support the process for transitioning technology from the technology base into program-specific preliminary design efforts; the Program Manager and Systems Engineer can compare the function, cost, and worth of each requirement and the derived specifications
- As part of the development and refinement of the functional and allocated baselines, VE can help:
    - Identify the necessary top-level functions for each of the missions considered
    - Identify technical approaches to the missions
    - Identify necessary lower-level functions for each technical approach
    - Evaluate each function in terms of technical feasibility
    - Estimate the cost of various functions
- VE can contribute to SE activities during production and deployment by devising alternative means for achieving required functions and developing alternative designs to meet functional needs
- VE evaluations can improve manufacturing processes, methods, and materials
- After fielding, VE can examine advances in technology or changes in user requirements to assess potential savings

Additional resources available to the Program Manager and Systems Engineer to learn more about VE as a tool to reduce costs include:

- Defense Acquisition University (DAU) Continuous Learning Module (click on CLE001)
- **DoD VE information** as provided by the Institute for Defense Analyses
- SD-24, Value Engineering: A Guidebook of Best Practices and Tools
- Office of Management and Budget Circular A-131

4.3.19.4. Lessons Learned, Best Practices, Case Studies

4.3.19.4. Lessons Learned, Best Practices, Case Studies

Most programs represent a new combination of existing capabilities or the insertion of incremental advances in technology. By reviewing the successes, failures, problems, and solutions of similar programs, Program Managers and Systems Engineers can gain insights into risks, uncertainties, and opportunities that their programs may encounter.

Lessons learned and case studies generally describe areas of risk, pitfalls encountered in programs, and strategies employed to mitigate or fix problems when they arose. Best practices are proven techniques and strategies that can avoid common problems and improve quality, cost, or both.

Best practices and lessons learned are applicable to all aspects of a program - technical, managerial, and programmatic - and at any point in the acquisition life cycle. However, they are not universal or "one-size-fits-all" solutions. The greatest benefits occur when Program Managers and Systems Engineers judiciously select successful practices or strategies from analogous programs/systems and tailor them to meet current program needs.

Design, build, test, and certification standards are an implementation of lessons learned over time. Program Managers and Systems Engineers should be aware that Standards are not ad hoc requirements developed by a single engineer or program office. They result from years of engineering, manufacturing, or sustainment knowledge that eventually migrates to a standard that should be followed.

Program Managers and Systems Engineers should be aware of available resources, and they should take advantage of prior experience and knowledge gained when appropriate. Various organizations in DoD, industry, and academia produce and maintain online repositories of lessons learned, best practices, and case studies. These resources can serve as a starting point for Program Managers and Systems Engineers to search for and find relevant data that can be applied to their current program. Knowledge sharing resources include, but are not limited to:

- Service lessons learned repositories (including Service safety centers)
- Government Accountability Office reports

- DoD Systems Engineering community of practice websites
- Other Departments and Agencies such as National Aeronautics and Space Administration (NASA) or Department of Energy (DoE)
- Professional organizations such as the International Council on Systems Engineering (INCOSE) or the Institute of Electrical and Electronics Engineers (IEEE)
- Industry organizations such as National Defense Industrial Association (NDIA) or Aerospace Industries Association (AIA)

Program Managers and Systems Engineers are encouraged to research current analogous programs, not just past programs, that may be experiencing similar challenges and have not yet formally documented what they have learned. The Program Manager and Systems Engineer should ensure that the program establishes and utilizes a robust process to identify and document best practices and lessons learned, to aid both internal activities and other programs. This process should focus on ensuring accurate and timely documentation of all relevant information, and the Systems Engineer should monitor its use and products throughout the life cycle. Each best practice or lesson learned that is developed throughout the program execution should include enough contextual information about the program and surrounding circumstances so that future practitioners find it useful. Program Managers and Systems Engineers should consider using this data as a form of process improvement feedback, or as evidence for proposing policy and guidance changes.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 5 -- Life-Cycle Logistics

5.0. Overview

DoD Directive 5000.01 requires Program Managers to:

"develop and implement performance-based logistics strategies that optimize total system availability while minimizing cost and logistics footprint."

Within the Defense Acquisition Management System, DoDD 5000.01 requires that:

"Planning for Operation and Support and the estimation of total ownership costs shall begin as early as possible. Supportability, a key component of performance, shall be considered throughout the system life cycle."

5.0.1. Purpose

This chapter provides the associated guidance the Program Manager (PM), Product Support Manager (PSM), and Life-Cycle Logisticians can use in influencing the design and providing effective, timely product support capability to achieve the systems materiel readiness and sustain operational capability. Emphasis is placed on integrating life-cycle management principles by using performance-based life-cycle product support strategies to provide effective support. This synchronized with the systems engineering process results in affordable materiel readiness at an optimal life-cycle cost (LCC) by reducing the frequency, duration, and related costs of availability degrader events to

reduce manpower and logistics footprint. An executive summary of key chapter principles is provided below.

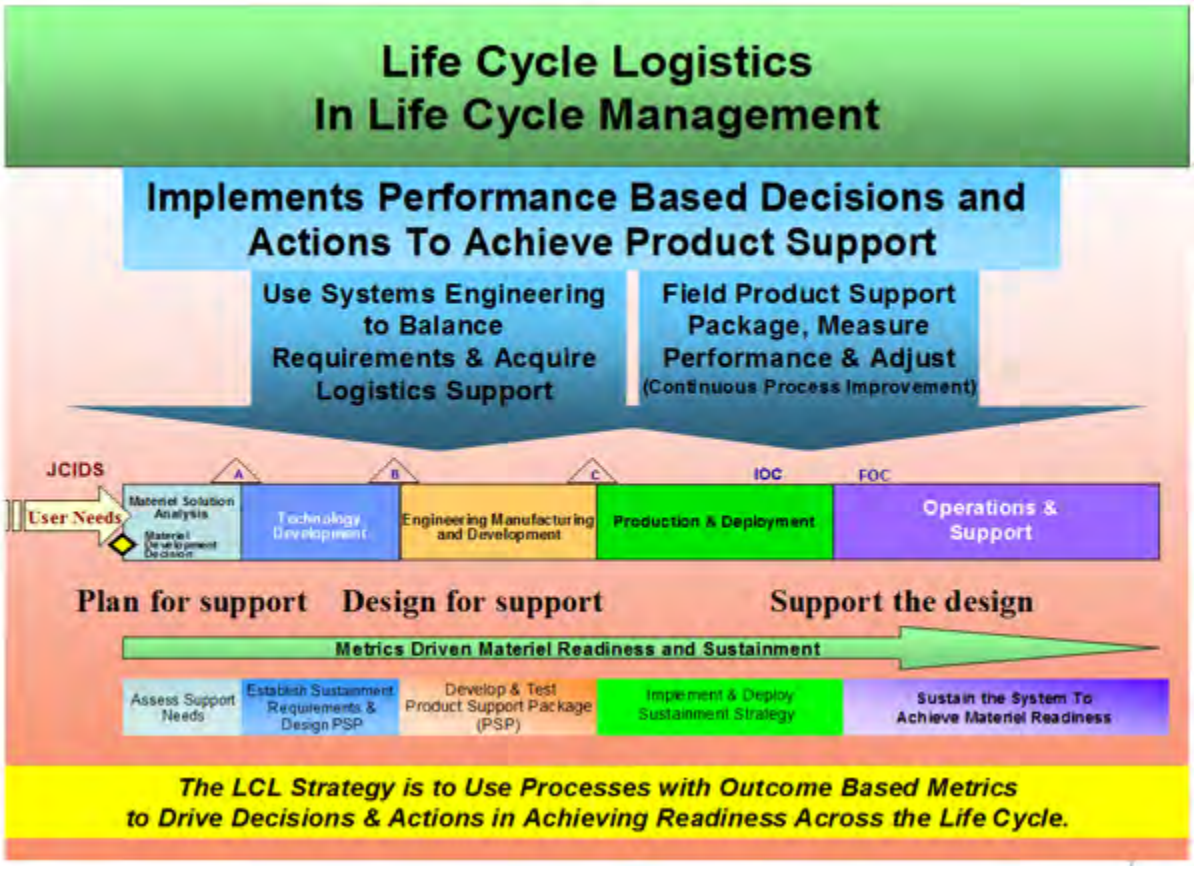
The PM, as the life-cycle manager, is responsible for accomplishing program objectives across the life cycle, including the operating & support (O&S) phase. Employing performance-based life-cycle product support tied to sustainment metrics is the overarching Department of Defense (DoD) concept for providing materiel readiness to the user. This logistics aspect of the life-cycle management approach is depicted in Figure 5.0.1.F1 and discussed in subsequent sections.

There are three DoD Decision Support Systems - Joint Capabilities Integration and Development System (JCIDS) , Defense Acquisition System , and Planning, Programming, Budgeting and Execution (PPBE) process - that frame the environment for implementing life-cycle management. In addition, there are three related but distinct communities, with corresponding reporting chains, within the DoD -- the acquisition, user, and sustainment chains involved in implementing the decision support systems. Working in tandem these communities share responsibilities which vary depending on the life-cycle phase. Consequently, the PM needs to be involved with each chain. The Defense Acquisition Guidebook focuses on the acquisition chain (e.g. the OSD, Service Secretariat, Program Executive Officer chain, etc.). Chapter 5 addresses the acquisition chain and highlights interfaces with the user chain (e.g. the type commander, Theater Commanders, etc.) and sustainment chain (e.g. supply chain (including the transportation system, maintenance facilities and depots, industrial base), in-service engineering organizations, etc.).

During acquisition the focus is primarily through the acquisition community with requirements input from the user and sustainment communities. These requirements include:

- Specification of design parameters for sustainment related system performance capabilities.
- Application of systems engineering to determine the right balance between the systems design requirements and the logistics support requirements to sustain the operational capabilities at an affordable price. This includes using supporting sustainment metrics (e.g. Mean Down Time, Logistics Footprint, etc.) as well as enablers (e.g. condition based maintenance, diagnostics, prognostics, corrosion protection/mitigation, etc.) with their associated metrics to achieve the mandatory sustainment metrics.
- Planning for, resourcing, and executing the design, acquisition, management, and fielding an integrated product support package to sustain the maintenance and support concepts that meet the materiel availability requirements.

Figure 5.0.1.F1. Life-Cycle Logistics Overview



During operations the focus is primarily through the user and sustainment communities with support from the acquisition community. The PM's focus is on supporting the user's ability to effectively meet mission requirements through the application of systems engineering to implement continuous process improvement initiatives. This involves monitoring performance to identify major readiness degraders (e.g., reliability, cycle time and cost) and to:

- Align and refine the product support package (e.g. the product support elements) and sustainment processes to achieve the sustainment metrics
- Engage the various communities to achieve optimum materiel readiness
- Optimize or reduce the logistics demand (including the logistics footprint) and support processes (e.g., training, technical data, supply chain, maintenance, etc.) based on actual conditions
- Reduce operating and support costs
- Identify and implement design changes to address evolving requirements, technological obsolescence, diminishing manufacturing sources, or materiel availability shortfalls.

To accomplish this life-cycle product support concept outcomes are estimated in the

design phase then measured during testing and operations and become the basis for actions to achieve materiel readiness. The sustainment metrics, including the Sustainment Key Performance Parameter (KPP) with its supporting Key System Attributes (KSAs), provide the common thread to integrate the product support elements and align the behaviors required to achieve the desired materiel readiness outcome across the entire enterprise. The goal is to use consistent outcome metrics as the basis for actions to provide and sustain affordable materiel readiness across the entire life cycle.

5.0.2. Contents

Section 5.1 5.3 present information applicable across the lifecycle, while the information in Section 5.4 has been tailored to specific portions of the lifecycle.

Section 5.1, Life-Cycle Sustainment in the Defense Acquisition Management System , describes life-cycle sustainment, explains it's role, and identifies the PM's primary life-cycle logistics and sustainment responsibilities. It provides the context for conducting sustainment-related activities relative to performance-based life-cycle product support and the sustainment metrics.

Section 5.2, Applying Systems Engineering to Life-Cycle Sustainment , focuses on the process to plan for, achieve and sustain affordable systems operational effectiveness. The concept of applying life-cycle cost, modeling and simulation, and supportability analyses to design out "sustainment disablers" to optimize the support system is presented in this section.

Section 5.3, Supportability Design Considerations , focuses on design features that should be incorporated to help make a system more sustainable, including reliability, diagnostic, and predictive monitoring capabilities.

Section 5.4, Sustainment in the Life-Cycle Phases , focuses on how life-cycle sustainment integrates into life-cycle management and the acquisition process/decision points. It identifies key activities in each program phase, whether it is a major new system, a modification to a fielded system, or a redesign of the product support system. This section applies the concepts discussed in sections 5.1, 5.2, and 5.3, placing them in the Defense Acquisition Management System to demonstrate when sustainment related activities take place. It also contains specific focus areas for consideration and the results expected in preparing for each milestone or review.

Section 5.5, References , provides references for further explanation and information.

5.1. Life-Cycle Sustainment in the Defense Acquisition Management System

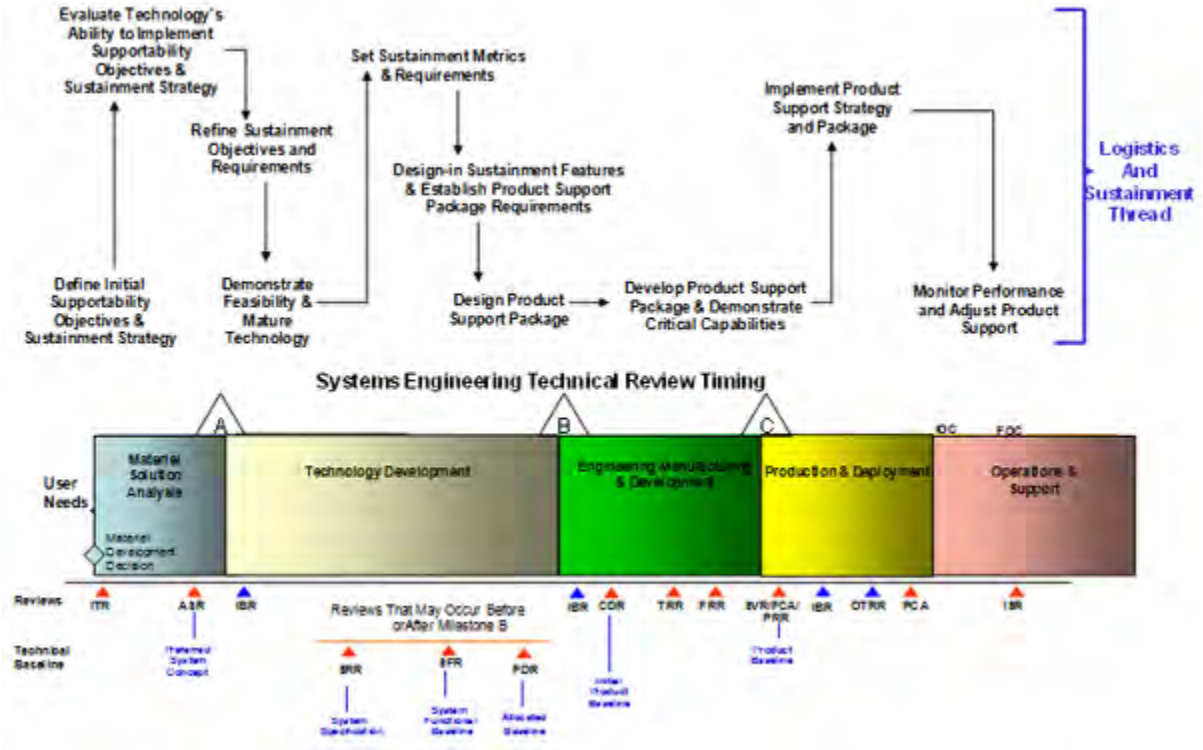
This section highlights important sustainment related activities a program manager should consider. Topics discussed in this section are applicable to multiple phases and it addresses the major deliverables to be prepared or updated during subsequent phases or increments. DoD Instruction 5000.02 provides a complete discussion of the activities and requirements encompassed in the Defense Acquisition Management System. More detailed sustainment related information can be found in subsequent sections and the references.

5.1.1. Life-Cycle Sustainment

Life-cycle sustainment involves the early planning, development, implementation, and management of a comprehensive, affordable, effective performance driven logistics support strategy. It plays a key role during all phases of the life cycle as Figure 5.1.1.F1 illustrates. The goal is to ensure sustainment considerations are integrated into all planning, implementation, management, and oversight activities associated with the acquisition, development, production, fielding, support, and disposal of a system across its life cycle. This includes:

- Participating in the design process to acquire a highly supportable and sustainable system
- Providing affordable, reliable, effective support strategies and systems that meet the users requirements with optimum materiel availability
- Developing the appropriate metrics to validate and verify the system engineering design process, and measure the performance of the support strategy/supply chain
- Providing the user effective systems with the minimal logistics footprint (e.g., the measurable size or "presence" of logistics support, including manpower, required to deploy, sustain, and move a system).
- Developing more integrated and streamlined acquisition and statutorily compliant logistics support processes
- Facilitating iterative technology enhancements during the system life cycle

Figure 5.1.1.F1. Sustainment Thread in the Defense Acquisition Management System



The goal can be accomplished by using metrics-driven outcome-based processes to drive decisions and actions by the stakeholders across the enterprise and life cycle. It should be carried out by a cross functional team of subject matter experts ensuring sustainment requirements are both consistently and comprehensively addressed and balanced with cost, schedule and performance. Sustainment should be considered in the systems engineering process to ensure decisions focused on the ability to operate and support a system are implemented during its design, development, production, and sustainment. Key tenets in accomplishing the goal include, but are not limited to:

- Single point of accountability for accomplishing program sustainment objectives including the logistics system and support;
- Incremental acquisition and statutorily compliant product support strategies;
- Comprehensive integration of hardware, software and humans throughout the life cycle to optimize usability, availability, maintainability, sustainability and affordability. This includes follow on modifications to address deficiency reports and sustainment issues.
- Metrics-driven decisions based on a meaningful user outcome measure (e.g., Materiel Availability) supported by a materiel quality measure (e.g., Materiel Reliability), a sustainment quality measure (e.g., Mean Down Time), and a cost measure (e.g., Ownership Cost);

- Understanding industrial base capabilities and service capabilities;
- Ensuring competition, or the option of competition, at both the prime and subcontract level throughout the program life cycle;
- Performance-based life-cycle product support strategies to project and sustain the force with minimal footprint that support the Sustainment KPP, it's associated KSAs, and overall affordability goals;
- Continuous process improvement including assessing the life-cycle product support strategies, to include end-to-end sustainment chain planning, assessment, and execution.

5.1.1.1. Product Support

Product Support is the application of the package of integrated product support elements and support functions necessary to sustain the readiness and operational capability of the system. While it varies by organization typically, the product support package (PSP) includes the product support elements contained in Figure 5.1.1.1.F1. They must be integrated because they impact each other and Materiel Availability. During the acquisition process the focus is on influencing the design for supportability and by fielding the support concept to satisfy user specified requirements for sustaining system performance at the lowest LCC. This applies to each increment of capability to be developed. Features include:

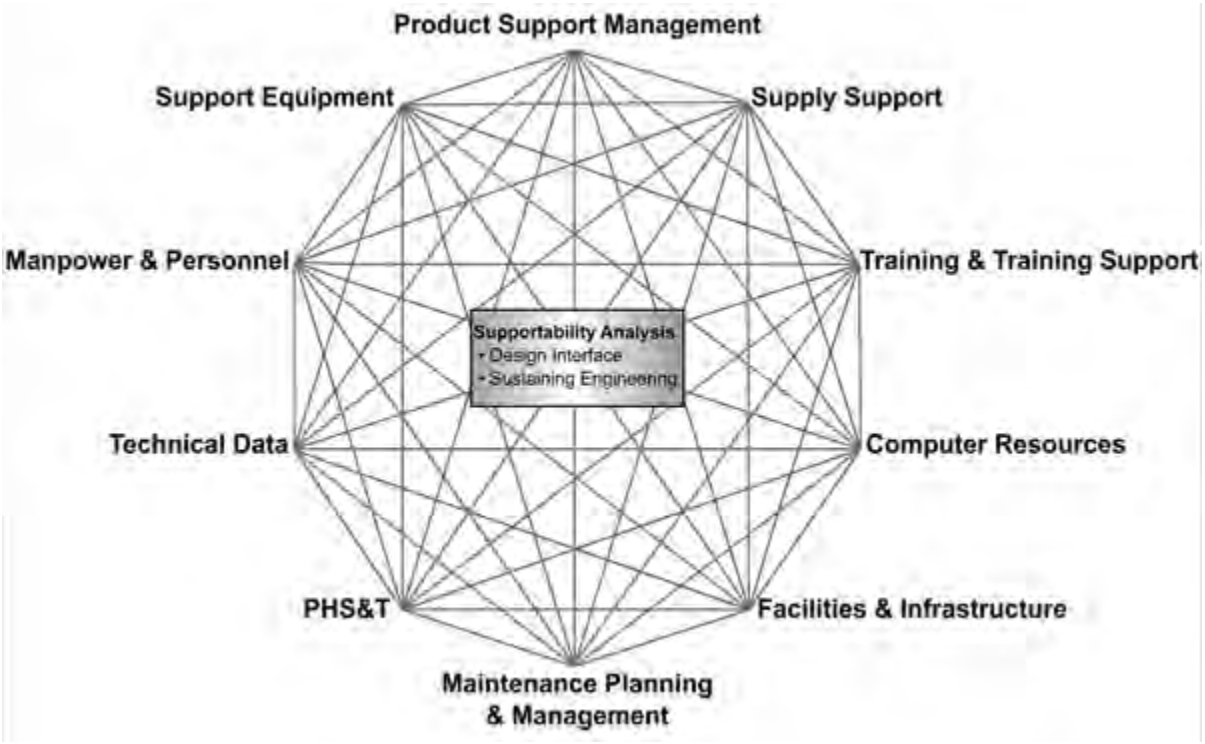
- Availability of support to meet Warfighter specified levels of combat and peacetime performance;
- Logistics support that sustains both short and long term readiness;
- Management of life-cycle cost (LCC) through analysis and decision prioritization;
- Maintenance concepts to integrate the product support elements and optimize readiness while drawing upon both organic and industry sources;
- Data management and configuration management that facilitates cost-effective product support throughout the system life cycle;
- A diminishing manufacturing sources and material shortages management process that ensures effective, affordable, and operationally reliable systems;
- Operator and maintainer training to encompass the full capability of the system.

Developing the **Product Support Strategy** that defines the overall end state is the first step in achieving product support. In developing the support strategy, each program should develop an affordable strategy that:

- Positions and delivers materiel to satisfy highly variable readiness and combat sustainment needs in a variety of unique and demanding environments.
- Meets all materiel management and maintenance statutory requirements.
- Supports rapid power projection.
- Improves readiness through performance-based sustainment strategies.
- Establishes end-to-end processes focused on outcomes.
- Implements contemporary business systems and practices that enable the integration of people, information, and processes.

- Protects critical program information including as it moves through the supply chain, as required in DoD Instruction 5200.39 .

Figure 5.1.1.1.F1. Product Support Elements



The support concept has to address the hardware and its associated technical data and computer software (including Commercial Off The Self (COTS) software) since software can be a major sustainment issue as systems become more software intensive. Programs need to plan for technology refreshment and maintaining the software after production. This includes how changes (for obsolescence/ technology refreshment and maintaining the software) will be budgeted and executed along with the necessary computer software documentation required to sustain the software throughout the system life. In addition to sustaining the software, aspects such as customer support, systems administration help desk support, etc. need to be considered.

Achieving the support concept and sustaining operational capability requires the involvement of the logistics, engineering, testing, program management, contracts, supply chain, and financial management experts. The overall support strategy, documented in the Life-Cycle Sustainment Plan, should include life-cycle support planning and address actions to assure sustainment and continually improve product affordability for programs in initial procurement, re-procurement, and post-production support. A performance-based product support plan will be used to align the support activities necessary to meet these objectives.

5.1.1.2. Sustainment Metrics

In a performance based environment, sustainment related requirements, with a specified range of minimum mandatory (threshold) and target (objective) performance capability design parameters are established with accompanying metrics covering the entire enterprise. This includes the system and the supply chain supporting it. (The same basic model holds for the supply chain, but this chapter focuses on the program manger's role.) Sustained materiel readiness of war fighting capability can then be achieved by developing optimally effective and affordable life-cycle costs investment strategies to achieve the sustainment metrics. The metrics should possess the following key attributes.

Traceable to User Requirements: Sustainment metrics must reflect user requirements. The metrics and their values should be derived from the systems operational requirements and expected use, (as articulated in the Capabilities-Based Assessment (CBA) process) and the product support strategy to sustain it. They should also be supported by comprehensive and early supportability planning and analyses to balance technology feasibility, life-cycle costs and operational needs.

Achievable and Verifiable: The sustainment metric requirements must be obtainable. (Unrealistic requirements adversely affect the development process, result in unachievable performance levels, and drive higher acquisition and sustainment costs.) They should also be stated in demonstrable terms reflecting the projected range of military operations (e.g., design reference missions) and intended operating environment that must be supported. These attributes are critical for sustainment requirements to be used within the design tradeoff process along with cost, schedule, and performance.

Minimum Reporting: The specific metrics should be tailored to the program and it's operational and sustainment needs. At a minimum, they should consist of four interrelated metrics: an outcome metric meaningful to the user in achieving and sustaining the operating tempo; a materiel metric to measure the systems quality; a response metric to measure the quality of the logistics system; and a cost metric. They should be consistently defined within the program and traceable to the operational need. At the top level, the sustainment metrics should focus on providing an effective system that is available and reliable with minimal down time at a reasonable cost. Exact definitions and details can be found in the JCIDS Manual . However, programs have the flexibility to tailor the metrics (including adding additional sustainment metrics (e.g. footprint, manning levels) as long as the intent is met. The following describes the general intent of each of the metrics:

- **Materiel Availability** the percentage of the total inventory (not just the operationally assigned assets) operationally capable at a given time based on materiel condition. This "total inventory" aspect is critical because it not only measures the ability to execute "today's" missions but also provides an indication of the "surge" ability. Materiel availability is primarily an indication of the

percentage of time a system is operationally capable of performing an assigned mission. In addition to the planned missions/scenarios, operating tempo, and sustainment concept of operations (CONOPS), this metric is dependent on system reliability and the mean downtime resulting from, but not limited to failures, scheduled downtime, general maintenance or servicing actions.

- **Materiel Reliability** - the probability the system will perform without failure over a specific interval. This metric focuses on reliability of the entire system and should not be confused with the mission success rate. Defining the criteria for measuring relevant failures (including consistent definitions for failures (e.g., criteria for counting assets as "up" or "down") and mission critical systems) and clearly defining how time intervals will be measured are important and must be consistent with the other metrics.
- **Mean Down Time** - the average time an end item is unavailable to perform it's assigned mission after it experiences unscheduled or scheduled maintenance actions. It includes all time where the system is not at the disposal of the Force Provider to initiate missions. In addition to the projected supply chain approach with its resultant logistics footprint, the impact of surge/deployment acceleration requirements should be determined for this and the Materiel Availability metric.
- **Ownership Cost KSA** - a subset of the operating and support costs, excluding manpower, training and indirect support cost. However, to address affordability it is important to use operations and support costs to influence program design, acquisition, and sustainment alternative decisions. Consequently, pending the official JCIDS Manual change, OSD is now requiring programs report the O&S costs along with the Ownership Cost KSA because the programs cost model must be consistent with the design specifications as well as the assumptions and conditions used for Materiel Availability, Materiel Reliability and Mean Down Time metrics. In all cases it is critical the cost structure being used be clearly defined (along with the cost estimating relationships/models, and assumptions) and all relevant costs for the trade-off decisions are included regardless of funding source. (see chapter 3).

The selection of the specific performance metrics should be carefully considered and supported by an operationally-oriented analysis, taking into account technology maturity, fiscal constraints, and the timeframe the capability is required. In implementing performance-based life-cycle product support strategies, the metrics should be appropriate to the scope of product support integrators and providers responsibilities and should be revisited as necessary to ensure they are motivating the desired behaviors across the enterprise. During operations the program can consider measuring additional metrics for configuration control, training effectiveness, overall user satisfaction, etc. The specific metrics selected should tie to existing user performance measures and reporting systems. In addition, existing logistics and financial metrics should be related to these top level user performance metrics and considered as supporting metrics to help provide confidence they can be met as well as identify risk areas.

5.1.1.3. Performance-Based Life-Cycle Product Support Implementation

DoD Directive 5000.01, E1.1.17 , requires program managers (PMs) to:

"develop and implement performance-based product support strategies that optimize total system availability while minimizing cost and logistics footprint. Sustainment strategies shall include the best use of public and private sector capabilities through government/industry partnering initiatives, in accordance with statutory requirements."

Building on the best features of the public and private sectors is a key component of the support strategy. The Performance-Based Life-Cycle Product Support Implementation Framework (Figure 5.1.1.3.F1) captures the range of capability solutions that could be employed. The framework is incremental, in that each alternative builds on the previous category. In all cases the systems sustainment parameters are projected and measured during the design process and then re-assessed once the system is operational so appropriate actions can be taken to achieve the Materiel Availability objective. Within each category, the program manager is responsible for working with the stakeholders to ensure the appropriate actions are taken to meet the user's needs. The difference is the amount of financial risk shared with the product support integrator or provider and sustainment aspects covered. The categories do not imply a level of "goodness" but only provide a means to illustrate the wide range of implementation options available to the program. Each category description is described below.

Category 1: In a life-cycle management environment, all programs should perform to at least this level. This is the traditional support concept where the program buys the various individual support elements. The government develops the requirements, integrates, procures, and balances the product support elements to achieve the material availability outcome. The contractor metrics are usually cost and schedule. The difference from the traditional approach is what happens once the system is operational. Once operational, the program manager measures the materiel availability and takes appropriate actions with the stakeholders to meet the user's needs. However, most of the fiscal risks are on the government side and the PM works with the product support element functional offices, government infrastructure/supply chain, and contractors to determine and ensure corrective actions are taken.

Category 2: At level 2 fiscal risks begin to transition, but only in narrow but critical supply chain functional areas. Typical functions falling within this level include providing material, inventory management, transportation, and/or maintenance where the provider is accountable for the responsiveness required to meet customer requirements. This level generally concentrates on providing parts with the government making design decisions. Part availability, mean down time (MDT) or logistics response time (LRT) are the typical metrics for Level 2 implementations where the time it takes the supplier to deliver the part, commodity or service to the user determines their payment. In using the approach, care must be given to the requirements and contract terms to ensure they drive the supplier's behavior so the government achieves an affordable material

readiness outcome.

The PM is still responsible for taking the appropriate actions with the providers; however, more risks are shared because there are fewer providers with whom to coordinate. The PM still procures many of the individual product support elements and manages the systems configuration. The program has to develop performance requirements, integrate, procure, and balance the elements not included in the Performance-Based Agreement (PBA) to achieve an affordable materiel availability outcome.

Category 3: This level expands the provider's fiscal risk level by transferring life-cycle support activities to the product support integrator (PSI), making them accountable for sustaining overall system materiel availability. Category 3 typically focuses on maintaining the required availability of key components or assemblies, such as a wing flap or auxiliary power unit, but can include the entire system. In Category 3, there is an additional PSI focus on life-cycle support, training, maintenance, repair and overhaul including logistics planning and execution, in-service engineering, configuration management and transportation. In Category 3, the PSI may also make repair or replace decisions. The preferred metric is materiel availability.

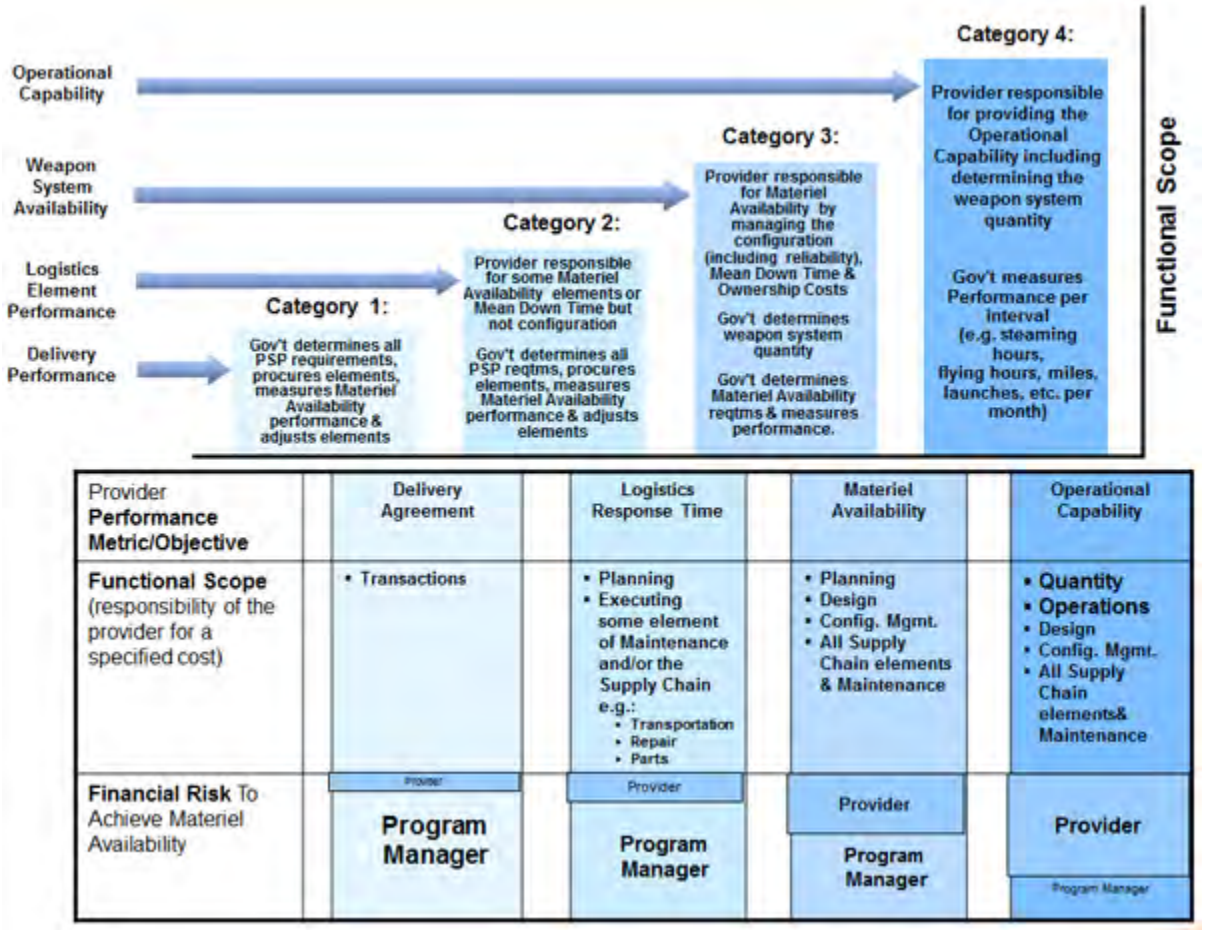
At this level the product support integrator is assigned specific life-cycle responsibility, solely or in partnership, for the breadth of processes affecting materiel availability. This includes aspects of sustainment engineering and configuration control, since reliability and maintenance of equipment and effectiveness of the supply chain influences continually affordable operational availability.

Category 4: This level transfers life-cycle support and design performance responsibilities making the product support integrator responsible for assuring operational availability (Ao) or operational capability. Typically this level applies to systems in the form of operational capability, such as "steaming hours, flying hours or miles per month"; "launches per month"; "power by the hour"; etc. The PSI is assigned responsibility, solely or in partnership, for the breadth of processes that influence Materiel Readiness. This gives the PSI the flexibility to adopt any practices and technology enablers needed to meet required performance levels, including the number of systems deployed and where they are located or staged.

Performance-Based Product Support Contracts (PBL): The DoD intent is to use performance-based support. This includes, where it provides the best long term value, using performance based contracts rather than transaction based contracts (i.e. buying Materiel Availability vice buying spares or support equipment). Any best value assessment has to consider not only cost, but also all other quantifiable and non-quantifiable factors associated with any resultant investment decision. The assessment should stand on its own and be able to withstand rigorous analysis and review by independent audit agencies. PMs should strive for the right mix of implementation in terms of functions provided and the extent to which they are applied to the system.

Contracting for performance based logistics is a multiple step process that can be applied to new, modified or legacy systems. The process is detailed on the web-based PBL Toolkit as a best practice. It is a proven process focusing on legacy programs that can be tailored and adapted to individual systems, subsystems or components to meet its needs and its business and operational environments.

Figure 5.1.1.3.F1. Performance-Based Life-Cycle Product Support Implementation Framework



5.1.1.4. Sustaining System Performance

Conditions change over the life of any system so it is critical that performance be measured against a plan and corrective steps be taken as conditions warrant. These steps can range from corrective actions anywhere within the program or it's supply chain to re-baselining the metrics. Care should be taken to ensure the appropriate stakeholders are involved with any requirements change decisions and that the baseline is not changed too often to avoid rubber baselines.

Monitoring actual performance (or projected performance during design) then taking the

appropriate corrective actions when needed is critical in achieving and sustaining performance. During testing, monitoring allows early corrective actions before the system is deployed. During operations, it can help the PM determine if the metrics are driving the desired behaviors (or if different metrics are needed) to achieve the desired behavior or performance. Consequently, the PM should have a strong monitoring and assessment program structured to fit the unique program conditions. Representatives from each of the functional areas that drive the metrics should be involved in the process.

The Condition Based Maintenance Plus (CBM+) is a specific initiative which can be useful in cost effectively sustaining performance. It is the application and integration of appropriate processes, technologies, and knowledge-based capabilities to improve the reliability and maintenance effectiveness of DoD systems and components. At its core, CBM+ is maintenance performed based on evidence of need provided by Reliability Centered Maintenance (RCM) analysis and other enabling processes and technologies. CBM+ uses a systems engineering approach to collect data, enable analysis, and support the decision-making processes for system acquisition, sustainment, and operations. CBM+ policy is established in DoD Instruction 4151.22.

The program team can often be too close to the day-to-day decisions, so independent program reviews can be useful in helping ensure the system will be able to maintain or improve performance. The DoD components each have their own structures to do this, usually tied to formal program reviews, but the PM should consider bringing in their own independent reviewers to help in the process and gain lessons learned from other programs.

5.1.2. Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment

5.1.2.1. Key Program Documents

5.1.2.2. Life-Cycle Sustainment Plan (LCSP)

5.1.2.3. Replaced System Sustainment Plan

5.1.2. Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment

Acquisition programs are structured in phases separated by milestone decisions in accordance with the Life-Cycle Management System established in DoD Instruction 5000.02 . (An on-line, interactive version of the Integrated Defense Acquisition, Technology, and Logistics Life-Cycle Management System is also available.) In each phase, from defining user needs to disposal, there are important sustainment issues and actions to address. Figure 5.1.2.F1 provides an overview of key sustainment activities by phase. In addition, under the evolutionary acquisition strategy, each block should address support implications. In those cases a thorough assessment of the existing support strategy vis--vis any new sustainment requirements should be conducted to ensure the support implications for each block are understood, and

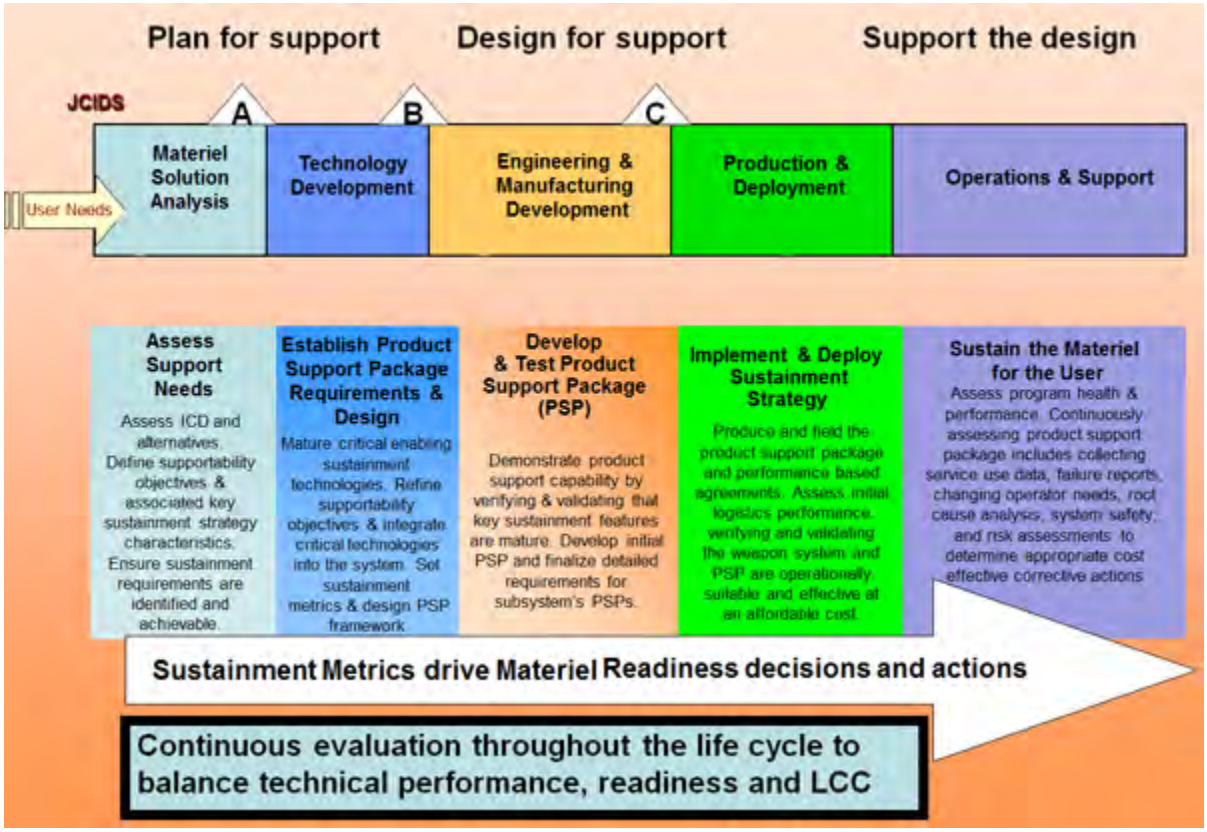
changes are made as necessary, to ensure an affordable materiel readiness strategy.

Statutory, Policy, and Guidance Factors. While the PM has latitude in developing the acquisition strategy, there are statutory requirements that must be taken into account. Congress has enacted a number of statutes capabilities to assure availability of a ready and controlled (i.e. government owned) source of technical competence and resources to ensure effective and timely response to a national defense contingency requirement (10 USC 2464) and ensure that there is a balance between the private and the public sector industrial base (10 USC 2466 and 10 USC 2474). The support strategy must ensure compliance with all statutory and regulatory requirements. These legislative and statutory requirements must be considered as an integral and evolving aspect of all Life-Cycle Management decisions. The PM must also follow Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) guidance, as well as appropriate DoD Directives and Instructions. Instructions, including the DoDD 4151.18 (Maintenance of Military Materiel), DoDI 4151.19 (Serialized Item Management (SIM) for Materiel maintenance), DoDI 4151.22 (Condition Based Maintenance Plus (CBM+) for Materiel Maintenance), DoDI 8320.04 (Item Unique Identification (IUID) Standards for Tangible Personal Property) need to be addressed.

Support strategy. PMs must balance multiple objectives in designing the strategy to achieve operational effectiveness while maintaining affordability. PMs accomplish this by laying out and executing a support strategy so every part of the product support package is integrated and contributes to the users mission capability. To ensure there is a means to assess performance the PM and product support provider(s) should redefine and augment system sustainment metrics used to meet system capability requirements. (Support providers may be public, private, or a mix, to include public private partnerships. Examples of public support providers include DoD maintenance depots, DoD Component and Defense Logistics Agency (DLA) inventory control points and distribution depots.) The PM and the support provider(s) should enter into Performance-Based Agreements that define the sustainment metrics necessary to meet the system performance requirements.

A program manager's best means of ensuring a system will meet its sustainment objectives and satisfy user sustainment needs, is to ensure sustainment considerations are infused in all phases of the program's life cycle. It is especially important that sustainment considerations are included in Pre-Systems Acquisition and Acquisition activities, including the Joint Capabilities Integration and Development System (JCIDS) process, structured program reviews, and tracking sustainment performance drivers during Test and Evaluation. Even after the Initial Operational Capability (IOC) date, the support strategy should be periodically reviewed and revised when sustainment metrics are not being met or requirements change. These actions should be defined in the Life-Cycle Sustainment Plan (LCSP) and other appropriate program documents.

Figure 5.1.2.F1. Key Sustainment Activities by Phase



5.1.2.1. Key Program Documents

This section addresses the sustainment aspects that should be included in key program acquisition documents that cut across life-cycle phases. (Phase unique documents and focus areas are addressed in subsequent sections). To help ensure a shared understanding of the program's intent, it is important the documents used by the PM in the acquisition process and program reviews be updated during subsequent phases, especially prior to milestone decisions.

Initial Capabilities Document (ICD) / Capability Development Document (CDD) / Capability Production Document (CPD) . These documents are the sponsor's means to specify authoritative and testable, performance capabilities for the program. The ICD prefaces a system materiel decision and evolves into the CDD, which prioritizes KPP and subset KSA performance capability design and development parameters. The baseline CPD is finalized after the system level Critical Design Review and before Milestone C. In addition to supportability related KPP/KSAs, the ICD, CDD, and CPD should also address the following:

- System maintenance/support concepts and usage scenarios
- Operational and support environments. This should include the general support

categories relative to the logistics support infrastructure (remote sites, organic depots, commercial facilities, air bases or ship yards, etc. without naming specific locations)
- Expected durations of support
- Support or maintenance effectiveness metrics and key enablers, such as diagnostics/ prognostics
- Conditions conducive to joint sustainment and to performance-based support strategies

Analysis of Alternatives (AoA) . The AoA should describe and include the results of the supportability analyses and trade-offs conducted to determine the optimum support concept as part of the preferred system concept. It should also include the assumptions used in the analyses.

Technology Development Strategy (TDS) . The TDS should also include the specific new sustainment related technologies required to achieve the Sustainment KPP/KSAs. Specific emphasis should be placed on technologies required to achieve logistics performance (including reliability) over what is currently achieved in today's operational environment.

Acquisition Program Baseline (APB) . The APB documents the performance requirements, schedules, and program cost funding and estimates. The program sponsor and program manager will ensure content includes Sustainment KPP/KSAs parameters, measurement metrics, and all programmatic direction affecting life-cycle support strategy planning and execution.

Acquisition Strategy . The Acquisition Strategy describes the PM's approach for acquiring the system and its support. The program manager must include the acquisition strategy for achieving the sustainment metrics and acquiring the product support package. The Acquisition Strategy should include the key upcoming contracting actions and the timeline to acquire the product support elements necessary to maintain the systems readiness and operational capability. Specifically, it should address how the product support package required to support the materiel management, distribution, technical data management, support equipment, maintenance, training, configuration management, engineering support, supply support, and failure reporting/analysis, functions will be acquired. It should also include a summary of the approach for acquiring key enablers for achieving the sustainment metrics (e.g., using diagnostics, prognostics, modular open systems approach, reliability growth).

Test and Evaluation Master Plan . Proper testing is critical to achieve the sustainment metrics thresholds and objectives. The program manager should therefore ensure the TEMP includes a description of the requirements and test points/methods for each of them as well as any appropriate enabler or logistics consideration.

Systems Engineering Plan . The systems engineering approach is an integral part in designing for sustainment and supporting the design. (See the Systems Engineering

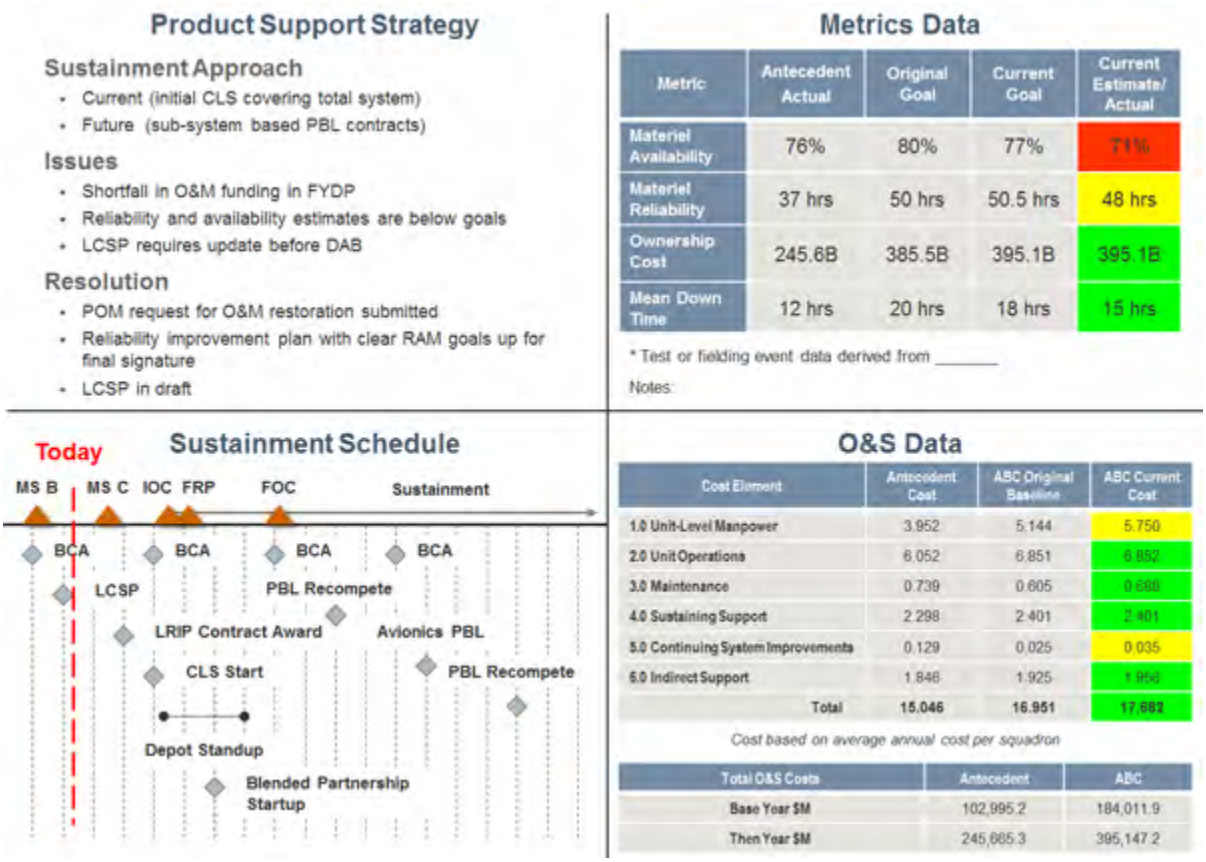
Plan (SEP) Outline) Accordingly, in developing and updating the SEP, the PM should integrate sustainment into the program's technical approach described by addressing how the:

- Sustainment metrics are to be integrated and managed with other requirements.
- Maintenance, sustainment and other support personnel aspects included in the Human Systems Integration (HSI) plan / process will be integrated with the Systems Engineering Process.
- Program will organize and staff it's Integrated Product Teams (IPTs) to address sustainment.
- Process for ensuring sustainment is considered, including the development and update of the Failure Mode, Effects & Criticality Analysis (FMECA) matrix; identification of critical safety items (CSIs); Failure Reporting, Analysis & Corrective Action System (FRACAS); and trend analysis for maturation purposes of the system and its support system.
- Technical baselines (functional, allocated, and product) will address the end item system and its product support package elements.
- Technical reviews will be used to define and assess sustainment and product support package technical maturity against the baselines. This is important because the reviews provide opportunities to ensure sustainment features are being designed into the system. They also provide the opportunity to assess the supportability design feature's maturity so the product support package can be adjusted as needed to achieve the sustainment metrics.

Diminishing Manufacturing Sources/Materiel Shortages (DMSMS) Plan. An efficient, proactive DMSMS management process is critical to providing more effective, affordable, and operational systems by proactively identifying and mitigating DMSMS issues that affect their availability and supportability. Actively addressing DMSMS concerns throughout the entire life of the program will help ensure effective life-cycle support and reduce adverse impacts on readiness or mission capability. The DOD DMSMS Guidebook (SD-22) provides a compilation of the best proactive practices for managing the risk of obsolescence. Establishment of the DMSMS program and proper planning during design will ensure successful implementation in sustainment and throughout the life cycle.

Sustainment Quad Chart. The Quad chart provides sustainment information in a standardized format (Figure 5.1.2.1.F1) that ACAT 1D PMs shall use in reporting status at Overarching Integrated Product Team (OIPT) and Defense Acquisition Board (DAB) reviews. It is used to strengthen sustainment governance by providing senior management visibility of key sustainment factors to help ensure the PMs sustainment strategy meets the Warfighter materiel readiness and long-term affordability objectives. Reporting begins at program initiation and continues through each subsequent milestone, the production decision, and at other reviews when directed. (Detailed instructions for how to fill out the chart can be found at Sustainment Quad Chart web site).

Figure 5.1.2.1.F1. Sustainment Chart



5.1.2.2. Life-Cycle Sustainment Plan (LCSP)

DoD Instruction 5000.02 requires that a LCSP be developed and provided as part of the program approval process to document how the sustainment strategy is being implemented. The LCSP documents the Program Managers plan for formulating, implementing and executing the sustainment strategy so that the systems design as well as the development of the product support package (including any support contracts) are integrated and contribute to the Warfighters mission requirements by achieving and maintaining the Sustainment KPP/KSAs. The LCSP is a living document describing the approach and resources necessary to develop and integrate sustainment requirements into the systems design, development, testing and evaluation, fielding and operations. The LCSP should be tailored to meet program needs documenting the current program plan in the following areas:

- The maintenance and support concepts
- How the sustainment metrics will be achieved and sustained throughout the life-cycle
- How sustainment is addressed as an integral part of the programs acquisition strategy and system design process
- The assigned responsibilities and management approach for achieving effective

and timely acquisition, product support, and availability throughout the life-cycle including the Program Managers role in planning for and executing sustainment
- The funding required and budgeted by year and appropriation for the main sustainment cost categories including operating & support costs
- The plan for identifying and selecting sources of repair or support
- The sustainment risk areas and mitigation plans
- Product support implementation status
- Results and recommendations from DoD Component Independent Logistics Assessments (ILA)

Figure 5.1.2.2.F1 provides the outline that will be used to document the PMs plan for how the Product Support Manger will implement the sustainment strategy. Details for each section and additional information including mandated content can be found at the LCSP web site .

Figure 5.1.2.2.F1. LCSP Outline

1 Introduction

2 Product Support Performance

2.1 Sustainment Performance Requirements

2.2 Demonstrated (tested) Sustainment Performance

3 Product Support Strategy

3.1 Sustainment Strategy Considerations

3.2 Sustainment Relationships

4 Product Support Arrangements

4.1 Contracts

4.2 Performance Based Agreements (PBA)

5 Product Support Package Status

5.1 Program Review Results

5.2 Product Support Package Assessment

6 Regulatory/Statutory Requirements That Influence Sustainment Performance

7 Integrated Schedule

8 Funding

9 Management

9.1 Organization

9.1.1 Government Program Office Organization

9.1.2 Program Office Product Support Staffing Levels

9.1.3 Contractor(s) Program Office Organization

9.1.4 Product Support Team Organization

9.2 Management Approach

9.2.1 Product Support Manager Roles and Responsibilities

9.2.2 Sustainment Risk Management

10 Supportability Analysis

10.1 Design Interface

10.1.1 Design Analysis

10.1.2 Technical Reviews

10.2 Product Support Element Determination

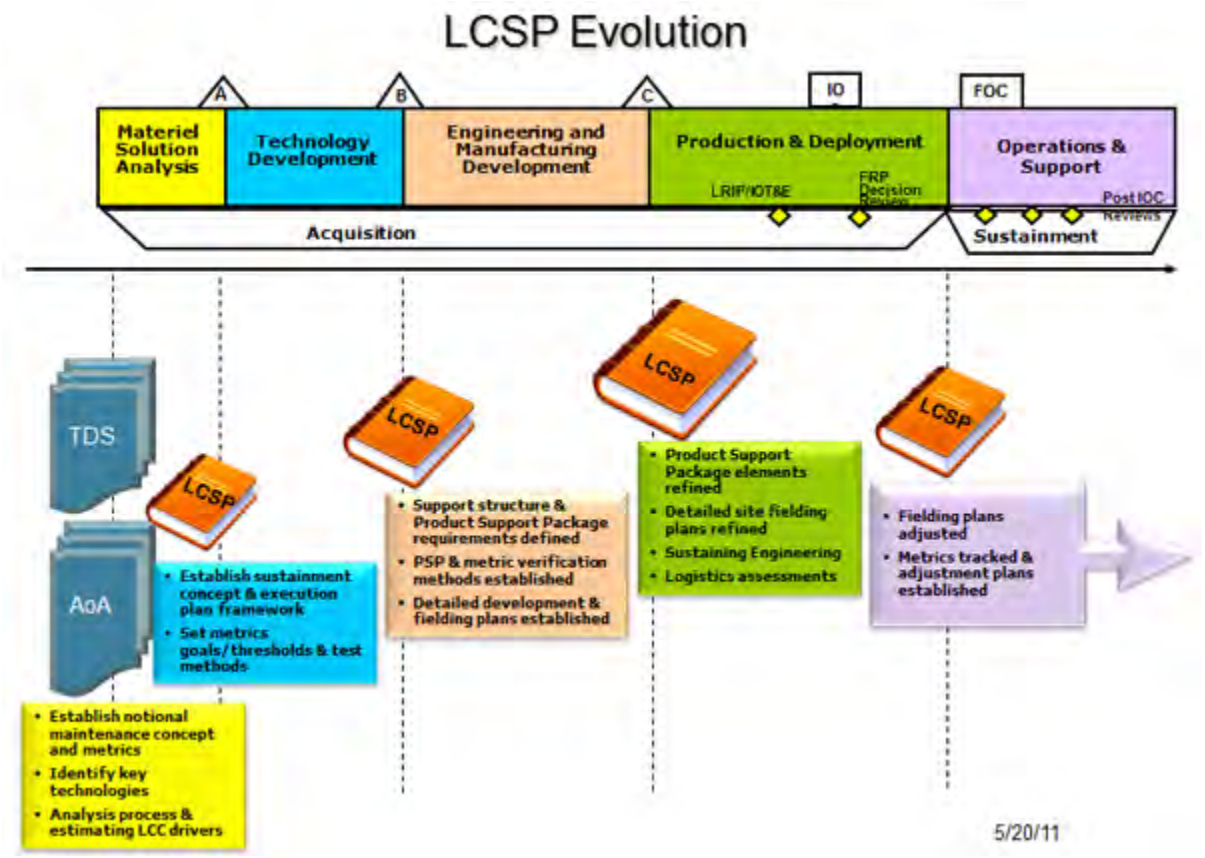
10.3 Sustaining Engineering

11 Additional Sustainment Planning Factors

LCSP Annexes

LCSP Evolution. Life-cycle sustainment planning and execution seamlessly span a systems entire life-cycle evolving over time (see Figure 5.1.2.2.F2). The LCSP begins in the Materiel Solution Analysis Phase by describing the notional product support and maintenance concepts used to determine the sustainment requirements optimizing readiness outcomes and minimal life cycle-cost. The LCSP evolves from a strategic outline to a management plan describing the sustainment efforts in the system design and acquisition processes to achieve the required performance and sustainment outcomes necessary to ensure required Warfighter capabilities. It evolves at Milestone B into a detailed execution plan for how the product support package is to be designed, acquired, sustained, and how sustainment will be applied, measured, managed, assessed, modified, and reported from system fielding through disposal.

Figure 5.1.2.2.F2. LCSP Evolution



By Milestone C, the LCSP describes the implementation status of the product support package (including any sustainment related contracts, e.g. Interim Contractor Support, Contractor Logistics Support) to achieve the Sustainment KPP/KSAs. In addition to sustaining the system performance capability threshold criteria and meeting any evolving user readiness needs, the LCSP details how the program will manage O&S costs and reduce the logistics footprint. After the Full Rate Production Decision Review update, the LCSP describes the plans for sustaining affordable materiel availability as well as accommodating modifications, upgrades, and re-procurement. It should be updated for any Post-IOC Sustainment Reviews and shall be updated, at a minimum every 5 years, or when:

- Subsequent increments are approved and funded to reflect how the support strategy will evolve to support multiple configurations.
- Significant changes are required to the product support package to achieve the objective sustainment metrics including major support provider changes.

As the program matures, the LCSP is updated to reflect increasing levels of detail as they become available. The detail and focus will vary depending on the life-cycle phase but in all cases the information should be in sufficient depth to ensure the acquisition, design, sustainment, and user communities have an early common understanding of

the sustainment requirements, approach, and associated risks. Section 5.4 expands on the primary focus areas for each life-cycle phase.

LCSP Development. The Program Manager is responsible for the content and preparation of the Life-cycle Sustainment Plan. The Product Support Manager is the PMs focal point for developing this document to function as the programs tool in managing all sustainment efforts. (**Note:** If this objective is achieved, then the same LCSP should effectively serve the needs of decision reviews.)

The Product Support Manager must capitalize on the product support expertise of the programs Sustainment Integrated Product Team (IPT) to produce a plan that can be useful, and credible to all stakeholders charged with executing the plan. Specifically in developing and executing the LCSP, the PM should work with the user, the Product Support Manager, Product Support Integrator(s), and Product Support Providers to document performance and sustainment requirements specifying objective outcomes, resource commitments, and stakeholder responsibilities. Once developed, to help ensure an integrated team approach, the LCSP should be approved by the Program Manager, Product Support Manager, Contracting Officer, lead financial analyst and lead engineer. Last but not least, the best way to ensure that the secondary purpose of supporting decision reviews is satisfied is to include a representative (Action Officer) from the appropriate Milestone Decision Authority as a member of the Sustainment IPT.

An effective LCSP services as the nexus of critical thinking for not only logisticians and sustainment stakeholders, but among all functional disciplines required to comprehensively deliver effective and affordable product support. The PSM Guidebook (section 4) addresses the process that should be used to generate the Product Support Strategy and the associated plan to implement the strategy. In addition, each section of the LCSP may require the integration of multiple sections of this chapter, and indeed multiple sections of the broader Defense Acquisition Guidebook. The following table provides a mapping of the individual LCSP sections to key relevant sections of this guidebook that the PSM will find useful for both context and direct guidance in formulating planning content.

Table 5.1.2.2.T1.

LCSP Table of Contents	Applicable DAG Chapter Contents
1 Introduction	5.1.2, 5.4 2.2.15, 2.3.15
2 Product Support Performance	5.3
2.1 Sustainment Performance Requirements	5.1, 5.3, 5.4 1.3, 2.1, 2.2, 2.3, 3.3, 4.3

2.2 Demonstrated (tested) Sustainment Performance	5.3, 5.4 2.0, 2.2, 2.3, 9.1, 9.4, 9.7
3 Product Support Strategy	5.1, PSM Guidebook (section 1) 2.2, 4.3.18, 6.3, 9.9, 11.7
3.1 Sustainment Strategy Considerations	5.1, 5.2, 5.3, 5.4 4.3.18, 11.2
3.2 Sustainment Relationships	5.2, 5.4 4.1.4, 6.2, 6.3, 9.2
4 Product Support Arrangements	5.1, 5.4, PSM Guidebook (sections 2 and 4) 2.2, 2.3
4.1 Contracts	5.1, 5.4 2.0.3, 2.2, 4.1, 11.3, 11.9, 11.10
4.2 Performance Based Agreements (PBA)	5.4 11.6
5 Product Support Package Status	5.4, PSM Guidebook
5.1 Program Review Results	5.4 4.2.8, 9.7, 10.5
5.2 Product Support Package Assessment	5.4 9.3, 9.4, 10.5
6 Regulatory/Statutory Requirements That Influence Sustainment Performance	5.1, 5.2, 5.4 4.3.18, DoDI 5000.02 Encl 4
7 Integrated Schedule	5.1, 5.4, PSM Guidebook (section 3) 2.2, 2.3, 4.2, 4.3.2, 9.6
8 Funding	5.1, PSM Guidebook Appx A 1.2, 2.2, 2.3, 3.1, 3.2, 3.3, 3.4, 3.5, 6.5, 10.5, 10.9,
9 Management	5.1, PSM Guidebook (all) 2.3, 3.3, 4.1, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 14

9.1 Organization	5.1 2.2
9.1.1 Government Program Office Organization	5.1
9.1.2 Program Office Product Support Staffing Levels	5.1
9.1.3 Contractor(s) Program Office Organization	5.1, 5.4.
9.1.4 Product Support Team Organization	5.1, 5.4 4.1.4, 6.2, 9.1, 9.6
9.2 Management Approach	5.1 11.3
9.2.1 Product Support Manager Roles and Responsibilities	5.1
9.2.2 Sustainment Risk Management	5.4 2.2, 2.3, 4.3.6, 6.2, 11.4
10 Supportability Analysis	5.2, 5.4 4.3.18.22
10.1 Design Interface	5.3, 5.4 2.0.3, 2.1.
10.1.1 Design Analysis	5.2, 5.4 4.3.18.19
10.1.2 Technical Reviews	5.4 4.2.8
10.2 Product Support Element Determination	5.2, 5.4 4.3.18.22, 4.3.19, 6.3, 9.3, 11.3.3.1, 11.13
10.3 Sustaining Engineering	5.1, 5.4
11 Additional Sustainment Planning Factors	5.4, 5.5, PSM Guidebook (section 2)
LCSP Annexes	5.1, 5.2, 5.3, 5.4, 5.5

5.1.2.3. Replaced System Sustainment Plan

Once a decision has been made that a system will replace another and it is required, the Service Secretary sponsoring the new Major Defense Acquisition Program (MDAP)

(or the Commander of the United States Special Operations Command) shall prepare a Replaced System Sustainment Plan for the existing system. (10 USC 2437) It will include at a minimum the following which will require close coordination between any effected programs:

- The budget estimates required to sustain the existing system until the new system assumes the majority of mission responsibility. Consequently, it is critical that once a program is operational, it's LCSP contain the current and required funding levels through the FYDP so that the additional funding through disposal can be easily added.
- The milestone schedule for developing and fielding the new system, including the scheduled dates for low-rate initial production, initial operational capability, full-rate production, full operational capability and the date of when the new system is scheduled to assume the majority of the mission responsibilities of the existing system.
- An analysis of the ability of the existing system to maintain mission capability against relevant threats including:
    - Anticipated funding levels necessary to ensure acceptable reliability and availability rates and maintain mission capability against the relevant threats.
    - The extent to which it is necessary and appropriate to transfer mature technologies from the new system or other systems to enhance the mission capability against relevant threats and provide interoperability with the new system during the period from initial fielding until the new system assumes the majority of responsibility for the existing system mission.

5.1.3. Life-Cycle Sustainment in the Integrated Product & Process Development (IPPD) Framework

5.1.3.1. The Program Manager's Role in Life-Cycle Sustainment

5.1.3.2. Product Support Manager (PSM)

5.1.3.3. Integrated Product Teams (IPTs)

5.1.3.4. Stakeholders

5.1.3. Life-Cycle Sustainment in the Integrated Product & Process Development (IPPD) Framework

The IPPD is a management technique using multidisciplinary teams (Integrated Product Teams (IPTs)) to optimize design, manufacturing, maintenance, and logistics processes. The IPPD facilitates meeting cost, statutory, and performance objectives across the life cycle. It is a broad, interdisciplinary approach that includes not only the logisticians, engineers, technical specialists, contract specialists, and customer's in the IPTs, but also business and financial analysts as well. (See also Guidebook sections

10.3 , 11.8 , and the IPPD Handbook .)

5.1.3.1. The Program Manager's Role in Life-Cycle Sustainment

Per DoD Directive 5000.01 , the Program Manager (PM) is accountable for accomplishing program objectives over the life cycle, including during sustainment. Consequently the PM is responsible for the implementation, management, and/or oversight of activities associated with the systems development, production, fielding, sustainment and disposal. Life-cycle management emphasizes early and continuing emphasis on translating performance objectives into an operationally available and affordable capability over the program life cycle including:

- Developing and implementing a life-cycle sustainment strategy acquiring an integrated product support package based on achieving key sustainment performance metrics (e.g., materiel availability, materiel reliability, mean down time, ownership costs, footprint, etc.).
- Providing continuous, reliable, affordable support in accordance with performance agreements with force providers.
- Ensuring the system is supported at optimum levels in accordance with performance agreements among government and industry support providers throughout the life cycle.
- Maintaining visibility into cost/capability/risk decisions across the life cycle.

The PM's responsibility is to provide the user with a sustainable system and product support that meets specified performance effectiveness and affordability requirements. PM's should continually measure, assess, and report program execution in terms of performance, schedule, sustainment, and cost outcomes. In addressing affordability, PMs should continuously perform Should-Cost analysis that scrutinizes every element of government and contractor costs. This includes driving productivity improvements into the program during contract negotiations and throughout program execution including sustainment as directed by the implementation of Will-Cost and Should-Cost Management. These efforts are critical both for establishing budgetary requirements and for tracking execution success over time for both new and legacy programs. In accomplishing this, the PM should examine and implement appropriate, innovative, alternative logistics support practices, including the best public sector and commercial practices and technology solutions. PMs should determine specific discrete and measurable items or initiatives that can achieve savings against the Will-Cost estimate. These actionable items will be presented via the Should-Cost estimate and will be tracked and managed as part of Should-Cost estimate progress reporting. (See Chapter 2.8.8.3 for additional information) The choice of logistics support practices is based on the PM's documented assessment that they can satisfy users in a manner meeting statutory requirements that are fully interoperable within DoD's operational, logistics systems and enterprise; will improve schedules, performance, or support; or will reduce LCC. Regardless of the chosen support strategy, PMs should collaborate with other key stakeholders, especially the user, to refine and establish logistics support program goals for cost, customer support, and performance parameters over the program life cycle.

The resultant decisions and planned actions are critical components in the Acquisition Strategy and the Acquisition Program Baseline.

During acquisition, the PM's focus is to base major decisions on system-wide analyses with the full understanding of the life-cycle consequences of those decisions on system performance and affordability. The emphasis should be on reducing system downtimes and reducing Life-Cycle Costs through deliberate use of systems engineering analysis to design out the maintenance burden, reduce the supply chain, minimize mission impacts and reduce the logistics footprint.

An important performance-based life-cycle product support aspect is the concept of a negotiated agreement between the major stakeholders (e.g., the PM, the force provider(s)/users, and the support provider(s)) that formally documents the performance and support expectations and commensurate resources to achieve the desired outcomes. Per DoD Instruction 5000.02, Enclosure 2, paragraph 8.c.(1)(d) , "The PM shall work with the user to document performance and sustainment requirements in performance agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities." The term "performance agreements," as cited in DoD 5000-series policy, is an overarching term suitable for policy guidance. In actual implementation, the more specific term "performance-based agreements" is used to ensure clarity and consistency.

Demilitarization and Disposal: From the very beginning of a program, it is important that program managers consider and plan for the ultimate system demilitarization and disposal once it is no longer militarily useful. The PM should minimize DoD's liability due to information and technology security, and Environment, Safety, and Occupational Health issues. During the systems engineering process as the design requirements are established, the PM should carefully consider the life-cycle impact of any hazardous material component requirements to minimize the impact on the end item regarding item storage, packaging, handling, transportation, and disposition. (See section 4.3.18.7.)

5.1.3.2. Product Support Manager (PSM)

The day-to-day oversight and management of the product support functions are delegated to a product support manager who is responsible for managing the package of support functions required to field and maintain the readiness and operational capability of major weapon systems, subsystems, and components. This includes all functions related to weapon system readiness including:

- Providing weapon systems product support subject matter expertise . The PSM shall provide weapon systems product support subject matter expertise to the PM for the execution of his or her duties as the total life cycle system manager, in accordance with DoDD 5000.01. In support of this PM responsibility, the PSM shall have a direct reporting relationship and be accountable to the PM for product support consistent with Public Law 111-84 National Defense Authorization Act for Fiscal Year 2010.

- Developing and implementing a comprehensive product support strategy . The product support strategy is designed to assure achievement of warfighter capability-driven life cycle product support outcomes documented in performance-based agreements, generally expressed in the preferred terms of weapon system materiel availability, reliability, and operations and support cost affordability. The strategy should identify the execution plan to deliver integrated product support (IPS) elements to the warfighter, producing the best value balance of materiel readiness and life-cycle costs.
- Promoting opportunities to maximize competition while meeting the objective of best-value long-term outcomes to the warfighter . Tradeoffs between the benefits of long-term relationships and the opportunity for cost reductions through competitive processes should be considered together with associated risk.
- Seeking to leverage enterprise opportunities across programs and DoD Components . Joint strategies are a top priority where more than one DoD Component is the user of the respective major weapon system or variant of the system. Likewise, product support strategies should address a programs product support interrelationship with other programs in their respective portfolio and joint infrastructure, similar to what is performed for operational interdependencies.
- Using appropriate analytical tools to determine the preferred product support strategy . Analytical tools can take many forms (analysis of alternatives, supportability analysis, sustainment business case analysis, life cycle impact analysis), dependent upon the stage of the programs life cycle. These analytical tools shall incorporate the use of cost analyses, such as cost-benefit analyses as outlined in Office of Management and Budget Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, as well as other appropriate DoD and Service guidance consistent with Public Law 111-84. These tools are used to help identify the best possible use of available DoD and industry resources at the system, subsystem, and component levels by analyzing all alternatives available to achieve the desired performance outcomes. Additionally, resources required to implement the preferred alternative should be assessed with associated risks. Sensitivity analyses should also be conducted against each of the IPS elements and tracked to determine those IPS elements where marginal changes could alter the preferred strategy.
- Developing appropriate product support arrangements for implementation . Development and implementation of product support arrangements should be a major consideration during strategy development to assure achievement of the desired performance outcomes. These arrangements should take the form of performance-based agreements, memorandums of agreements, memorandums of understanding, and partnering agreements or contractual agreements with product support integrators (PSIs) and product support providers (PSPs), depending on the best-value service integrators or providers.
- Periodically assessing and adjusting resource allocations and performance requirements to meet warfighter needs during strategy implementation . Planning, programming, budgeting, and execution of the product support strategy need to be accomplished and aligned to the warfighters performance-based agreements with the PM and PSM. PSMs, working in concert with the PM, users,

resource sponsors, and force providers, should adjust performance levels and resources across PSIs and PSPs as necessary, but not less than annually, to optimize implementation of the strategy based on current warfighter requirements and resource availability.

- Documenting the product support strategy in the LCSP . The LCSP describes the plan for the integration of sustainment activities into the acquisition strategy and operational employment of the support system. The PSM prepares the LCSP to document the plan for formulating, integrating, and executing the product support strategy (including any support contracts) to meet the warfighters mission requirements. In accordance with Public Law 111-84 and DoDI 5000.02, the LCSP shall be updated to reflect the evolving maturity of the product support strategy at each milestone, full rate production (FRP), and prior to each change in the product support strategy or every 5 years, whichever occurs first. The LCSP is approved by the milestone decision authority at each milestone and FRP decision. Updates to the LCSP for all major weapons systems after the FRP decision shall be approved by the CAE, in coordination with the Deputy Assistant Secretary of Defense for Materiel Readiness.
- Conducting periodic product support strategy reviews . The product support strategy evolves with the maturation of the weapon system through its various life cycle phases. At FRP, the LCSP should describe how the system is performing relative to the performance metrics and any required corrective actions to ensure the metrics are achieved. Reviews and revalidations of the strategy should be performed at a minimum of every 5 years or prior to each change in the strategy to ensure alignment across system, subsystem, and component levels in support of the defined best-value outcomes. In those situations where a support strategy is at the weapon systems level, the PSMs reassessment should explore potential opportunities for evolving toward a portfolio approach. In those situations where an LCSP is based on a collection of outcome-based product support strategies at the subsystem or component level, the periodic review should explicitly address integrated performance at the weapon systems level. In all situations, the reassessment should consider opportunities to make better use of industry and DoD resources. (See the Logistics Assessment Guidebook for additional information.)

Specific guidance in accomplishing these functions can be found in the Product Support Manager Guidebook . In developing and implementing the performance-based product support strategy the PSM can delegate responsibility for delivering specific outcomes. In doing so, while remaining accountable for system performance, the PM and PSM may employ any number of sub system PSMs or product support integrator(s) to integrate support from all support sources to achieve the performance outcomes specified in a performance-based agreement. They can be further supported by product support providers (PSPs) who provide specific product support functions.

In accomplishing the outcomes, PSIs should have considerable flexibility and latitude in how the necessary support is provided. The activities coordinated can include functions provided by organic organizations, private sector providers, or partnerships. The

following, or any combination of partnerships between them, are candidates for the role:

- A DoD Component organization or command.
- The systems original equipment manufacturer or prime contractor.
- A third party private sector logistics integrator.

While product support execution is accomplished by numerous organizational entities, the PSI is accountable for integrating all sources of support necessary to meet the agreed to support performance metrics as specified in product support arrangements. To effectively coordinate the work and business relationships necessary to satisfy the user agreement the product support integrator should be knowledgeable about the system, involved early in the program life, and incentivized to continuously improve reliability, maintainability, and sustainment technology.

Regardless of the approach taken, the government is ultimately accountable for delivering performance and warfighting capability to the user. Consequently the PSM is responsible for accomplishing the overall integration of product support either directly through government activities or via a contract when commercial organizations are involved. If any part of the product support strategy is contracted, a description of how it will be acquired should be documented in the Acquisition Strategy and LCSP.

5.1.3.3. Integrated Product Teams (IPTs)

The PM should establish multidisciplinary teams to develop and manage the implementation of the performance-based support strategy. The IPTs should consider all factors and criteria necessary to achieve an optimum support strategy using the best capabilities of the public and private sectors in a cost effective manner. DoD Component and DLA logistics activities should participate in support strategy development and IPTs to ensure the support concept is integrated with other logistics support and combat support functions and provide agile and robust combat capability. These participants can help to ensure effective integration of system oriented approaches with commodity oriented approaches (common support approaches), optimize support to users, and maximize total logistics system value.

The teams should be structured to provide a system orientation focused on the performance outcome instead of focusing on the individual logistics support elements or technical disciplines. The teams can consist of government and private sector functional experts; however, it is important they are able to work across organizational and functional boundaries. Consequently, representatives from DoD Component headquarters, operational commands, engineering, procurement, test, comptroller, information technology and logistics representatives from supply, maintenance, and transportation organizations should be considered for inclusion on the IPTs.

5.1.3.4. Stakeholders

Stakeholders consist of any group or organization with a related or subsequent

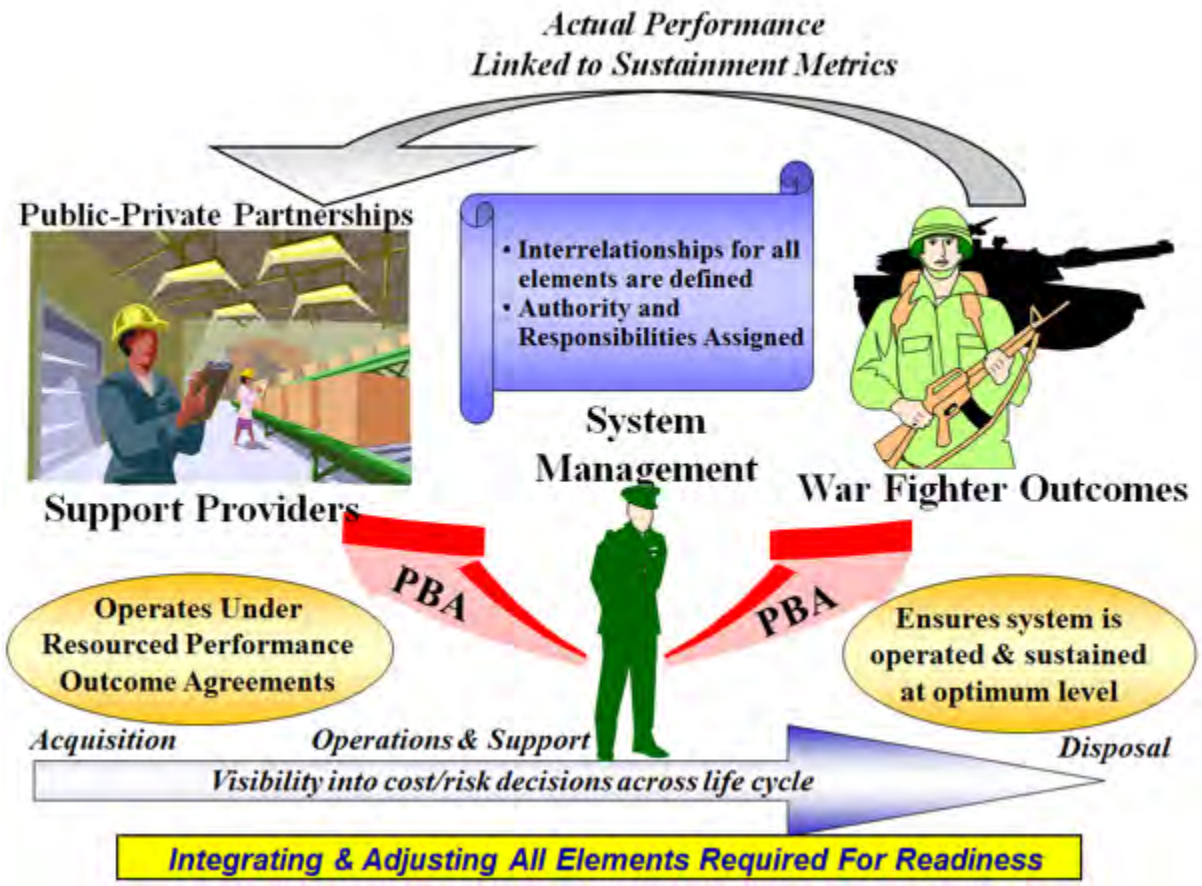
responsibility that is directly related to the outcome of an action or result. Generally speaking they can influence the outcome or are the recipient of the results. The range of personnel selected to participate as stakeholders is based on the outcome and processes involved. Typical stakeholders are: users or operators, acquisition commands, test communities, depots, manpower, personnel & training communities, maintainers, and suppliers (e.g., DLA, the Inventory Control Point (ICP), US Transportation Command (TRANSCOM), industry, and other organizations associated with the sustainment chain).

5.1.4. Performance-Based Agreements (PBAs)

5.1.4. Performance-Based Agreements (PBAs)

PBAs formally document the agreed to level of support and associated funding, required to meet performance requirements. The PBA with the user states the objectives that form the basis of the performance-based product support effort. They establish the negotiated baseline of performance and corresponding support necessary to achieve that performance, whether provided by commercial or organic support providers. The PM negotiates the required level of support to achieve the users desired performance at a cost consistent with available funding. Once the performance and cost are accepted by the stakeholders, the PM enters into PBAs with the user community which specify the level of support and performance. Likewise, PMs enter into performance-based agreements with organic sources and/or contracts with commercial sources which focus on supporting the users in terms of cost, schedule, and performance. Consequently, PBAs can describe agreements between 1) user and PM, 2) PM and support integrator(s), or 3) support integrator and support provider(s). The agreements should maintain flexibility to facilitate execution year funding and/or priority revisions and spell out the 1) objective outcomes, 2) performance measures, 3) resource commitments, and 4) stakeholder responsibilities. (See figure 5.1.4.F1.)

Figure 5.1.4.F1. Performance-Based Agreements



Sustainment metrics should provide the objectives that form the basis of the PBAs. The PBA performance metrics should reflect the highest level of metrics that are most critical in producing the desired performance outcome(s). Generally, a focus on a few properly incentivized performance-based outcome metrics such as materiel availability, materiel reliability, etc. will lead to more effective solutions. However, in developing the agreements, it may not be possible to directly state these high level performance objectives as metrics due to lack of support provider control of the support activities necessary to produce the user performance (e.g., availability). This is because some DoD Component logistics policies and/or guidance mandate a preference for DoD Component performed maintenance and retail supply functions that cut across multiple organizations. Accordingly, the PM may select the next echelon of metrics for which the support provider can be held accountable and which most directly contribute to the sustainment metrics.

The outcome metric to achieve the user requirements (e.g., materiel availability) should be a balance between a quality metric (e.g., materiel reliability), a response metric (e.g., turnaround time), and a cost metric that are appropriate for the outcome needed. Many existing logistics and financial metrics can be related to top level user performance outcomes. These include, but are not limited to, logistics footprint, not mission capable

supply (NMCS), ratio of supply chain costs to sales, maintenance repair turnaround time, depot cycle time, and negotiated time definite delivery. In structuring the metrics and evaluating performance, it is important to clearly delineate any factors that could affect performance, but are outside the control of the support providers.

While objective metrics form the bulk of the evaluation of a provider's performance, some elements of product support might be more appropriately evaluated subjectively by the user and the PM team. This approach allows some flexibility for adjusting to potential support contingencies. For example, there may be different customer priorities to be balanced with overall objective measures of performance.

Agreements with Organic Providers: Organic providers, like commercial providers, will have a set of performance metrics that will be monitored, assessed, incentivized, and focused on the system. For support provided by organic organizations a performance-based agreement, similar in structure to a memorandum of agreement, memorandum of understanding, or service level agreement, may be used to represent and document the terms of the agreement for organic support. One important distinction, however, between PBAs and other types of agreements and understandings is that PBAs contain the agreed to performance and/or sustainment metrics meeting the user requirements tied to funding.

5.1.5. Contracting for Sustainment

5.1.5.1. Contract Characteristics

5.1.5.2. Methodology for Implementing Sustainment Contracts

5.1.5. Contracting for Sustainment

For support provided by commercial organizations, the contract is the PBA reflecting the agreed to user performance requirements. Note that the source of support decisions do not favor either organic or commercial providers. Non-core source of support decisions should optimize the best public and private sector competencies based on a best value determination of the provider's capability to meet set performance objectives. The major shift in the performance-based environment from the traditional approach is how programs acquire support, not from whom it is obtained. The Sustainment Strategy normally results in a blend of commercial and organic product support providers built on the strengths of each to achieve an affordable strategy.

Implementing a performance-based acquisition and sustainment strategy begins with Supportability Analysis to establish the right performance metrics and organic/commercial blend. This upfront analysis is required because instead of buying set levels or varying quantities of spares, repairs, tools, and data, the focus is on designing in sustainment features and buying a predetermined level of readiness to meet the users objectives. (See section 11.6, Implementing a Performance-Based Business Environment.) Executing the Performance-Based Product Support Strategy

also relies on the optimum blend between the organic/commercial providers. For example, when executing commercial product support strategies, the use of on-hand and due-in government inventory should be standard practice of all Performance-Based Logistics and partnering agreements.

5.1.5.1. Contract Characteristics

The preferred contracting approach is the use of long term firm fixed price contracts with incentives tied to outcome performance to fulfill the product support and integrated sustainment chain management responsibilities. Consequently, the contract should provide support over a specific period of time for a predetermined fixed cost per operating measure. Sustainment contracts should require the delivery of a capability to the user using a Statements of Objectives or a Performance Work Statement approach. (Level of effort or labor hour type contracts are not preferred because they limit the contractor's ability to make necessary trade-offs to meet and/or exceed the threshold performance outcomes within the funding profile.)

A sustainment contract may take many forms and the degree to which the outcome is defined varies. It should purchase support as an integrated performance package designed to optimize system readiness. It must specify performance requirements; clearly delineate roles and responsibilities on both sides; specify metrics and their definitions; include appropriate incentives, maximize the use of government-owned inventory before procuring the same parts from private contractors; specify how performance will be assessed. The contract should cover the procurement of a capability to support the user versus the individual parts or repair actions and provide the ability to manage support providers.

Award term contracts should be used where possible to incentivize industry to provide optimal support. Incentives should be tied to metrics tailored to reflect the DoD Component's specific definitions and reporting processes. Award and incentive contracts should include tailored cost reporting to enable appropriate contract management and to facilitate future cost estimating and price analysis. Sustainment contracts should strive to specify a fixed cost per outcome (e.g., operating hour (e.g., hour, mile, cycle) or event (e.g., launch)) vice a cost plus contract. However, lack of data on systems performance or maintenance costs or other pricing risk factors may necessitate cost type contracts until sufficient data is collected to understand the risks. Full access to DoD demand data should be incorporated into any contracts. The contracts should be competitively sourced wherever possible and should make maximum use of small and disadvantaged businesses.

Contracts must follow Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) guidance, as appropriate, for the acquisition of logistics services and support throughout the program life cycle. In addition, competition over the entire life cycle can be a valuable tool for achieving affordable sustainment. Consequently, early in the program, the PM should consider the cost versus benefit of the data and other support elements required to achieve

competitive versus sole source contracting for sustainment functions (e.g. parts, repairs and other supply chain processes).

5.1.5.2. Methodology for Implementing Sustainment Contracts

The contracting methodology is a multiple step process that can be applied to new, modified, or legacy systems at the system, subsystem, or major assembly level covering a range of functions depending on program unique circumstances. Additional guidance is contained at https://acc.dau.mil/pbl but the steps can be summarized in the following general areas:

Define the Requirements: The initial step is to relate or determine the performance outcome metric meeting the user's needs rather than to rely on discrete transactional logistics functions. Care should be given to ensure the costs and performance metrics selected focus measurable contractor behavior in terms of the metrics selected. Defining and documenting the requirement involves answering three key questions: Who are the key stakeholders? What are the operations and sustainment environment and infrastructure? What are the total system cost and performance objectives? To develop an effective contracting strategy, the PM needs to identify the risks and benefits to achieve the desired outcome. Evolving system sustainment requirements should be constantly equated to long term financial resources.

In determining the extent to which contracts will be used, the PM should determine the best mix of public and private sector capabilities to meet evolving user requirements, joint sustainment opportunities, and the statutory requirements. (DoD Directive 5000.01, E1.1.17) This involves identifying the best mix in terms of: capability, skills, infrastructure, opportunities for partnering, compliance with Title 10, public/private flexibility, and affordability for each support function. As operating scenarios and technologies change, supportability related performance requirements may change. Thus, refining and resources for system requirements is a continual management process.

Sustainment contracts should produce measurable performance outcomes that cumulatively contribute to the sustainment of system KPP/KSAs, to their threshold or objective levels. To motivate the contractor to achieve the desired behavior, appropriate contract incentives (including award fee, incentive fee, award term, and cost sharing) need to be developed to promote and facilitate contractor performance.

Develop and Award the Contract: From a sustainment perspective, contracts should be structured to balance three major objectives throughout the life cycle of the system: 1) delivering sustained materiel readiness; 2) minimizing the requirement for logistics support through technology insertion and refreshment; and 3) continually improving the cost-effectiveness of logistics products and services. Careful balancing of investments in logistics and technology to leverage technological advances through the insertion of mature technology is critical. In addition, the PM should ensure the contract addresses user requirements during peacetime, contingency operations, and war and provides for

the capability for the government to compete or take over the sustainment responsibility in the future.

Contract development is a lengthy, complex process, led by the PM, involving multiple stakeholders. No two contracts are exactly the same each must be tailored to the unique requirements of the system considering, at minimum, the factors and criteria listed below:

- **Statutory requirements:** Title 10 U.S.C. 2460 , 2464 , 2466 , 2469 , and 2474 (Core, 50/50, public/private partnering, etc.). Depot maintenance partnerships can be effective tools to implement performance-based product support arrangements if properly structured. The contracts should allow partnering with public depot maintenance activities to satisfy the requirements. (Examples and further discussion of public private partnerships can be found on the Acquisition Community Connection web site.)
- **Regulatory requirements:** DoD (e.g., DFARS) and DoD Component policy (including contractors on the battlefield, service performance of organizational level support functions, etc.).
- **Financial Enablers:** Ensuring the financial enablers are commensurate with the risks.

Implement and Assess Performance: The life-cycle management concept includes assessing actual system performance, readiness, and LCC and then revising the sustainment strategy and contracts as necessary. During contract execution, the program manager also acts as the users agent to certify performance and approve incentive payments. Since no contract/agreement is self-regulated, the PM must accurately capture, analyze, and report sustainment related performance and cost data. PMs should periodically validate the contract business case with actual cost and performance data to ascertain if projected returns on investments are being attained and whether the basic support strategy still save the government money and should be continued.

5.1.6. Technical Data, Computer Software, and Intellectual Property Rights

5.1.6. Technical Data, Computer Software, and Intellectual Property Rights

Technical data is critical in executing a PMs life-cycle management responsibilities. Affordable product support and the ability to maximize competition require that the PSM be involved in the development and execution of the programs approach to intellectual property rights identified with the Technical Data Rights Strategy (See Chapter 2, Paragraph 2.8.7.6.) As discussed in Chapter 2, a programs Acquisition Strategy must be forward thinking with respect to intellectual property. Unless data rights considerations are considered up-front when developing an acquisition strategy, critical data and software may not be specified for delivery, rendering it unavailable (or unaffordable) years later for use on a program during its sustainment phase. For these

reasons sustainment strategies need to be considered early on in a programs life cycle.

The PSM needs to pay particular attention to the following areas of the Technical Data Rights Strategy as well as it's execution to ensure that all data and software required to successfully sustain the system is available throughout the systems life cycle:

- Data deliverables included in the RFPs and subsequent contracts
- Data rights, including the responses to the contractors data assertion lists
- The data management approach including how the data will be delivered, accessed, maintained, and protected

5.1.7. Configuration Management

5.1.7. Configuration Management

Program Managers establish and maintain a configuration control program, and are required to "base configuration management decisions on factors that best support implementing performance-based strategies throughout the product life cycle" (DoD Directive 5000.01). An effective configuration management program should include configuration control over the functional and allocated baselines as well as the physical baseline. The approach and responsibility for maintaining configuration control will depend on a number of program specific factors such as design rights, design responsibility, support concept, and associated costs and risk. Nominally the government maintains configuration control of the system design specification and retains the authority/responsibility for approving design changes impacting the system's ability to meet specification requirements. The contractor(s) has the right to access configuration data at any level required to implement planned or potential design changes and support options.

Section 4.3.7 provides additional configuration management (CM) information including useful references. In addition, the ANSI/EIA-649 National Consensus Standard for CM and corresponding handbook are key joint government/industry developed documents intended to give guidance on the development and execution of a Configuration Management Plan. These configuration management discussions generally apply to legacy programs with traditional CM programs; however, the use of performance-based product support contracts and public private partnerships necessitate DoD logisticians understand, apply and address the CM impacts as they implement the sustainment strategy. This is because if the configuration of the system is not monitored closely, design control could be lost, resulting in procuring a useless product support package. This would make it difficult to provision or ensure the proper support equipment, spares, and data are available to complete repairs, thereby adversely affecting materiel availability and increasing program costs.

The logistician's involvement in the configuration management process is vital throughout the systems life cycle. The logistics process enters into the configuration management world through support and maintenance planning, since the maintenance

plan drives the level of government configuration control and support element requirements. During the maintenance planning process, factors such as reliability and volatility of the design technology are used to determine how the system/component will be supported, e.g., throwaway or repair, and commercial or organic repair.

In commercial support strategies, it is not uncommon to delegate broad Class II (no change in form, fit, function, or testability of an item) configuration management to the product support provider. Since the provider is tasked to deliver performance outcomes with broad flexibility regarding how to provide those outcomes, it is consistent to also provide him flexibility to implement configuration changes (with government knowledge) stemming from his investments to improve reliability, availability, and repair processes that benefit both the government in terms of improved readiness and the commercial provider in terms of profit opportunities by reducing cost over the contract term.

Also, in PBL contracts, provisions should be made to protect the government in the event the contractor is unable to provide the contracted performance and at contract conclusion. Technical Data and Computer Software are important components of the configuration management process so it is vital the PM understand the level of access to Technical Data Packages (TDPs) and the appropriate levels of computer software (to include source code when necessary) required to successfully procure, compete, and sustain the system over its entire life cycle. This level will vary from system to system and often down to the component or part level. Specific clauses must be included in the contract to ensure the government retains access to or takes control of the necessary TDP(s) and software and their corresponding updates. This ensures the government will have the data necessary to duplicate the existing configuration with little to no interruption in the support provided to the user if the support provider changes or the contract is re-competed. Without this exit ramp, the government will not be able to cost effectively re-compete a system and/or component.

5.2. Applying Systems Engineering to Life-Cycle Sustainment

5.2. Applying Systems Engineering to Life-Cycle Sustainment

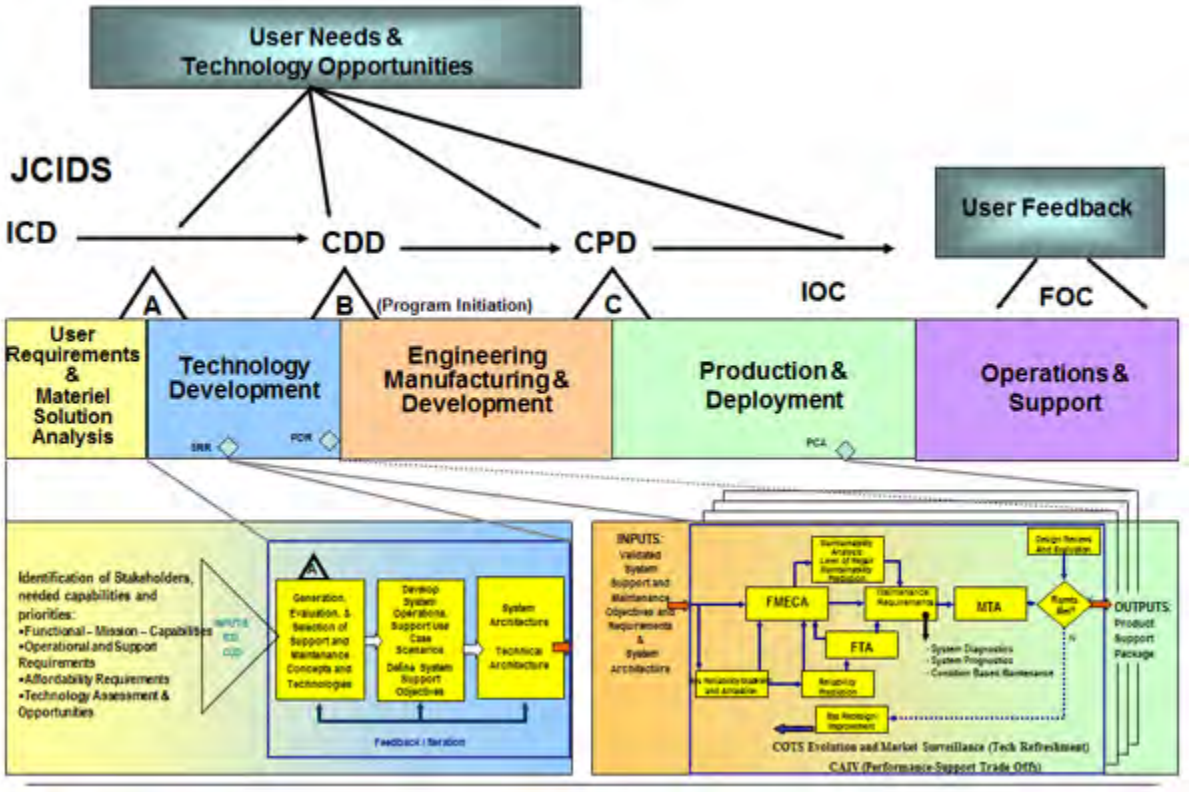
Figure 5.2.F1 depicts the Life-Cycle Management System and relates key sustainment design and systems engineering activities. (Figure 5.2.F1 provides an overview roadmap during the acquisition process. Expanded versions are shown by phase in section 5.4 .) These system engineering processes are not carried out in a strictly linear progression; they are typically carried out iteratively, expanding into lower levels of detail as the design evolves. Incremental acquisition present challenges in both acquisition and sustainment activities. An obvious challenge is the potential cost and configuration management challenges that can arise with multiple configurations of end items as well as the support system. This should be addressed early in development and evolution of the acquisition strategy. If planned correctly, configuration management efforts combined with rapid prototypes can provide the PM the opportunity to observe and evolve the success of tentative support strategies. Conversely, poor management

of multiple system configurations can create a significant sustainment burden.

Program teams manage programs "through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs" (DoD Directive 5000.01). In doing so, the PM's overriding program objective should be to maximize system effectiveness from the users perspective. To accomplish this, sustainment considerations are addressed in the JCIDS process, demonstrated in test & evaluation, and implemented by fielding and sustaining the system. To reach that objective within resource and statutory constraints, trade-offs are continually conducted to balance performance, availability, process efficiency, risks, and cost. This requires the PM to think in both long and short terms.

Short term pressures to achieve system performance and schedule imperatives are very real, and cannot be ignored in a financially and statutorily constrained environment. However, system sustainability and affordability are also important program elements to be considered. Consequently CJCS Instruction 3170.01 established the Sustainment Key Performance Parameter and KSAs to reinforce the total life-cycle approach to program decisions. This is because a system that meets performance requirements but saves acquisition dollars by not expending the resources to make it reliable, maintainable, or supportable is a liability to the user. Ultimately, over the system life cycle, balancing this composite of long term objectives will provide greater benefit.

Figure 5.2.F1. Supportability Analysis in Acquisition



Achieving Affordable System Operational Effectiveness. The PM can address the long versus short term issue by designing for the optimal balance between performance (technical and supportability), life-cycle costs, schedule, and process efficiency. A development program that targets only some categories of technical performance capability; or fails to optimize system Reliability, Availability, and Maintainability (RAM) technical performance, risks financial burden during operations and support. The PM should therefore design for the optimal balance between technical performance (including RAM), categories of LCC, schedule, and process efficiencies. The affordable system operational effectiveness concept is important because it is what the user sees in terms of how well the system is able to perform it's missions over a sustained period as well as the ability to surge given the users operating budget. In this concept the emphasis is not only on the system's ability to execute its mission or its reliability and maintainability, but also on the cost effective responsiveness of the supply chain. The challenge is in how to relate these interrelated elements into an integrated shared vision across the wide range of stakeholders. The major elements impacting a systems ability to perform its mission that should be considered in the design process are depicted in Figure 5.2.F2 and addressed below:

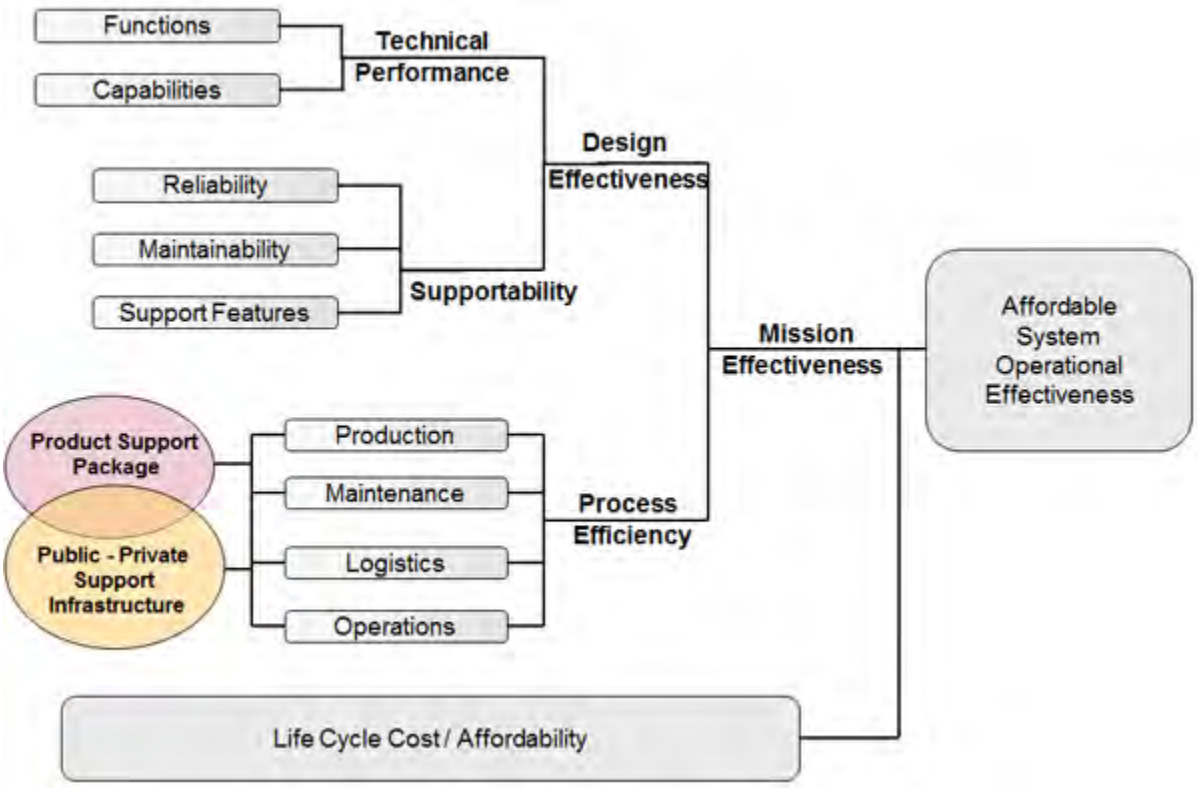
Mission effectiveness is critical because it reflects the Warfighter's ability to accomplish the mission (including the number of systems/sorties required to accomplish the mission) and directly impacts their workload. It reflects the balance achieved

between the design and the process efficiencies used to operate and support the system, including the product support package and the supply chain. In addition, each of its elements directly influences the life-cycle cost. The key is to ensure mission effectiveness is defined in terms meaningful to the Warfighter over a meaningful timeframe. (e.g., number of systems required to move X ton miles in a 30 day period, or number of systems required to provide continuous surveillance coverage over 60,000 square mile area for a 6 month period).

The design effectiveness reflects key design features - technical performance and supportability features. These system aspects should be designed-in synergistically and with full knowledge of the expected system missions in the context of the proposed system operational, maintenance, and support concepts. To be effective, technical performance and supportability objectives should be defined in explicit, quantitative, testable terms. This is important to facilitate trade-offs as well as the selection and assessment of the product and process technologies. Each of the major elements controlled by the program manager in the design process is addressed below.

Technical performance is realized through designed-in system functions and their corresponding capabilities. In this context, functions refer to the desired mission abilities the system should be capable of executing in the operational environment. This includes high level functions such as intercept, weapons delivery, electronic jamming, surveillance, etc. down to the lowest subsystem level supporting functions (e.g., process signal). Capabilities refer to the various desired performance attributes and measures, such as maximum speed, range, altitude, accuracy (e.g., "circular error probable") down to the lowest subsystem level (e.g., frequencies). Each of these must be prioritized and traded off to achieve an acceptable balance in the design process.

Figure 5.2.F2. Affordable System Operational Effectiveness



In this context, supportability (see sections 5.3 and 4.3.18.22) includes the following design factors of the system and its product support package:

- **Reliability** is the ability of a system to perform as designed in an operational environment over time without failure.
- **Maintainability** is the ability of a system to be repaired and restored to service when maintenance is conducted by personnel using specified skill levels and prescribed procedures and resources (e.g., personnel, support equipment, technical data). It includes unscheduled, scheduled maintenance as well as corrosion protection/mitigation and calibration tasks.
- **Support features** include operational suitability features cutting across reliability and maintainability and the supply chain to facilitate detection, isolation, and timely repair/replacement of system anomalies. It also includes features for servicing and other activities necessary for operation and support including resources that contribute to the overall support. Traditional factors falling in this category include diagnostics, prognostics (see CBM+ Guidebook), calibration requirements, many HSI issues (e.g. training, safety, HFE, occupational health, etc.), skill levels, documentation, maintenance data collection, compatibility, interoperability, transportability, handling (e.g., lift/hard/tie down points, etc.), packing requirements, facility requirements, accessibility, and other factors that

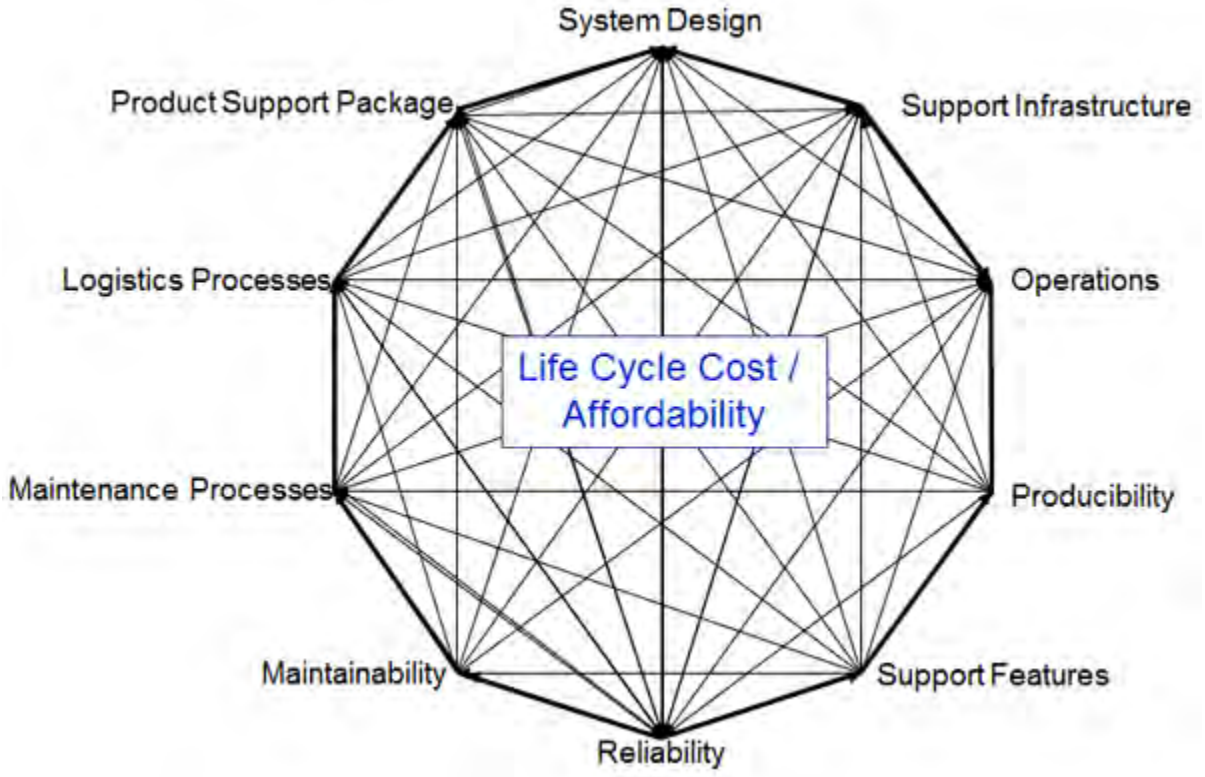
contribute to an optimum environment for sustaining an operational system.

Supportability features cannot be easily "added-on" after the design is established. Consequently supportability should be accorded a high priority early in the program's planning and integral to the system design and development process. In addition to supportability features, the associated product support package, along with the supply chain, are important because they significantly impact the processes used to sustain the system, allowing it to be ready to perform the required missions. While not specifically identified in figure 5.2.F2, producibility (i.e. the degree to which the design facilitates the timely, affordable, and optimum-quality manufacture, assembly, and delivery) can also impact supportability. This is because easily producible items are normally faster to obtain and have lower life-cycle costs.

Process efficiency reflects how well the system can be produced, operated, serviced (including fueling) and maintained. It reflects the degree to which the logistics processes (including the supply chain), infrastructure, and footprint have been balanced to provide an agile, deployable, and operationally effective system. While the program manager does not fully control this aspect, the program directly influences each of the processes via the system design and the fielded product support package. Achieving process efficiency requires early and continuing emphasis on the various logistics support processes along with the design considerations. The continued emphasis is important because processes present opportunities for improving operational effectiveness even after the "design-in" window has passed via lean-six sigma, supply chain optimization and other continuous process improvement (CPI) techniques. Examples of where they can be applied include supply chain management, resource demand forecasting, training, maintenance procedures, calibration procedures, packaging, handling, transportation and warehousing processes.

The relationships illustrated in figure 5.2.F2 are complex and not as clean as shown in the figure. Figure 5.2.F3 is more accurate relative to how the basic system operational effectiveness elements interface. For example, each of the supportability elements influences the process aspects which in turn can impact supportability. (e.g., while reliability drives the maintenance requirements, the implemented maintenance processes and the quality of the spare and repair parts as reflected in the producability features can impact the resultant reliability.) In addition, how the system is operated will influence the reliability and both can be influenced by the logistic processes. Last but not least, each of the design and process aspects drives the life-cycle costs. Achieving the optimal balance across these complex relationships requires proactive, coordinated involvement of organizations and individuals from the requirements, acquisition, logistics, and user communities, along with industry. Consequently, because of the complexity and overlapping interrelationships full stakeholder participation is required in activities related to achieving affordable mission effectiveness. Models that simulate the interactions of the elements, as depicted in Figure 5.2.F3, can be helpful in developing a balanced solution.

Figure 5.2.F3. Affordable System Operational Effectiveness Interrelationships



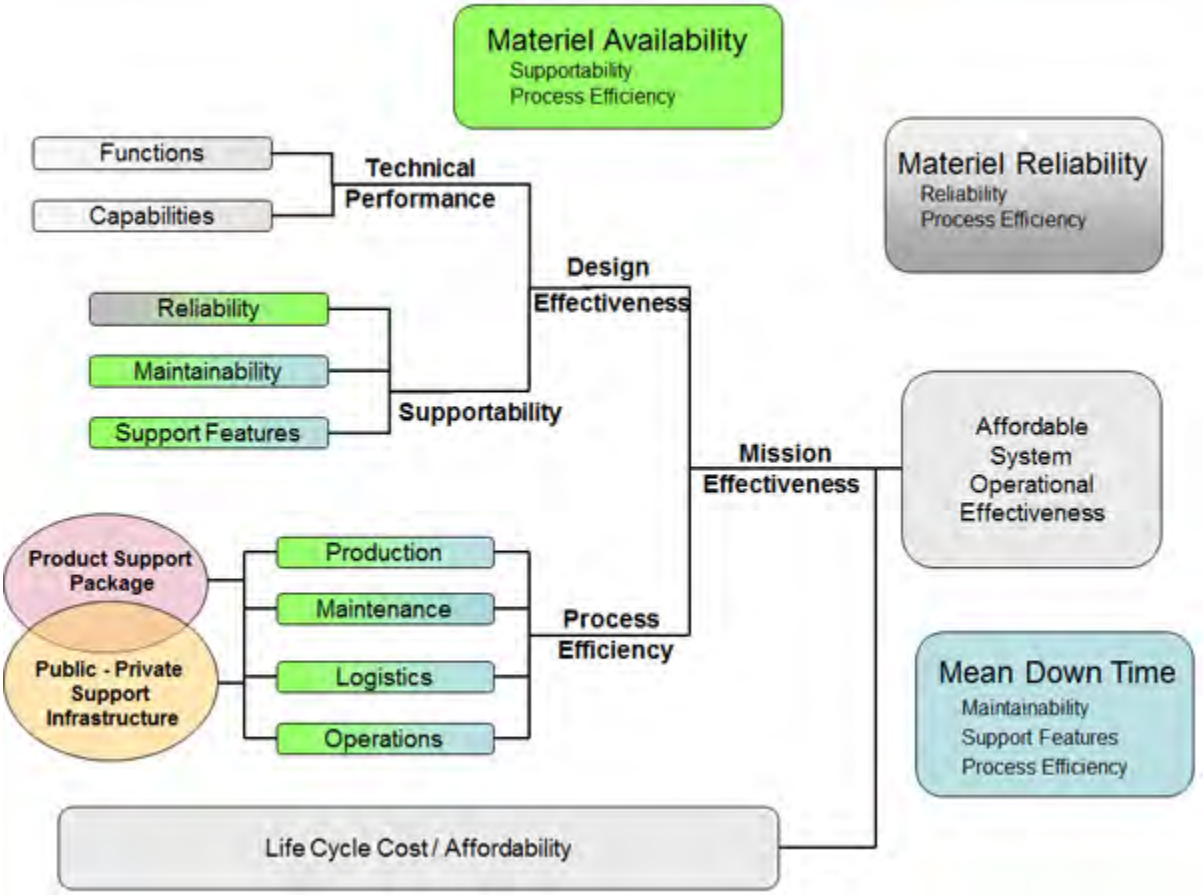
Each of the elements reflected in Figure 5.2.F2 contribute to achieving the top level affordable operational effectiveness outcome and have associated metrics which can be measured to assess efficiency and effectiveness. However, they don't mathematically add up as implied in Figure 5.2.F2. This is because, in addition to the complex interrelationships between the elements, the various stakeholders only measure portions of the supply chain and often use different metric definitions. Consequently DoD has adopted 4 key sustainment metrics (including the Sustainment KPP and 2 KSAs) for projecting and monitoring key affordable operational effectiveness performance enablers to:

- Provide a standard set of encompassing measures to continuously estimate and assess affordable operational effectiveness
- Complement the traditional readiness metrics to help overcome the overlapping interrelationships,
- Provide a common communications link across the diverse systems and organizations
- Provide the programs latitude in determining the optimum solution.

Figure 5.2.F4 indicates the minimum set of sustainment metrics the PM should use to facilitate communication across the stakeholders and the elements affecting them. The color code indicates the elements measured by Materiel Availability, Materiel Reliability

and Mean Down Time metrics. The metrics are interrelated and along with the CONOPS impact the LCC.

Figure 5.2.F4 Sustainment Metrics & Affordable System Operational Effectiveness



This overarching perspective provides context for the trade space available to a PM and for articulation of the overall objective of maximizing the operational effectiveness. This is critical because trade-offs outside the trade space (i.e., program parameter changes) can require approval of both the Milestone Decision Authority and Validation Authority since validated KPP threshold values cannot be reduced without Validation Authority approval. Consequently, it is critical the design trade space established by the values selected for the sustainment metrics are established early and be acceptable to the user and acquirer communities. As a result, the user and sponsor should be involved with the determination of the design trade space. Finally, to help ensure the metrics goals are met, the program should establish supporting metrics for key drivers (e.g., logistics footprint, manning levels, ambiguity rates for diagnostics) uniquely tailored for the system and the projected operating environment as the design requirements are allocated.

5.2.1. Supportability Analysis

Sustainment requirements should be an integral part of the systems engineering design process. (A detailed discussion of the systems engineering process can be found in section 4.3.) Regardless of the life-cycle phase, effective supportability begins with the development of sustainment requirements to drive the design and development of reliable, maintainable and affordable systems through the continuous application of the systems engineering methodology focusing on affordable system operational effectiveness. The key is to smoothly integrate the systems engineering processes and design maturation processes together with the Defense Life-Cycle Management System and it's milestones. A key product of the supportability analysis is the maintenance plan which evolves and drives all sustainment resource requirements throughout the life cycle.

5.2.1.1. Supportability Analysis Phases

Section 5.4 provides areas of focus for each acquisition phase. In general, however, life-cycle management can be thought of in terms of three broad periods.

- **Pre-Systems Acquisition:** Determining the capabilities and major constraints (cost, schedule, available technology) that frame the acquisition strategy and program structure for both the system and its support concept
- **Acquisition:** Designing, producing and deploying the equipment and it's support system
- **Operations:** Adjusting to the operational environment by assessing readiness trends/issues, cost trends, evolving materiel conditions, and taking timely corrective actions to support the users

Pre-Systems Acquisition: Here, supportability analysis should be used to evaluate the suitability of material alternatives, shape life-cycle sustainment concepts and determine the product support capability requirements. Each alternative should be assessed to determine the likely materiel availability and it's life-cycle affordability. Generally the analysis starts at the system level but can selectively go to lower levels of indenture if key enabling technologies are required to meet the CONOPS (for both the system and the product support system). This includes using supportability analysis to:

- Evaluate alternatives until an optimum balance is achieved between mission effectiveness and the KPPs (including the Sustainment KSAs). Specifically it

should be used to ensure the preferred System Concept & Support CONOPS, are consistent with the projected Operational CONOPS taking into account "real world" constraints including "core", statutory requirements, existing supply chain, etc. Generally this is done by considering the sustainment effectiveness and O&S affordability of systems currently performing the same or similar capabilities. These are analyzed and serve as benchmarks to assess alternatives; with the intent of incremental improvement over current (legacy) system capability readiness and cost.

- Evaluate product support capability requirements using a notional Support CONOPS for trades and LCC estimates in evaluating the alternatives.
- Identify enabling sustainment technology needed to meet life-cycle sustainment goals especially when the risk of achieving the incremental improvements is high (e.g., a robust software architecture, health management, diagnostics, prognostics. etc.).
- Assess the operational and life-cycle risks associated with sustainment technologies, especially those requiring development.
- Assess the intellectual property considerations needed, to include the technical data rights and computer software needed to sustain and support a system.
- Integrate supportability performance into systems engineering, initial acquisition strategic planning, and as benchmark criteria for test and evaluation.
- Refine associated performance requirements based on technology development results (positive and negative) to achieve the preferred system concept & Support CONOPS.
- Refine supportability performance requirements and life-cycle sustainment concepts, based on evolving technology and changes in the CONOPS.

Acquisition: Here, supportability analysis helps reduce risks and create/field the system and its supply chain with provided feedback into the design process. This is accomplished by assessing the effect of system plans, development, and production on sustainment effectiveness, readiness, and O&S affordability. The intent is to act early to mitigate evolving circumstances that may adversely impact deployed readiness. This includes using systems engineering in designing the system and its supply chain; producing both concurrently; and testing to verify the total system requirements have been achieved. Specifically systems engineering is used in designing for support and:

- Taking Warfighter requirements (Including the Operational CONOPS) and developing the sustainment objectives, Support and Maintenance CONOPS and determining their detailed "design-to" and "build to" requirements. (It also includes identifying the performance requirements for the supporting supply chain segments to support the Operational CONOPS.) In accomplishing this, the trades/analyses are used to identify:
    - The key metric values (e.g., the drivers) required to meet the operational/campaign model assumptions/requirements as well as the impact on Warfighter mission capability (e.g., ability to generate a mission (operational readiness) and perform during a mission) of the various trades.

    - LCC drivers for the system, it's support concept and maintenance concept/plan.
    - The optimum mix of driver values to meet KPPs and their corresponding confidence levels.
    - Effectiveness (KPP/KSA Outcomes) if the supply chain performs at today's levels (as well as if current trends continue or with anticipated trends).
- Taking the test/initial operations results and predicting likely mature values for each of the KSA and enabler drivers.
- Providing integrated Sustainment KPP/KSA estimates into the Defense Acquisition Management Information Retrieval (DAMIR) system.

During this period more realistic and detailed data is used in the models/simulations to reduce risk and define achievable performance & sustainment requirements. Consequently, a mix of design estimates/contract requirements, sustainment, and Maintenance Plan metrics are used when conducting sustainment trades/analysis depending on the period and objective. In addition, expected trends for system, enabler & supply chain metrics and their confidence levels are also needed requiring the use of data models. This requires that:

- Data realism is based on systems engineering/technology assessments.
- Metric values can be evaluated and re-adjusted as necessary.
- The required data elements performance requirements can be defined in contract terms.
- There is a means to verify the maturity growth over time.

Operations: Here, supportability analysis is used to help in adjusting the program based on the sustainment program's achieved effectiveness as well as on changing hardware and operational conditions. This includes using supportability analysis to:

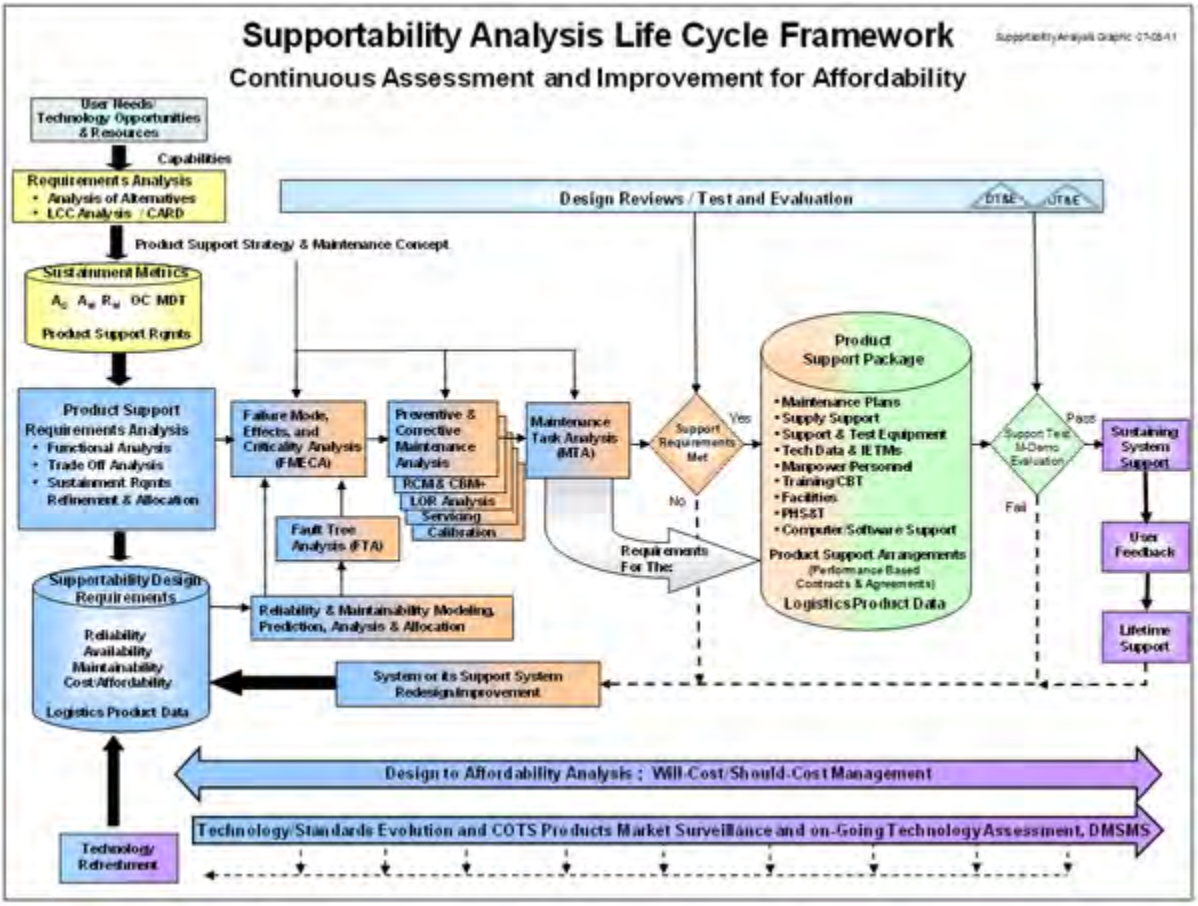
- Analyze the impact of proposed re-design alternatives on the sustainment metrics and mission effectiveness.
- Analyze the impact of proposed process changes on the sustainment metrics.
- Take use data and user feedback including Failure & Discrepancy Reports to:
    - Project trends (with confidence levels) so proactive actions are taken as conditions warrant to minimize adverse impacts on the users.
    - Identify areas in the supply chain where performance is adversely affecting materiel availability, increasing LCC or missing areas of potential savings/improvements. (Note, that care is needed, since, in some cases, an increase within a specific system may be significantly offset by a major saving elsewhere within the DoD Component or DoD. Consequently, higher level organizations may have to be engaged in the final decision.)
    - Identify and analyze readiness risk areas and develop corrective action alternatives.
- Relate/quantify various business process outcomes with resources.

During this period, the system program measures and tracks the supply chain and its effectiveness and use models that include the driver metrics to determine root causes of problems or anticipate future problems.

5.2.1.2. Supportability Analysis Steps

As discussed in section 4.3.18 , designing for optimal system affordability and operational effectiveness requires balance between mission effectiveness and life-cycle cost. The emphasis is not only on the reliability and maintainability of the system to achieve mission capability, but also on human systems integration and optimization of all human interfaces across the HSI domains to ensure the cost-effective responsiveness and relevance of the support systems and supply chain. This is critical since a significant portion of LCC are human related and are locked in early in the acquisition life cycle. Consequently it is important that a comprehensive HSI program be initiated early in the life cycle to address the major LCC drivers. These objectives can best be achieved through integration with the system design and CONOPS (both operational and sustainment) and by focusing on the sustainment requirements. As depicted in Figure 5.2.1.2.F1, the supportability analysis process is most effectively carried out through inclusion from the very beginning of a program, starting with the definition of required capabilities. The colors in the figure provide a rough idea as to the life-cycle phase in which specific tasks are conducted. However, in reality, the time Supportability Analysis phasing for a specific piece of hardware is really dependent on the maturity of the design process, not strictly based on the programs milestone reviews.

Figure 5.2.1.2.F1. Supportability Relationships



Implementation of a disciplined supportability analysis approach, including systems engineering activities such as CBM+, Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Reliability Centered Maintenance (RCM) (see Enclosure 3, DoDI 4151.22 RCM Process), and level of repair analysis (considering cost and availability implication of the maintenance level and locations) will produce a Maintenance Task Analysis (MTA) directly linked to the systems reliability and maintainability characteristics. The Maintenance Task Analysis is the opportunity to determine whether the design has met the supportability requirements defined in the system specification, and provides a feedback loop to the Systems Engineer that is either positive (design has met requirements) or that there is a need for re-evaluation of either the requirement or the design itself. The results of the re-evaluations permit's the trade space required for the PM to make a justifiable decision. The RCM analytical process which determines the preventive maintenance tasks is critical in providing recommendations for actions necessary to maintain a required level of safety, maximize materiel availability, and minimize operating cost. In addition to DoD Component guides and handbooks (e.g. MIL-P-24534A), SAE JA1011 (Evaluation Criteria for RCM Programs) and SAE JA1012 (A Guide to the RCM Standard) are illustrative commercial

standards for this method.

The technical input and maintenance task analysis provide a detailed understanding of the necessary logistics support element requirements to sustain required materiel availability. The MTA process identifies support tasks and the physical location where they will be accomplished considers the costs, availability implications, and statutory requirements. (The Depot Source of Repair (DSOR) process is key in determining location.) This in turn produces a product support package that identifies support element requirements and associated product data based on the system reliability and maintainability. The product support package provides descriptions of the following topics:

- Supply Support (Spare/Repair Parts)
- Maintenance Plan and Requirements
- Support, Test & Calibration Equipment
- Technical Data (Paper Based and/or Electronic Interactive)
- Manpower & Training including Computer Based Training
- Facility Requirements
- Packaging, Handling, Storage, & Transportation
- Computer Resource Support

The steps shown in figure 5.2.1.2.F1 are not necessarily carried out in a linear progression. Design increments and the continuous assessment of test results and in-service system performance will identify needs for system improvements to enhance reliability, and maintainability and to overcome obsolescence, corrosion, or other sustainment problems. Additional information including a detailed process description, considerations in implementing the process and data element definitions, can be found in MIL-HDBK-502 . (**Note:** This document is currently in the update process.)

5.2.1.3. Key Depot Maintenance Analysis Elements

Program managers should analytically determine the most effective levels of maintenance and sources based on materiel availability and cost factors. 10 U.S.C. 2464 and DoD policy require organic core maintenance capabilities be in place to provide effective and timely response to surge demands and to ensure cost efficiency and technical competence. In addition per 10 USC 2464, core sustaining workload must be accomplished in Government owned facilities with Government owned equipment and personnel. The PM should perform an analysis to determine the maintenance source that complies with statutory requirements, operational readiness and best value for non-core workloads. (Initial organic depot maintenance source of repair assignments must employ merit-based selection procedures to select among alternative sources. Depot maintenance workloads previously accomplished at organic facilities, with a value of at least three million dollars, must also be subjected to merit-based selection procedures when deciding between alternative organic sources of repair. Additional information including exceptions to the requirement can be found in DoDD 4151.18 and

DoD Instruction 4151.20 .)

Core Logistics Capability. Title 10 U.S.C. 2464 and DoDI 4151.20 require core logistics capability that is government-owned and government-operated (including government personnel and government owned and operated equipment and facilities) to ensure a ready and controlled source of technical competence with the resources necessary to ensure effective and timely response to mobilization, national defense contingency situations, or other emergency requirements. These capabilities must be established no later than 4 years after achieving IOC. These capabilities should include those necessary to maintain and repair systems and other military equipment that are identified as necessary to fulfill the strategic and contingency plans prepared by the Chairman of the Joint Chiefs of Staff. (Excluded are special access programs, nuclear aircraft carriers, and commercial items, as defined by (Title 10 U.S.C. 2464).) Core logistics capabilities should be performed at government owned-government operated (GO-GO) facilities of a military department. Such facilities should be assigned sufficient workload to maintain these core capabilities and ensure cost efficiency and technical competence in peacetime while preserving the surge capacity and reconstitution capabilities necessary to fully support strategic and contingency plans.

Depot Source of Repair (DSOR) Analysis. The process to help the PM select the best value in depot maintenance support is implemented through the Depot Source of Repair (DSOR) analysis. The Depot Source of Repair Guide provides additional information for accomplishing the required Core Logistics Analysis/Source of Repair Analysis in determining the source of repair for depot level workload. The DSOR decision process is an integral part of sustainment planning and mandatory for systems/equipment requiring depot maintenance. DoD Directive 4151.18 , Maintenance of Military Materiel, requires DSOR assignments be made by the PM using the DSOR assignment decision logic. The process should be completed before entering into firm commitments or obligating funds for other than interim depot support. The DSOR decision is typically made during the Engineering & Manufacturing Development and the Production and Deployment phases.

The DSOR decision process consists of two major elements, normally performed sequentially: The first is the organic versus contract source of repair determination. This determination is made by the PM using a DoD Component approved analysis process that gives consideration to core requirements. Title 10 USC 2464 , Core Logistics Capabilities; Title 10, USC 2466 , Limitations on the Performance of Depot Level Maintenance of Materiel, and DoD Directive 4151.18 provide further guidance for this process.

The second element in the DSOR decision process is consideration of interservice depot maintenance support. This element, known as the Depot Maintenance Interservice (DMI) review, is required regardless of the outcome of the contract versus organic selection. The DMI review is prescribed in the Joint Depot Maintenance Program regulation Logistics, Joint Depot Maintenance Program with individual DoD Component details spelled out in OPNAVINST 4790.14A, AMC-R 750-10, AFI 21-

133(I), MCO P4790.10B, and DLAD 4151.16 . All new acquisitions, equipment modifications, and items moving to or from contract depot maintenance support are to be reviewed for interservice potential in accordance with this regulation.

The DSOR decision process has the potential to reduce program costs by effectively using commercial and organic depot maintenance resources. The process helps ensure the DoD Components maintain the core depot maintenance capability, as required by statute that meets military contingency requirements and considers interservice depot maintenance support and joint contracting. In performing this analysis, the PM should ensure that maintenance source of support decisions comply with the following statutory requirements.

Depot Maintenance 50 Percent Limitation Requirement. Title 10 U.S.C. 2466 requires not more than 50 percent of the funds made available in a fiscal year to a military department or defense agency for depot level maintenance and repair workload as defined by Title 10 U.S.C. 2460 be used to contract for performance by non-federal government personnel. As this is a military department and agency level requirement and not a system specific requirement, the PM should not undertake depot maintenance source of support decisions without consultation with accountable military department logistics officials to get the DoD Component position on this statutory requirement.

5.2.2. Life-Cycle Costs (LCC) and Product Support Business Case Analysis (BCA)

5.2.3. Sustainment Modeling and Simulation (M&S)

5.2.4. Process Models

5.2.2. Life-Cycle Costs (LCC) and Product Support Business Case Analysis (BCA)

LCC is the cost to the government to acquire and own a system over it’s useful life. LCC includes all life-cycle management costs (e.g. development, acquisition, operations, support, and disposal). As such it consists of the elements of a program's budget, as well as supply chain or business processes costs that logically can be attributed to the operation of a system. Section 3.1.5 provides additional information but generally LCC includes direct program costs as well as any allocable "indirect cost" elements. This can include such costs as delivering fuel/batteries, recruiting/ accession training of new personnel, individual training, environmental and safety compliance, management headquarters functions, etc.

Early program decisions ultimately determine and drive the LCC, the majority of which is incurred after a system is deployed. Consequently beginning with the requirements determination and during each life-cycle phase, LCC estimates should play a major role in the program decision process for evaluating affordable alternatives during the design and trade-off processes. (See DoD Directive 5000.01, E1.1.4, E1.1.17, and E1.1.29 .) As a result, the operating and support portion of the LCC is now treated as a military requirement via the JCIDS's Ownership Cost KSA. For this reason, LCC analysis should

be performed to the level appropriate for the decision and alternatives considered. However, since projections are based on assumptions, cost estimates shall include an assessment of confidence levels and should also include the associated cost drivers.

The Product Support Business Case Analysis (BCA) is used to assist in identifying the product support strategy that achieves the optimal balance between Warfighter capabilities and affordability. (Other names for a BCA are Economic Analysis, Cost-Benefit Analysis, and Benefit-Cost Analysis. Regardless of the name, is it a structured analytical process that aids decision making in identifying and comparing alternatives by examining the mission and business impacts (both financial and non-financial), risks, and sensitivities.) The PSM should prepare a Product Support BCA for major product support decisions, especially those that result in new or changed resource requirements. The BCA should consider organic and commercial alternatives when determining the optimal support solution (e.g. DLA, TRANSCOM, Service activities and commercial options). Each of the key stakeholders should be informed of the BCA process and support the analysis by providing the information needed to make an informed decision. To aid this process, the Product Support BCA Guidebook provides an analytic, standardized, and objective foundation upon which credible decisions can be made.

In general, traditional life-cycle cost estimates are adequate in scope to support decisions involving system design characteristics, with indirect cost elements being handled via standard cost factors/surcharges/burdened rates. However, in special cases depending on the issue, the broader perspective may be more appropriate than just the traditional life-cycle cost elements a program can directly influence. For example, when determining the materiel solution to meet requirements (e.g., manned vs. unmanned, or space based vs. ship based, etc.) cost elements dealing with the supply chain will need to be considered since each materiel solution has a significantly different cost impact to the tax payer. During the design and sustainment phases, indirect cost elements may also be broken out rather than using cost factors when considering decisions directly impacting the wholesale logistics infrastructure processes. Examples of these types include decisions dealing with required skill levels to maintain the system, alternative system support concepts and strategies, reengineering of business practices or operations, and competitive sourcing of major supply chain activities.

Life-cycle cost analysis can be very effective in reducing the LCC of the system and its support strategy. (Within DoD, reduction and control of LCC is also done through a variety of initiatives including Will-Cost and Should-Cost Management, etc.) However, one cost model is not sufficient to address all of the alternatives a PM must consider. The level of detail, analysis process used, and LCC elements considered should be tailored to the decision being made, focusing on cost drivers and costs that will be incurred by the government and not just on direct program office costs. The objective is to seek and eliminate low-value added ingredients of program costs.

For most decisions, the sunk costs, costs that will not be impacted by the alternatives

and absolute value of the alternatives can be ignored. The analysis should be focused instead on the relative cost element differences between the alternatives considered and the cost drivers for each. Consequently, the cost analysis should include appropriate key performance measure, such as O&S cost-per-operating-hour, cost-per-pallet miles, cost-per-seat miles, etc., when assessing alternative solutions. The Cost Analysis Requirements Description (see section 3.4.4.1) reflects the life-cycle sustainment requirements for preparing the LCC estimate and the Cost Analysis Improvement Group Operating and Support Cost Estimating Guide also provides useful information relative to the cost estimating process, approach, and other considerations.

5.2.3. Sustainment Modeling and Simulation (M&S)

M&S can be an effective tool in the supportability analysis and evaluation process in implementing life-cycle management principles because all the sustainment/materiel readiness driver metrics can be considered in parallel (also see section 4.3.19.1). Consequently, the sustainment M&S objective should be to use validated models to consider materiel availability/readiness implications when assessing the merits of alternatives throughout the life cycle. M&S should be used in assessing the alternatives for major decisions affecting the design and deployment of both the end item and it's support system. Properly applied M&S encourages collaboration and integration among the varied stakeholders (including the test and transportation communities) facilitating materiel availability and system effectiveness.

The models should be used throughout the life cycle and should include the multiple materiel availability stakeholder contribution and funding streams for the supply chain components. (The level of detail used varies based on several factors including, but not limited to, the systems complexity, criticality to the user, program phase, and risk.) In all cases, M&S efforts should consistently and credibly look at/trade off life-cycle alternatives in a repeatable fashion. In addition, the underlying assumptions and drivers for the values of each of the sustainment metrics should be documented as thresholds, objectives, and estimates evolve through the life cycle. (See the RAM-C Guide for additional information.)

5.2.4. Process Models

M&S and continuous process improvement initiatives are dependent on defined processes. The government and industry have undertaken a series of initiatives to define generic multi-level processes with associated metrics that might prove useful when developing new analysis models. The following general models have been developed.

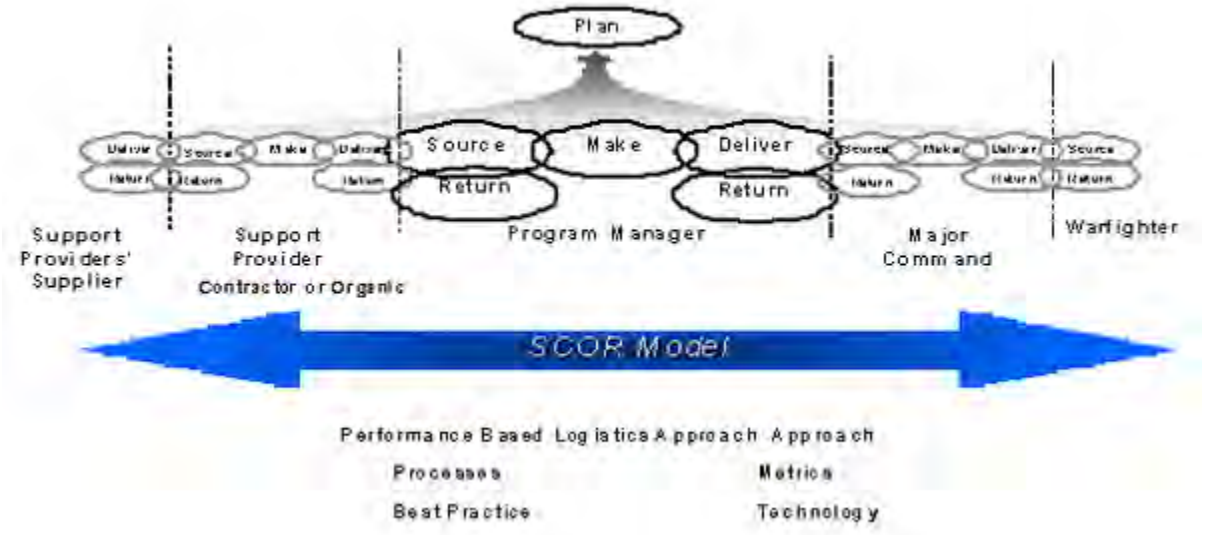
The Supply Chain Operations Reference (SCOR) model, figure 5.2.4.F1, captures a consensus view of the supply chain plan, source, maintain/make, deliver, and return, processes in a framework linking business process, metrics, best practices, and technology features into a unified structure for effective supply chain management and for improving related supply chain activities. In this context, the supply chain includes

the transportation and maintenance chains as well as the spare/repair parts chain required to provide the user flexible and timely materiel support during peacetime, crises, and joint operations. Most of these supply chain activities are governed by DoD regulation 4140.1-R, Supply Chain Materiel Management Regulation which provides further DoD guidance and information. Maintenance requirements within the supply chain are governed by DoD Directive 4151.18 , Maintenance of Military Materiel.

Building off the SCOR efforts, the **Design Chain Operations Reference (DCOR)** model links business process, metrics, best practices and technology features into a unified structure to support communication among design chain partners and to improve the effectiveness of the extended supply chain. The model is organized around five primary management processes which focus on product development and research & development. As is in the case of SCOR, this consensus model can be used to describe design chains can be simple or complex using a common set of definitions.

The **Customer Chain Operations Reference (CCOR)** model captures a consensus view of the feedback processes including the health and welfare of the customer supplier relationship. This model is the least mature and also undergoing refinement by practitioners. However, combined and tailored, the 3 models can provide an end to end view of the entire enterprise wide process covering processes, activities and metrics.

Figure 5.2.4.F1. The Supply Chain Operations Reference (SCOR) Model



5.3. Supportability Design Considerations

Logistics Infrastructure and Footprint Reduction. Programs can best support evolving military strategy by providing forces with the best possible system capabilities while minimizing the logistics footprint. Consequently, programs are responsible for achieving program objectives throughout the life cycle while minimizing cost and logistics footprint (see DoD Directive 5000.01, E1.17 and E1.29). To achieve these goals, the support posture of a system needs to be designed-in up front (i.e., logistics and availability degraders are designed out) since the opportunities for decreasing the logistics footprint decline significantly as the system evolves from design to production to deployment. Minimizing the logistics footprint through deliberate and integrated logistics/engineering design efforts means that a deployed system will require fewer quantities of support resources especially:

- Spares and the supply chain
- Test, support and calibration equipment
- Manpower and personnel requirements (including highly specialized or unique skill/ training requirements)
- System documentation/technical data

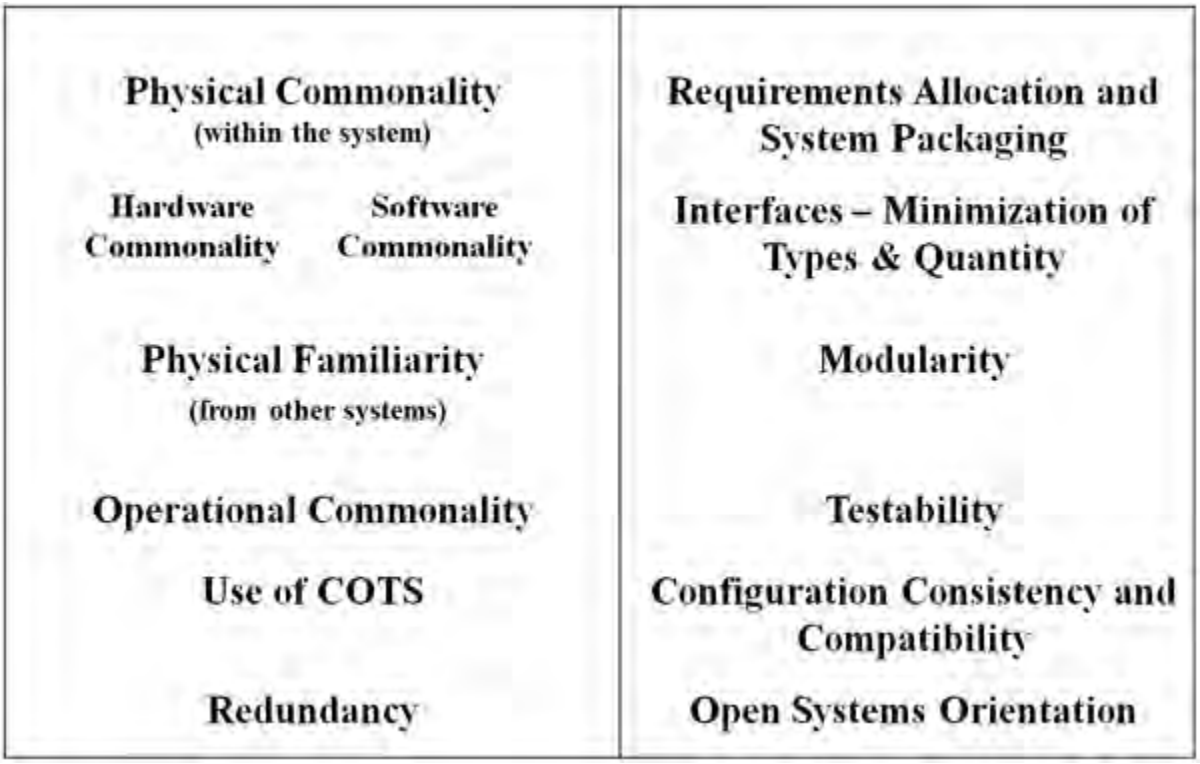
Sustainment analyses should include a basic understanding of the concept of operations, system missions, mission profiles, and system capabilities to understand the rationale behind functional and performance priorities. Understanding the rationale paves the way for decisions about necessary tradeoffs between system performance, availability, and LCC, with impact on the cost effectiveness of system operation, maintenance, and logistics support. There is no single list of sustainment considerations or specific way of grouping them as they are highly inter-related. They range from: compatibility, interoperability; transportability; reliability; maintainability; manpower; human factors; safety; natural environment effects (including occupational health; habitability); diagnostics & prognostics (including real-time maintenance data collection); and corrosion protection & mitigation. The following are key considerations that should be considered for the System Specification.

5.3.1. Architecture Considerations

Figure 5.3.1.F1 lists key system architecture attributes which can provide a solid

sustainment foundation. The focus on openness, modularity, scalability, and upgradeability is critical to implementing an incremental acquisition strategy. In addition, the architecture attributes that expand system flexibility and affordability can pay dividends later when obsolescence and end-of-life issues are resolved through a concerted technology refreshment strategy. However trade-offs are required relative to the extent each attribute is used as illustrated in the Commercial Off-the-Shelf (COTS) case.

Figure 5.3.1.F1. Illustrative attributes for System Architecture Supportability Assessments



Maturity and use of Commercial Off-the-Shelf (COTS) Items . Technology risk should receive consideration as the system is developed. Maximum use of mature technology (including non-developmental and/or standards based COTS software or computer hardware) provides the greatest opportunity to adhere to program cost, schedule, and performance requirements by leveraging industry's research & development and is consistent with an incremental acquisition approach. However, this is not a one-time activity. Unanticipated changes and the natural evolution of commercial items may drive reconsideration of engineering decisions throughout the life cycle. In addition, the program must consider the logistics implications of supporting commercial items in a military environment. Finally, because COTS items have a relatively short manufacturing life, a proactive diminishing manufacturing sources and material shortages / obsolescence approach should also be considered. Consequently, care must be taken to assess the long term sustainability of COTS options and to avoid

or minimize single source options.

Modular Open Systems Approach (MOSA) . Open system architectures help mitigate the risks associated with technology obsolescence and promote subsequent technology infusion. MOSA can also help to provide interoperability, maintainability, and compatibility when developing the support strategy and follow-on logistics planning for sustainment. It can also enable continued access to cutting edge technologies and products and prevent being locked into proprietary technology. Applying MOSA should be considered as an integrated business and technical strategy when examining alternatives to meet user needs. PMs should assess the feasibility of using widely supported commercial interface standards in developing systems. Closely related to MOSA is the Open System Architecture (OSA) approach to software development. This concept, which relies upon the sharing of software code can significantly enhance affordability. For a detailed discussion of OSA see the Open Systems Architecture Guide (insert hyperlink here to the Guide and BCA). MOSA should be an integral part of the overall acquisition strategy to enable rapid acquisition with demonstrated technology, incremental and conventional development, interoperability, life-cycle sustainment, and incremental system upgradeability without major redesign during initial procurement and re-procurement.

Standardization . Parts management is a design strategy that seeks to reduce the number of unique, specialized, and defined problem parts used in a system (or across systems) to enhance standardization, commonality, reliability, maintainability, and supportability. In addition to reducing the need and development of new logistics requirements (e.g. documentation, spares, etc.) it reduces the logistics footprint and also mitigates parts obsolescence occurrences due to diminishing manufacturing sources and material shortages.

Materiel and Interoperability/Joint Architecture. The Materiel and Interoperability/Joint Architecture concept can be used to help reduce the logistics footprint. (For further discussion on this topic see Chapter 7 .)

5.3.2. Reliability

Reliability is critical because it contributes to a systems war fighting effectiveness as well as it's suitability in terms of logistics burden and the cost to fix failures. For each system, there is a level of basic reliability that must be achieved for the system to be militarily useful, given the intended CONOPS. Reliability is also one of the most critical elements in determining the logistics infrastructure and footprint. Consequently, system reliability should be a primary focus during design (along with system technical performance, functions, and capabilities). The primary objective is to achieve the necessary probability of mission success and minimize the risk of failure within defined availability, cost, schedule, weight, power, and volume constraints. While performing such analyses, trade-offs should be conducted and dependencies should be explored with system maintainability and integrated with the supportability analysis that addresses support event frequency (i.e. Reliability), event duration and event cost. Such

a focus will play a significant role in minimizing the necessary logistics footprint, while maximizing system survivability and availability.

The requirements determination process offers the first opportunity to positively influence a system from a reliability perspective. Trade-offs among "time to failure," system performance, and system life-cycle cost are necessary to ensure the correct balance and to maximize materiel availability. Options that should be considered and implemented to enhance system reliability and achieve the Materiel Reliability KSA include:

- Over-designing to allow a safety margin;
- Redundancy and/or automatic reconfiguration upon failure allowing graceful degradation;
- Fail safe features (e.g., in the event of a failure, systems revert to a safe mode or state to avoid additional damage and secondary failures). Features include real time reprogrammable software, or rerouting of mission critical functions during a mission;
- Calibration requirements; and
- Reliability Growth Program.

Reliability estimates evolve over time. Generally, the initial estimates are based on parametric analyses and analogies with like or similar systems operating in the same environment and adjusted via engineering analysis. As the design evolves and as hardware is prototyped and developed, the engineering analysis becomes more detailed. In addition to estimates and modeling, testing at the component, subsystem, or system level may be necessary to assess or improve reliability. Approaches such as accelerated life testing, environmental stress screening, and formal reliability development/growth testing, should be considered and incorporated into program planning as necessary. To assure the delivery of a system that will achieve the level of reliability demanded in field use, a methodical approach to reliability assessment and improvement should be a part of every well-engineered system development effort. The Reliability Availability and Maintainability (RAM) Guidance provides a structure, references, and resources to aide in implementing a sound strategy. It is crucial the reliability approach be planned to produce high confidence the system has been developed with some margin beyond the minimum (threshold) reliability. This will allow for the inevitable unknowns that result in a decrease between the reliability observed during development and that observed during operational testing and in-service. In addition to reliability, the Reliability, Availability, Maintainability & Cost (RAM-C) Rationale Report Manual provides guidance in how to develop and document realistic sustainment Key Performance Parameter (KPP)/Key System Attribute (KSA) requirements with their related supporting rationale; measure and test the requirements; and manage the processes to ensure key stakeholders are involved when developing the sustainment requirements.

5.3.3. Maintainability

The design emphasis on maintainability is to reduce the maintenance burden and supply chain by reducing the time, personnel, tools, test equipment, training, facilities and cost to maintain the system. Maintainability engineering includes the activities, methods, and practices used to design minimal system maintenance requirements (designing out unnecessary and inefficient processes) and associated costs for preventive and corrective maintenance as well as servicing or calibration activities. Maintainability should be a designed-in capability and not an add on option because good maintenance procedures cannot overcome poor system and equipment maintainability design. The primary objective is to reduce the time it takes for a properly trained maintainer to detect and isolate the failure (coverage and efficiency) and affect repair. Intrinsic factors contributing to maintainability are:

- **Modularity:** Packaging of components such that they can be repaired via remove and replace action vs. on-board repair. Care should be taken not to "over modularize" and trade-offs to evaluate replacement, transportation, and repair costs should be accomplished to determine the most cost effective approach.
- **Interoperability:** The compatibility of components with standard interface protocols to facilitate rapid repair and enhancement/upgrade through black box technology using common interfaces. Physical interfaces should be designed so that mating between components can only happen correctly.
- **Physical accessibility:** The designed-in structural assurance that components requiring more frequent monitoring, checkout, and maintenance can be easily accessed. This is especially important in Low Observable platforms. Maintenance points should be directly visible and accessible to maintainers, including access for corrosion inspection and mitigation.
- **Designs that require minimum preventative maintenance** including corrosion prevention and mitigation. Emphasis should be on balancing the maintenance requirement over the life cycle with minimal user workload.
- **Embedded training and testing** , with a preference for approved DoD Automatic Test Systems (ATS) Families when it is determined to be the optimal solution from a LCC and Materiel Availability perspective.
- **Human Systems Integration (HSI)** to optimize total system performance and minimize life-cycle costs. (For further discussion, see Chapter 6 and section 4.3.18.10 .) This includes all HSI domains (Manpower, Personnel, Training, Human Factors Engineering, Environment, Safety, Occupational Health, Survivability, and Habitability) to design systems and incorporate technologies that require minimal manpower, provide effective training, can be operated and maintained by users, are suitable (habitable and safe with minimal environmental and occupational health hazards), and survivable (for both the crew and the equipment).

Condition Based Maintenance Plus. When it can support the materiel availability, prognostics & diagnostics capabilities/technologies should be embedded within the system when feasible (or off equipment if more cost-effective) to support condition

based maintenance and reduce scheduled and unscheduled maintenance. Health management techniques can be very effective in providing maintainers with knowledge, skill sets, and tools for timely maintenance and help reduce the logistics footprint. Condition based maintenance plus (CBM+) (the application of technologies, processes, and procedures to determine maintenance requirements based, in large part, on real time assessment of system condition obtained from embedded sensors), coupled with reliability centered maintenance can reduce maintenance requirements and reduce the system down time. (CBM+ references include the DoDI 4151.22 , the CBM+ Guidebook , and the CBM+ DAU Continuous Learning Module (CLL029) .) The goal is to perform as much maintenance as possible based on tests and measurements or at pre-determined trigger events. A trigger event can be physical evidence of an impending failure provided by diagnostic or prognostics technology or inspection. An event can also be operating hours completed, elapsed calendar days, or other periodically occurring situation (i.e., classical scheduled maintenance). Key considerations in implementing this concept include:

- Use of **diagnostics** monitoring/recording devices and software (e.g., built-in test (BIT) and built-in-self-test (BIST) mechanisms) providing the capability for fault detection and isolation, (including false alarm mitigation) to signal the need for maintenance. It should include user friendly features to convey system status and the effect on mission capabilities to the operator and maintainer.
- Use of **prognostics** monitoring/recording devices and software monitoring various components and indicate out of range conditions, imminent failure probability, and similar proactive maintenance optimization actions to increase the probability of mission success and anticipate the need for maintenance. (As in the case for diagnostics prognostics includes BIT and BIST mechanisms with user friendly features and false alarm mitigation.)
- Maintenance strategies that balance scheduled (preventive) maintenance and minimize unscheduled corrective maintenance with risks.

Key characteristics in implementing the CBM+ concept include:

- Hardware-system health monitoring and management using embedded sensors; integrated data
- Software-decision support and analysis capabilities both on and off equipment; appropriate use of diagnostics and prognostics; automated maintenance information generation and retrieval
- Design-open system architecture; integration of maintenance and logistics information systems; interface with operational systems; designing systems that require minimum maintenance; enabling maintenance decisions based on equipment condition
- Processes-RCM analysis; a balance of corrective, preventive, and predictive maintenance processes; trend-based reliability and process improvements; integrated information systems providing logistics system response; CPI; Serialized Item Management (SIM)
- Communications-databases; off-board interactive communication links

- Tools-integrated electronic technical manuals (i.e., digitized data) (IETMs); automatic identification technology (AIT); item-unique identification (IUID); portable maintenance aids (PMAs); embedded, data-based, interactive training
- Functionality-low ambiguity fault detection, isolation, and prediction; optimized maintenance requirements and reduced logistics support footprints; configuration management and asset visibility.

In accordance with DoDI 4151.22 , it is envisioned that elements of CBM+ should be revisited as the life cycle progresses, conditions change, and technologies advance. Consequently CBM+ should be considered and revisited in each life-cycle phase. See CBM+ Guidebook , Section 4 which provides basic steps for planning and implementing CBM+ throughout the life cycle.

5.3.4. Other Logistics Technologies

Program managers can minimize life-cycle cost while achieving readiness and sustainability objectives through a variety of methods in the design of the system and its maintenance / sustainment program. Below are technologies that should be considered to improve maintenance agility and responsiveness, increase materiel availability, and reduce the logistics footprint:

- **Serialized Item Management (SIM).** SIM (DoDI 4151.19) can be used to aid asset visibility and the collection and analysis of failure and maintenance data. (Also see section 4.3.18.14) The SIM program should be structured to provide accurate and timely item related data that is easy to create and use. While SIM is a DoD wide initiative, the primary function for the program is in ensuring the marking of the population of select items (parts, components, and end items) with a universal item unique identifier (IUID) (DoDI 8320.04). IUID should be used on tangible property, including new equipment, major modifications, and re-procurement of equipment and spares. As a minimum populations from the following categories should be considered for marking:
    - Repairable items down to and including sub-component repairable unit level;
    - Life limited, time controlled, or items with records (e.g., logbooks, equipment service records, Safety Critical Items); and
    - Items that require technical directive tracking at the part number level.

Serialized item management techniques including the use of automatic identification technologies (AIT) such as item unique identification (IUID) technology, and radio frequency identification (RFID) using data syntax and semantics should conform to International Organization for Standardization (ISO) 15418 and ISO 15434 .

- **Automatic Identification Technology.** AIT is an integral element of serialized item management programs. IUID markings and accompanying AIT capabilities facilitate paperless identification, automatic data entry, and digital retrieval of supply and maintenance related information. The program has a wide range of

technologies from which to choose, ranging from simple bar codes to radio frequency identification technology. In choosing the specific technology, the PM should consider that the technology will change over the life cycle both for the program and the supply chain management information systems using the information. Consequently, it is important the PM take into account the need to plan for and implement an iterative technology refreshment strategy. In addition, since AIT is used by supply and maintenance management information systems it is important that items selected for serialized item management be marked in conformance with MIL STD 129.

- **Need for special handling or supportability factors.** This includes the need for special facilities or packaging, handling, storage, and transportation (PHS&T) considerations. This is usually driven by physical needs (e.g., size, weight, special materials) but can also include eliminating excessive set up and teardown times or the in ability to transport systems without disassembly and reassembly.

5.4. Sustainment in the Life-Cycle Phases

5.4.1. Developing the Support Concept and Establishing Requirements

5.4.1.1. Sustainment in the Joint Capabilities Integration and Development System (JCIDS) Process

5.4.1.2. Materiel Solution Analysis Phase Overview

5.4.1.3. Activities/Processes

5.4.1.3.1. Identifying and Evaluating Alternatives

5.4.1.3.2. Sustainment Metrics

5.4.1.3.3. Technical Reviews

5.4.1.3.3.1. Sustainment Considerations in the Initial Technical Review (ITR)

5.4.1.3.3.2. Sustainment Considerations in the Alternative System Review (ASR)

5.4.1.4. Materiel Solution Analysis Phase Results/Exit Criteria

5.4.1.5. Sustainment Considerations in the Materiel Solution Analysis Phase

5.4.1.6. Best Practices during the Materiel Solution Analysis Phase

5.4.1.6.1. Life-Cycle Cost

5.4.1.6.2. Modeling and Simulation

5.4.1. Developing the Support Concept and Establishing Requirements

Effective sustainment begins with the supportability analysis to form CDD specifications for each supportability parameter to be designed, developed, or procured as proven commercial technology. It is these analysis-driven supportability parameter specifications, once integrated through systems engineering with all other technical parameters, which drive deployed system operational availability, sustainment effectiveness, and operator ownership affordability. As discussed below, supportability analyses establish supportability performance capability KPP/KSA parameters for Sustainment in the Joint Capabilities Integration and Development System (JCIDS) requirements documentation and are central to the systems engineering process of identifying and refining all system technical performance capabilities.

5.4.1.1. Sustainment in the Joint Capabilities Integration and Development System (JCIDS) Process

Performance-based life-cycle product support implementation begins in the JCIDS process with the exploration of capabilities defined in terms of overall performance and linking sustainment to performance. Every system is acquired to provide a particular set of capabilities in a specific concept of operations, and sustained to an optimal level of readiness. Understanding user needs in terms of performance is an essential initial step in developing a meaningful support strategy because changes to the CONOPS or the sustainment approach may impact the effectiveness, suitability, or cost of the system. Consequently, operational commands and organizations supporting the combatant commanders should be involved in establishing the requirements since they are generally the system users. Their needs should be translated into performance and support metrics to serve as the primary measures of support system performance.

An effective and affordable logistics support program should be represented as a performance capability priority. As discussed in section 1.3, the JCIDS process documents performance capabilities where Warfighters, or their operational user representatives, identify needed supportability and support related performance capabilities parameters (e.g., sustainment metrics, footprint limitations, cost per operating hour, diagnostic effectiveness). Sustainment planning and resource requirements should be mapped to these specific user needs for support related system performance. Further, programs can more easily invest in sustainment features such as condition based maintenance plus (CBM+) and related embedded instrumentation technology, when they are tied to JCIDS performance parameters.

The JCIDS analysis process is composed of a structured methodology that defines capability gaps, capability needs, and approaches to provide those capabilities within a specified functional or operational area. Based on national defense policy and centered on a common joint war fighting construct, the analyses initiate the development of integrated, joint capabilities from a common understanding of existing joint force operations and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) capabilities and deficiencies. The JCIDS analyses

are led by the sponsor and linked into the Life-Cycle Management System at each phase and milestone.

The JCIDS Instruction (CJCS Instruction 3170.01) and Manual require that key considerations for sustainment be addressed early in the analysis as indicated below:

- A Key Performance Parameter for Sustainment has been mandated which treats logistics supportability as a performance capability inherent to the systems design and development
- A Sustainment Key Performance Parameter (Materiel Availability) and two mandatory supporting KSAs (Materiel Reliability and Ownership Cost) are required for all JROC Interest programs involving materiel solutions.
- Logistics supportability becomes an inherent element of operational effectiveness.
- The Capability Development Document and Capability Production Document (CPD) must state the operational and support-related/sustainment performance attributes of a system that provides the desired capability required by the Warfighter -- attributes so significant that they must be verified by testing and evaluation
- The DOTMLPF includes analysis of the entire life cycle, including the sustainment; environment, safety, and occupational health (ESOH); and all Human Systems Integration (HSI) domains.
- The process to identify capability gaps and potential materiel and non-materiel solutions must be supported by a robust analytical process that objectively considers a range of operating, maintenance, sustainment, and acquisition approaches and incorporates innovative practices -- including best commercial practices, HSI, systems engineering (including safety and software engineering), collaborative environments, modeling and simulation, and electronic business solutions.
- The approaches identified should include the broadest possible range of joint possibilities for addressing the capability gaps. For each approach, the range of potential sustainment alternatives must be identified and evaluated as part of determining which approaches are viable.

Initial Capabilities Document (ICD). JCIDS analyses provide the necessary information for the development of the ICD. The lessons learned, cost drivers of current systems, and/or constraints impacting the supportability related design requirements of the planned system, and support system should be documented in the ICD. In addition, the sustainment metrics and the following supportability drivers should be included in the ICD because they guide the acquisition community in refining the concept selected and identify potential constraints on operating and support resource requirements:

- System maintenance/support profiles and use case scenarios;
- Reliability and maintenance rates;
- Support environment and support locations;
- Support and maintenance effectiveness needs; and

- Duration of support.

5.4.1.2. Materiel Solution Analysis Phase Overview

The purpose of this phase is to assess potential materiel solutions and developing a Technology Development Strategy (TDS). This includes identifying and evaluating affordable product support alternatives with their associated requirements to meet the operational requirements and associated risks. Consequently, in describing the desired performance to meet mission requirements, the sustainment metrics should be defined in addition to the traditional performance design criteria (e.g., speed, lethality). This is because reliability, reduced logistics footprint, and reduced system life-cycle cost are most effectively achieved through inclusion from the beginning of a program and therefore should be addressed in the AoA Plan.

Along with articulating the overall system operational effectiveness objective, this phase is critical for establishing the overarching trade space available to the PM in subsequent phases. User capabilities are examined against technologies, both mature and immature, to determine feasibility and alternatives to fill user needs. Once the requirements have been identified, a gap analysis should be performed to determine the additional capabilities required to implement the support concept and it's drivers within the trade space.

5.4.1.3. Activities/Processes

While considered pre-system acquisition, this phase is critical to acquisition program success and achieving materiel readiness because it is the first opportunity to influence systems supportability and affordability by balancing technology opportunities with operational and sustainment requirements. The phase provides the widest latitude for considering requirement alternatives and has the greatest impact on the life-cycle cost. In determining the optimally balanced requirements, emphasis is not only on the reliability and maintainability of potential materiel solutions, but also on assessing cost-effective responsiveness and the relevance of support system and supply chain alternatives.

5.4.1.3.1. Identifying and Evaluating Alternatives

During this phase, various alternatives are analyzed to select the materiel solution and develop the TDS to fill any technology gaps. Key activities involve identifying and evaluating alternatives and their system sustainment and product support implications. This process is critical because the resulting details guide the acquisition community on refining the concept selected and identifying potential operating and support resource constraints.

Analysis of Alternatives (AoA) . The analysis should evaluate the mission effectiveness, operational suitability, and estimated life-cycle cost of alternatives to meet a mission capability in determining the system concept. The AoA team should include

functional sustainment performance and associated life-cycle cost analysis expertise to help ensure the AoA assesses the ability of each material alternative candidate to meet and sustain the systems JCIDS performance sustainment capability parameters. It is important that the analysis of alternatives includes alternative maintenance and sustainment concepts consistent with the physical and operational environment of the proposed system. Specific consideration should be given to the associated performance metrics to achieve the required effectiveness goals and the overall ability to accomplish a mission, including the ability to sustain the system. Consequently, during this phase the focus is on determining the system level sustainment metrics and values that provide the balance between mission effectiveness, LCC, logistics footprint, and risk that best represents Warfighter needs. This needs to be done for each system alternative analyzed and for their associated sustainment and maintenance strategies. The strategies must then be broken down to their respective drivers to determine the gaps between what is needed to achieve the mission capability and what is currently achievable. The drivers then become performance-based metrics for sustainment enablers. The gaps indicate risk areas and become candidates for potential technology development initiatives. Since operational suitability is the degree to which a system can be used and sustained satisfactorily in the field (in war and peace time), consideration should be given to reliability, availability, maintainability, compatibility, transportability, interoperability, sustainment, documentation, and all the HSI domains (Manpower, Personnel, Training, HFE, Environment, Safety, Occupational Health, Survivability, and Habitability).

This analysis should be accomplished by:

- Forecasting the physical and maintenance environment of the proposed system. This should include the projected sustainment demands.
- Using the forecasted environment to assess the functional characteristics of the proposed system, it's complexity, and the obstacles and enablers for effective sustainment.
- Assessing the impact of the proposed system on the maintenance capabilities planned for the period in which the system will be introduced.
- Assessing the preliminary manpower and personnel requirements and constraints in both quantity and skill levels.
- Compiling initial information and requirements for the logistics footprint, deployment requirements, and other factors affecting the in-theater operational concept. Even this early Rough Order of Magnitude (ROM) estimates can be performed with comparisons to prior systems or systems of similar capability.
- Developing initial operating and support reliability objectives and their corresponding benefit's and resource requirements. This can be done by comparing the performance histories of prior systems or systems of similar capability where feasible for the critical maintenance/sustainment enablers required to achieve the operational requirements.
- Developing ROM life-cycle cost estimates.

Data collected and analyzed during the analysis of alternatives should be retained

because it can be useful for subsequent performance-based product support analysis including providing the baseline for logistics footprint and other factors affecting the in-theater operations concept. (See section 3.3.3) As a result, the sustainment related data should be maintained in a manner to make it easy to update program deliverables during subsequent phases, especially prior to milestone decisions.

5.4.1.3.2. Sustainment Metrics

During the Capabilities-Based Assessment (CBA) process, the operational framework and the Combatant Commander's priorities should be defined sufficiently to guide the development of alternative materiel and sustainment solutions. Relevant sustainment criteria and alternatives should be evaluated and addressed in the Initial Capabilities Document in sufficient depth to support the analysis of alternatives and establish the foundation for developing the Sustainment Key Performance Parameter and supporting KSAs in the Capability Development Document and Capability Production Document . At this time, the metrics should be defined and analyzed against the alternatives and a rough plan as to how they will be measured should be developed.

The focus should be on ensuring the metrics are traceable to the ICD, CDD, other JCIDS analysis, or agreement with the user community on the values for each metric and on documented analyses. The analyses should use the most appropriate data sources and include comparisons of corresponding values for analogous existing systems. Where there is a wide difference between values being achieved by today's systems and those needed for the projected environment, further analysis should be done to determine the enabler technologies (e.g., diagnostics, prognostics) required to achieve the sustainment metrics. The analysis should identify the corresponding performance requirements for key enabling technologies. The results should be included in the TDS and Draft CDD.

5.4.1.3.3. Technical Reviews

Many of the actions and subsequent results in this phase are reviewed during technical reviews. The actions and results discussed in this section should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which the actions should be accomplished.

5.4.1.3.3.1. Sustainment Considerations in the Alternative System Review (ASR)

The ASR helps ensure the preferred system and product support solution satisfies the Initial Capabilities Document. Generally, the review assesses the evaluated alternative systems to ensure that at least one of the alternatives has the potential to be cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution at an acceptable level of risk. See section 4.2.9 for additional information on how the ASR ensures the requirements agree with the customer's' needs and expectations.

For this review to be fully effective, the support concept should be addressed as an integral part of the system concept. During the review, the system concept should be assessed with particular attention to understanding the driving requirements for reliability, availability, maintainability, down time, life-cycle costs, and the enabling technologies required to meet user requirements. Completion of the ASR should provide:

- An agreement on the support concept to be used as the baseline for subsequent trade studies. The support concept should include the conceptual description, scope, and risk for both the system, as well as any supply chain system/software needs beyond what is currently available.
- The results of any sustainment and support concept trade studies/technical demonstrations to develop the concept or reduce risks.
- Refined thresholds and objectives (initially stated as broad measures of effectiveness). This should include a comprehensive rationale for the preferred solution and the proposed sustainment requirements based on an analysis of alternatives that included cost, schedule, performance (including hardware, human, software), and technology risks.
- Product support constraints to enable integration with the operational and support environments.
- Planning for the Technology Development phase addressing critical sustainment enabling hardware and software to be developed and demonstrated/prototyped, their cost, and critical path drivers. Planning should be based on a comprehensive assessment of the relative risks associated with the preferred support concept including commercial off-the-shelf items in the program. It should emphasize host platform environmental design, diagnostic information integration, and maintenance concept compatibility.
- Sustainment requirements for the draft system requirements document, consistent with technology maturity and the proposed program cost and schedule for the technical baseline and preferred support concept. This should include any commonality, compatibility, interoperability, integration or joint requirements.

5.4.1.4. Materiel Solution Analysis Phase Results/Exit Criteria

The focus of this phase is on identifying the initial concept and any critical product support capability requirements. Affordable operational effectiveness is the overarching sustainment objective that should be considered during the JCIDS process. Implementing the process contained in figure 5.4.1.3.1.F1 results in the preferred system concept and the planning to mature the enabling technologies. The conclusion of this phase produces the initial acquisition strategy (including the sustainment strategy), contractual documents required to continue into the Technology Development Phase and includes the initial support & maintenance concepts as well as LCC and manpower estimates for the system concept.

Table 5.4.1.4.T1 identifies the most critical documents that should incorporate or address sustainment/logistics considerations. Entry documents should be complete

when the phase is initiated and include the specific product support issues to be addressed in the phase along with a notional Maintenance & Sustainment Concept of Operations (CONOPS) consistent with the projected Operational CONOPS. Exit documents are completed or, in the case of the Maintenance & Sustainment CONOPS, updated based on the analysis of alternatives results. The key sustainment elements to be addressed in the next phase should be included in the Acquisition Strategy, the Technology Development Phase RFP, and Source Selection Plan.

Table 5.4.1.4.T1. Sustainment Considerations in Materiel Solution Analysis

Entry Documents:
Initial Capabilities Document
Analysis of Alternatives Plan
Alternative Maintenance & Sustainment Concept of Operations
Exit Documents:
Analysis of Alternatives (including Market Research results)
Draft Capability Development Document
Test and Evaluation Strategy
Technology Development Strategy
SEP
Life-Cycle Sustainment Plan

The **Analysis of Alternatives Report** should describe the alternative maintenance and sustainment concepts consistent for each alternative analyzed along with the support capabilities drivers and any gaps.

The exit documents should contain the following sustainment related information for the preferred system concept:

- **ICD/Draft Capability Development Document** the description of the specific enabling technology capabilities required to achieve the drivers and/or to reduce risks in achieving the sustainment metrics values required to meet the operational requirements. The same should be done for each of the corresponding enabling technologies
- **Technology Development Strategy** - the approach for achieving the required enabling sustainment technologies (including design criteria in the Preliminary Design Specification for each of the sustainment drivers). It should also identify the required associated performance metrics and their values.
- **Test and Evaluation Strategy** the identification of the metrics and the key design features to be evaluated in subsequent phases along with the approach for evaluating the likely achievement of each

Life-Cycle Sustainment Plan In this phase and preparing for MS-A, the LCSP focuses

on the approach for developing the sustainment metrics and product support strategy. Emphasis is on the:

- Sustainment metrics (including their threshold and objective values) as well as the supporting design characteristics included in the contract along with the corresponding test methods incorporated in the T&E Strategy/TEMP
- Support and Maintenance Concepts including any real world constraints or limitations (including "core" requirements, statutory requirements, etc.) as well as the extent to which the program is taking advantage of existing supply chain processes and maintenance capabilities.
- Critical sustainment technologies requiring development, their corresponding development plan and how their maturity will be demonstrated.
- Management approach and analytical process for determining affordable metrics (for both the weapon system operational performance and supply chain performance) and for identifying cost and availability degraders so that they can be addressed in the design process.

5.4.1.5. Sustainment Considerations in the Materiel Solution Analysis Phase

Use of M&S should be considered to gain an understanding of the dependency and interplay between designed-in capabilities, processes, availability, and life-cycle cost. While at a high level during this phase, each design alternative examined within the operational concept should be considered as to system availability, LCC, and maintenance and sustainment concept drivers. It is important the analysis of alternatives consider the physical and maintenance environment of the proposed systems in the assessment of the alternative system support concepts.

During this phase, support considerations should address the degree to which a systems design and planned logistics resources support its readiness requirements and wartime utilization. This includes consideration of activities and resources (such as fuel) necessary for system operation as well as real world constraints and environment. It also includes all resources that contribute to the overall support cost (e.g., personnel; equipment; technical support data; and maintenance procedures to facilitate the detection, isolation, and timely repair/replacement of system anomalies).

5.4.1.6. Best Practices during the Materiel Solution Analysis Phase

Modeling and simulation combined with LCC analysis are critical best practices and should be included in the AoA Plan. In addition, both should be used as a source selection factor in the Technology Development Phase selection process and to define the desired ranges for the sustainment metrics thresholds and objectives.

5.4.1.6.1. Life-Cycle Cost

During this phase, both acquisition and O&S costs need to be considered in evaluating affordable alternatives. Also during this phase, key sustainment related cost

performance criteria, such as O&S cost per operating hour or cost per ton-mile, can be considered when conducting design trade-off analyses.

Logistics footprint minimization in projecting and sustaining the force is an overarching DoD goal because minimizing the logistical burden a system will place on deployed forces benefit's the user, improves deployment time, and can help reduce the LCC. During this phase, footprint metrics appropriate to the system and its operational environment should be analyzed and considered as subsequent KPP, KSA, or design requirements. At a minimum, logistics footprint metrics to meet the concept of operations should be established to be used in baseline trade analyses throughout the life cycle to help impact the design and establish a minimal logistics footprint for the system concept.

5.4.1.6.2. Modeling and Simulation

During this phase M&S supports the requirements determination efforts by analyzing the impact of various alternatives to determine an achievable range of the sustainment metrics values to meet the functional requirements. M&S should be used to assess the alternatives, ensuring all sustainment metrics are considered in parallel and not at the expense of the others. In addition, sensitivity analyses should be used to determine the:

- Optimum mix of key metric values (e.g., LCC and readiness drivers) required to meet the requirements and identify corresponding confidence levels for each of the alternatives
- Impact on sustainment, LCC, and readiness drivers if the supply chain performs at today's performance levels.
- Associated sustainment/maintenance concepts for each of the alternatives to be used as the baseline in subsequent phases

Combining these factors will help identify specific areas where new technology is required to achieve or to reduce risks and increase the probability of achieving the requirements.

5.4.2. Sustainment in the Technology Development Phase

5.4.2.1. Overview

5.4.2.2. Activities/Processes

5.4.2.2.1. Initial Life-Cycle Sustainment Plan

5.4.2.2.2. Maintenance & Sustainment Strategy Development

5.4.2.2.3. Technical Reviews in Technology Development

5.4.2.2.3.1. Sustainment Considerations in the System Requirements Review

5.4.2.1. Overview

The purpose of this phase is to reduce technology risks (including required sustainment technologies to achieve the needed materiel availability) and determine the technologies to be integrated into the system. The focus is on developing the preliminary design (down to the subsystem/equipment level), reducing integration and manufacturing risk, and, from a sustainment perspective:

- Designing-in the critical supportability aspects to reduce sustainment technology risks and ensuring features (including CBM+ technologies) are incorporated into the system specifications and test plans.
- Developing the initial product support package framework, options, and requirements for the long-term performance-based support concept.

This phase is the most critical for optimizing system sustainment through designed-in criteria to help ensure sustainability. Particular attentions should be paid to reducing the logistics footprint, implementing human systems integration, and designing for support to help ensure life-cycle affordability. Also, during this phase detailed plans for organizing to manage the implementation of the product support package should begin.

The support concept should be defined going into this phase. The phase should be used to define the design-to requirements and to design the product support package. Technology demonstrations and prototyping should be conducted to help determine mature, affordable technologies to be included in the system and support system designs. The demonstrations results coupled with analysis should be used to refine

requirements and the LCC estimate, narrow the ranges of all program metrics, and increase confidence the values can be met at an affordable cost.

5.4.2.2. Activities/Processes

This phase is important because cost/schedule/performance/sustainability trade-off analyses linked to demonstrated technologies increase the confidence performance, cost, and schedule thresholds can be achieved. During this phase, the logistics emphasis is on maturing the technologies that enable achievement of supportability objectives, on performing requirements refinement and trade-offs to evaluate the achievable performance given the demonstrated technologies, on refining the supportability objectives in both range and depth, and on identifying any constraints that will limit the system or it's supply chain to achieve the operational readiness or mission effectiveness.

Cost/Schedule/Performance/Sustainment Trade-Offs. In all life-cycle phases, cost, schedule, performance, and sustainability may be traded within the trade space between the objective and the threshold without obtaining Milestone Decision Authority approval. Consequently, it is critical the trade space be established early and be acceptable to the user and acquisition communities. As a result, the operational user and sponsor should be involved with the determination of the trade space and involved in trade-off decisions during this phase. The following are the key steps for establishing the trade space and determining the specific developmental requirements:

- Include sustainment requirements and/or considerations in Advanced Concept Technology Demonstrations, Advanced Technology Demonstrations, and other technology oriented demonstrations and prototyping. The demonstrations should be used to help assess the maturity of available and planned technology required for:
    - The preferred operating and support concepts.
    - Achieving the best balance between mission effectiveness, life-cycle cost, logistics footprint, and risk.
    - The sustainment performance driver parameters that best represent user needs in achieving operational readiness.
- Forecast the physical and operational environment of the proposed system along with corresponding notional operating and support concepts. The forecast should include consideration of future projections of domestic and foreign facilitation and logistics infrastructure. Specific consideration should be given to the performance-based requirements to achieve the objectives / thresholds for each of the alternatives considered and determining gaps based on technology availability. The gap analysis needs to take into account the complexity and the obstacles to, as well as, the required enablers for effective sustainment likely to be available when the system is deployed considering the current state of the art and likely funding. These gaps should then be used to eliminate alternatives or to determine specific technologies to be developed. It should also form the foundation for a corresponding technology development and verification strategy.

- Perform a market analysis (both public and private) for the needed system and product support capabilities to fill the gaps. The analysis should address the extent and scope of opportunities for using commercial items and processes. It should consider and assess the:
    - Elements of support currently provided (for any legacy systems to be replaced).
    - Current measures used to evaluate support effectiveness.
    - Current effectiveness of required support.
    - Existing support data across the logistics support elements.
    - Existing technologies and associated support that impact the new system.
- Develop the functional characteristics and performance specification of the system and its support system based on the best balance between mission performance, life-cycle cost, logistics infrastructure and footprint, and risk. An analysis should be conducted to identify key performance and related support parameters for inclusion in the CDD. The analysis should form the basis of design requirements for subsequent phases and will affect the KPPs/KSAs and the overall capability of the system to perform and endure in the required mission environment. ROM LCC estimates should be developed and included in the analysis results based on the following key elements:
    - Preliminary manpower and personnel requirements estimates. This should also include an assessment of any constraints in both quantity and skill levels and the use of contractor support.
    - Operational effectiveness, reliability, maintainability, supportability and interoperability drivers. This should include embedded and external diagnostics, prognostics, and other maintenance enabler technologies that will be required based on suitably mature new design technology. In identifying the drivers and their threshold and objective values, performance histories of similar systems should be examined to determine the feasibility/risks of achieving the required levels and develop a risk mitigation plan. If one has to be developed, the corresponding benefit's and resource requirements for each of the drivers should be identified.
    - Logistics footprint metric estimates, deployment requirements, and other factors affecting the in-theater operational concept. This should include the elements the program will be responsible for and the supply chain performance requirements upon which the program will require to meet operational effectiveness objectives.

Depot Maintenance: During this phase, the following actions are required:

- Finalization in the determination of the organic source of repair to be assigned primary responsibility for maintenance and repair of each system and each sub-system having a core capability requirement.
- Estimate the ROM for the depot-level maintenance workload to be performed at organic facilities for the system and each subsystem.
- Determine the technical data, facility and equipment requirements to ensure the capability to support these workloads.

- Program the resources for the technical data, facilitation, and equipment requirements.
- Summarize the results of these actions in the Acquisition Strategy submitted for Milestone B approval.

5.4.2.2.1. Initial Life-Cycle Sustainment Plan

During this phase, and in preparing for MS-B, the program focuses on finalizing the sustainment metrics, sustainment requirements integration into the design, expanding on the sustainment strategy and maintenance concept and an execution plan describing the design, acquisition, fielding, and competition of sustainment activities to deliver the product support package. The LCSP documents the maintenance & support concepts based on the results of any technology demonstrations and analyses performed to date. It should describe the envisioned sustainment capabilities as viewed by the user and major support providers (e.g., the maintainer, supplier and transportation providers). Taking into account the real world constraints and limitations (including "core" requirements, statutory requirements, etc.), it should include the:

- Sustainment metrics (including their threshold and objective values) as well as the supporting design characteristics included in the contract along with the corresponding test methods incorporated in the TEMP.
- Envisioned Product Support Arrangements, including the level that will be covered by performance-based incentives tied to metrics.
- Approach for developing and fielding the product support package describing who is doing what, where, and when with the associated budgets.
- Analytical process for determining affordable design to metrics goals and thresholds at the subsystem level and for the supply chain are established including how they will be kept aligned/balanced as the design and the supply chain evolve.

5.4.2.2.2. Maintenance & Sustainment Strategy Development

The maintenance & sustainment strategy should be refined from the projected systems reliability and the preliminary sustainment concept of operations to meet the operational requirement in the planned environment. They are then used to determine the supply chain performance requirements, along with the key enabling features needed to implement the strategy. These enablers can range from system design features (e.g. condition based maintenance) to supply chain features (e.g., rapid distribution of tailored support packages, just in time training / distance support, total asset visibility anywhere in the support chain, dedicated rapid response support teams analyzing real time data). The details should be described in sufficient detail to provide assurance that risks are understood and the gaps can be filled.

Core logistics and repair sources are critical elements in establishing appropriate repair and support capability. New and emerging systems may lack mature data at this stage, but by using data from similar current systems and subsystems, planning for a

sustainment strategy can evolve. Key activities should include establishing the baseline for trade studies by identifying notional maintenance levels and activities for major subsystems, taking into account system/subsystems with a core capability.

The gaps between the current state of the art and current sustainment/maintenance capabilities versus what is required (along with the risk) should be used to identify technologies needing to be developed and demonstrated in subsequent phases. They should also be used in developing the implementation plan for proceeding with the best value alternative and summarized in the LCSP. The following are key considerations in developing the performance/cost/schedule/ sustainment and risk tradeoff analysis:

- The relative cost vs. benefits of different support strategies.
- The methods and rationale used to quantify benefits and costs.
- Data required to support and justify the best value support strategy.
- Sensitivity of the data to change.
- Analysis and classification of risks.

Core Capability Planning and Analysis. The requirement for determining core requirements and applying this methodology extends to all weapon systems and equipment operated by each DoD Component, regardless of where depot-level maintenance is actually performed (DoDI 4151.20 , "Depot Maintenance Core Capabilities Determination Process"). The following depot maintenance core capability requirements determination methodology is used to determine essential DoD depot maintenance capability requirements for each DoD Component, and the workloads needed to sustain those capabilities.

- Programs requiring a core capability/DSOR decision shall be identified by the managing Service Acquisition Program Manager (PM) (or Joint Program Office (JPO) in the case of Joint Service acquisitions) to the Service organization(s) responsible for depot-level maintenance management (hereafter referred to as MMOs). Joint programs, and those having depot-level maintenance inter-servicing potential, shall be identified by each DoD Component MMO in conjunction with the PM/JPO.
- The identification of the need for a core determination will occur at least 180 days prior to the Acquisition Milestone B decision need date. For systems entering the acquisition process after Milestone B, identification will occur immediately following the acquisition approval.
- It is the responsibility of the Acquisition Program Manager (PM) (or Joint Program Office (JPO)) in conjunction with the DoD component that owns the depot-level maintenance assets to ascertain the potential need for establishing an organic core capability requirement by addressing, at a minimum, the following questions. Other considerations may be applied, as appropriate.
- Is the system replacing a system having a core capability requirement at either the system or the subsystem level? If the answer is "Yes" then it can be assumed that this system and it’s subsystems will require the same core capability requirements as the system being replaced, adjusted for known inventory and

workload differences.
    - If not, will the system be used or is it planned to be used in support of a JCS contingency scenario? If the answer is "Yes" then Section 2464 of Title 10, United States Code requirements for the establishment of organic core capability apply.
    - If the answer to either question is 'yes', an initial core capability requirement determination analysis must be conducted and candidate Depot Source of Repair (DSOR) depot-level maintenance facilities identified by the DoD Component(s).
- After core requirements have been determined, the PM/JPO shall take appropriate steps to assure that the requirements for the establishment of organic capability are included in all product support acquisition requirements (e.g. need for tech data, peculiar support equipment, facilities and/or Public Private Partnership).
- While not part of the core determination process it is at this stage that any requirements to assign a portion of the proposed workload to an organic depot to provide reasonable assurance of future compliance with the 50/50 requirements be identified and provided by the DoD Component(s) MMOs to the PM/JPO along with justification and documentation for use in designing the product support strategy.

5.4.2.2.3. Technical Reviews in Technology Development

Many of the actions and subsequent results in this phase are reviewed during technical reviews. The actions and results discussed in this section should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which they should be accomplished.

5.4.2.2.3.1. Sustainment Considerations in the System Requirements Review (SRR)

The SRR is conducted to ascertain the results of the prototyping and demonstrations relative to the system technical requirements. It determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete system baseline. (See section 4.2.10 for additional information.) The purpose is to ensure all system requirements (performance requirements and sustainment requirements) derived from the Initial Capabilities Document (ICD) or draft CDD are defined, consistent and achievable within cost, schedule and any other constraints. Generally the SRR assesses the prototyping results with respect to the system requirements captured in the system specification and support strategy to ensure they are consistent with the system and support solution as well as available technologies.

The SRR is important in understanding the performance requirements, cost, and scheduling impacts on the system and its support concept. During the SRR, the systems requirements are evaluated to determine whether they are fully defined and consistent with a demonstrated mature technology solution. A successful review is

predicated on determining the system and support element requirements are based on available technology, a sustainable support concept, and program resources (e.g., funding, staffing, processes and schedule). Logistics and product support subject matter experts should participate to ensure the critical sustainment system and support elements enabler technologies required to implement the support strategy and achieve the needed materiel availability are included in the planning and performance specifications. Understanding and accepting the program risk inherent in the system specification, Systems Engineering Plan and Life-Cycle Sustainment Plan is key to a successful review. The SRR should provide:

- An approved system performance specification with achievable system, supportability, human systems integration, and sustainment enabler requirements which satisfy and are traceable to the ICD or draft CDD and support concept.
- A preliminary allocation of system requirements to hardware, human, and software subsystems. The system sustainment requirements should be sufficiently detailed and understood to enable system functional definition and functional decomposition.
- Demonstration that critical sustainment system and support element enabler technologies required to implement the support strategy and achieve the needed materiel availability are sufficiently mature to enable low risk entry into development.
- Approved support and sustainment concepts with the corresponding metrics.
- A preliminary Cost Analysis Requirements Description consistent with the approved system performance specification and sustainment concept.

5.4.2.2.3.2. Sustainment Considerations in the System Functional Review (SFR)

The SFR ensures the system functional baseline has a reasonable expectation of satisfying the CDD requirements within the allocated budget and schedule. A critical SFR aspect is the development of representative operational and product support use cases for the system. System performance and the anticipated functional requirements for operations, maintenance and sustainment are assigned to sub-systems and support systems hardware and support systems hardware & software after analysis of the operational and support environments. The SFR determines whether the systems functional definition is fully decomposed to its lowest level forming the functional baseline, and that IPTs are prepared to start preliminary design. Additional information for this review can be found in section 4.2.11 .

Product support IPT members as well as independent supportability and sustainment subject matter experts should participate in the review to ensure the system functionality is consistent with the supportability requirements and the support strategy contained in the evolving Life-Cycle Sustainment Plan (LCSP). This involves:

- Addressing the supportability requirements to support the CDD and the supportability functionality as defined in the functional baseline ensuring

adequate processes for achieving the sustainment metrics are in place.
- Defining the detailed support concept functionality requirements for system and subsystem elements to ensure system functional requirements are sufficiently detailed and understood to enable system design supportability analyses to proceed.
- Ensuring program sustainment development efforts (including system and software critical path drivers), with corresponding schedules, are included in LCSP updates.
- Ensuring the updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the system functional baseline, captures the key program sustainment cost drivers, development costs, production costs, and operation & support costs for all aspects of sustainment and human system integration.

5.4.2.2.3.3. Sustainment Considerations in the Preliminary Design Review (PDR)

The PDR helps ensure the systems allocated baseline and its associated support system have a reasonable expectation of satisfying the CDD requirements within the allocated budget, staffing, and schedule and have an acceptable risk level. Details can be found in section 4.2.12 but in summary the PDR assesses the preliminary design captured in the preliminary subsystem product specifications for each configuration item (hardware and software) and ensures each function, in the functional baseline, has been allocated to one or more system configuration items. The PDR evaluates the subsystem requirements to determine whether they correctly implement all system requirements allocated to the subsystem. The Integrated Product Team (IPT) should review the results of peer reviews of requirements, preliminary design documentation (including Interface Control Documents) along with the plans for development and testing for both system performance and supportability aspects to ensure the system is ready to proceed into detailed design and test procedure development.

Product support IPT members, as well as independent supportability and sustainment subject matter experts, should participate in the review to ensure the supportability requirements and the support strategy contained in the Life-Cycle Sustainment Plan (LCSP) are consistent with the evolving design. This involves:

- Addressing the supportability requirements to support the CDD and ensuring the supportability functionality are allocated to each system or subsystem and they can be achieved within the budgets and schedule. This includes ensuring the Failure Mode Effects and Criticality Analysis, Maintainability Analysis, and Reliability Centered Maintenance Analysis results have been factored into the allocated requirements, preliminary design, and risk assessment. In addition to ensuring adequate processes for achieving the sustainment metrics are in place, this includes ensuring the HSI design factors have been reviewed and included in the overall system design.
- Setting the allocated baseline for any system and/or major subsystem product support package elements. This includes defining the detailed support concept

functionality requirements for subsystem product support package elements to ensure system functional requirements are sufficiently detailed and understood to enable more detailed supportability analyses to proceed.
- Defining the test success criteria for development testing and operational testing (for both operationally effective and suitable) requirements and the general test approach for key sustainment enablers or drivers.
- Ensuring program sustainment development efforts (including system and software critical path drivers with corresponding schedules) are included in LCSP updates.
- Ensuring the updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the system allocated baseline, captures the key program sustainment cost drivers, development costs, production costs, and operation & support costs for all aspects of sustainment and Human Systems Integration (HSI.)

5.4.2.2.3.4. Sustainment Considerations in the Technology Readiness Assessment (TRA)

The TRA is a metrics based process that assesses the maturity of critical technology elements, including sustainment drivers, conducted concurrently with technical reviews. From a sustainment perspective, the process should be used for assessing risk and the adequacy of technology maturation planning when the support concept or sustainment drivers depend on specific new or novel technologies to meet system threshold requirements in development, production, or operation. If a key enabler or sustainment driver (e.g., reliability, turnaround time) does not meet required performance levels or significant performance advances is required over what is currently achieved with existing technology, then a plan for maturing the critical technology should be developed, explaining in detail how the performance level will be reached within the programs schedule and resources. See section 10.5.2 for additional information.

5.4.2.2.3.5. Sustainment Considerations in the Integrated Baseline Reviews (IBR)

IBRs are used throughout the program whenever earned value management is used. IBRs establish a mutual understanding of the project performance measurement baseline. While they have a business focus, IBRs can also be useful in ensuring sustainment is considered in the acquisition process when the efforts required to achieve the Sustainment KPP, KSAs and any other key sustainment enabler metrics are included in the reviews. These reviews and resultant understanding also provide for a plan of action to evaluate the risks inherent in the program measurement baseline and the management processes during project execution. Additional information can be found in section 11.3.1.3 .

5.4.2.3. Technology Development Phase Results/Exit Criteria

The focus of this phase is on reducing risk and defining achievable performance and sustainment requirements. This begins with the analysis of alternatives that include

examining alternative operating and system support concepts, with specific consideration of performance-based requirements. Success is demonstrated by identifying key performance and related sustainment metrics (with their basis) as design requirements that affect the overall capability of the system to perform and endure in the required mission environment. (In addition to the Sustainment KPP/KSAs, the metrics can include other supportability, maintainability, interoperability, manpower or footprint measures.) Implementing the process contained in figure 5.4.2.2.F1 produces the refined supportability objectives and, in some cases, anticipated constraints based on the technology assessments. The conclusion of this phase results in the contractual documents required to continue (including the related sustainment requirements and actions) and updated system baseline support & maintenance concepts, LCC, and manpower estimates.

Table 5.4.2.3.T1 identifies the most critical documents that should incorporate or address sustainment/logistics considerations. The key sustainment elements to be addressed in the next phase should be included in the Acquisition Strategy and the materiel availability enabler requirements should be included in the Engineering and Manufacturing System Development RFP as well as the Source Selection Plan. The exit documents from this phase should focus on the materiel availability driver metrics (including drivers for the enablers) and the baseline support strategy. They should also contain the following sustainment related information:

Table 5.4.2.3.T1. Sustainment Considerations in Technology Development

Entry Documents:
Analysis of Alternatives
Technology Development Strategy Draft Capability Development Document (including sustainment technology issues)
Test and Evaluation Strategy
Life-Cycle Sustainment Plan
Exit Documents:
Analysis of Alternatives (including Market Research results)
System Performance Specification
Capability Development Document
Preliminary Design Review Results
Test and Evaluation Master Plan (TEMP)
Information Support Plan
Acquisition Strategy
Cooperative Opportunities
Technical Data Rights Strategy
Core Logistics Analysis/Source of Repair Analysis
Industrial Capabilities

Life-Cycle Sustainment Plan
Life-Cycle Cost Estimate and Manpower Estimate
Preliminary Maintenance Plans
Acquisition Program Baseline (APB)
Affordability Assessment (including DoD Component Cost Analysis & ICE)

- **AoA** - the sustainment driver metrics and product support strategies for each alternative considered along with any gaps and major assumptions
- **System Performance Specification** - objectives and thresholds for the sustainment driver metrics including the corresponding enabler drivers
- **CDD** - the information necessary to deliver an affordable and supportable capability using mature technology. The following sustainment drivers information should be included:
    - System maintenance/support profiles and use case scenarios
    - The corresponding support and maintenance effectiveness measures
    - Description of the specific capabilities required to achieve the support concept and/or to reduce risks in achieving the values required to meet the operational requirements. It should include metrics for each of the key enabling technologies (e.g., reliability/ maintenance rates, diagnostics/prognostics effectiveness measures)
- **Preliminary Design Review Results** the description and status of the sustainment driver design features
- **Technology Readiness Assessment** - approach for achieving the required enabling sustainment technologies (including design criteria for each of the drivers in the preliminary system design specification) (see section 10.5.2)
- **Test and Evaluation Master Plan (TEMP)** identification of the metrics and enabling/driver technologies to be evaluated in subsequent phases, the approach for evaluating them, and test points (see section 9.5.5)
- **Data Management Strategy** the long term strategy integrating data requirements across all functional disciplines.
- **Information Support Plan** for acquiring and managing the data required to execute the support concept in the operational environment (see section 7.3.6)
- **Acquisition Strategy** containing the LCSP executive summary
- **Life-Cycle Sustainment Plan (LCSP)** summary of the maintenance & sustainment concepts including the support locations and duration. It should focus on the support strategy including the contracting strategy to acquire the major elements of the support concept and the specific incentives being used to help achieve the sustainment drivers and enablers
- **Life-Cycle Cost Estimate and Manpower Estimate** the major assumptions and values being used for the sustainment drivers and enablers (see Chapters 3 and 6) It should also include the confidence level of the values being achieved
- **Acquisition Program Baseline (APB)** description of the sustainment metrics, criteria, and logistics funding requirements (see section 10.9)
- **Affordability Assessment** an assessment based on the likelihood of the key

sustainment metrics being achieved (also see section 3.2.2)

5.4.2.4. Sustainment Considerations in the Technology Development Phase

During this phase, the focus should be on refining the threshold and objective range value estimate for each sustainment metric based on more detailed analysis identifying the technical capabilities, risks, and limitations of the alternative concepts and design options. Analysis should also be performed to identify the impacts the sustainment metrics will have on mission success and materiel availability. The key enabling requirements to achieve the sustainment metrics should be allocated to the major system level and included in the system specification. Even this early it is important to establish the reliability requirements and assess the extent to which the system will likely meet the requirements. Consequently, the reliability of the technology or system should be included in the technology readiness assessments.

Detailed plans for monitoring, collecting and validating key metrics should be established to provide empirical data to evaluate technical performance, system maturity, and the projected logistics burden. Detailed test criteria should be developed for each metric (including any key dependent enabling technologies) to provide information about risk and risk mitigation as the development and testing continue. The test strategy/requirements to provide data and analysis support to the decision process should be documented in the TEMP.

5.4.2.5. Best Practices during the Technology Development Phase

M&S combined with LCC analysis are important best practices to help assess the success in reducing program risk. In addition, both should be used in the Engineering & Manufacturing Development Phase source selection process and to define the sustainment objectives and thresholds to be placed on contract. The data used for the assessments and analysis (including the projected sustainment demand) should be complied and saved for analyses in subsequent phases.

5.4.2.5.1. Supportability Analysis

During this phase, supportability analysis focuses on the technology trade-offs. As indicated in figure 5.4.2.5.1.F1, the analysis process is iterative. They are re-run as required as the design is refined. Trade-off impacts are identified and evaluated to ensure the selection of a system concept that not only delivers system performance, but also achieves supportability, interoperability and system affordability objectives. The supportability analysis goal within this phase is to establish affordable and obtainable thresholds and objectives to achieve the user requirements in the projected environment within the Concept of Operations.

The analyses are iterative, evolving and expanding as more specific design and other technical information on the actual equipment is identified. While the focus is high level for the system at the beginning of this phase, it should also consider requirements for

key enablers in terms of "what is required" vice "how it is accomplished". As the phase progresses, the analysis should determine the relative cost vs. benefits of different support strategies (including potential source of support decisions). The impact and value of performance/cost/schedule/sustainment trade-offs based on the preliminary design should continue expanding to the lowest level of the work break down structure as the design evolves across this and subsequent life-cycle phases.

A complete supportability analysis should be performed for any parts of the system for which the government is going to provide the product support package vice using a contracted approach with materiel availability as the performance measure. Figure 5.4.2.5.1.F1 shows the key system reliability, maintainability and supportability system engineering processes. The affordable system operationally effectiveness analysis process coupled, with available tools and opportunities - such as modeling and simulation, performance testing, supportability testing/demonstration, technical data validation, and maintenance assessments - should be proactively applied and integrated with the systems engineering process. For example, system requirements can be used to develop a system reliability/availability block diagram as a basis for modeling and analysis. This approach can identify opportunities for targeted system redundancy, ease of reconfiguration, and derating, etc., and can thereby enhance system level reliability and availability. In addition, reliability, maintainability (BIT/prognostics), and supportability/ logistics demonstrations can provide the data to assess achievement of RAM requirements.

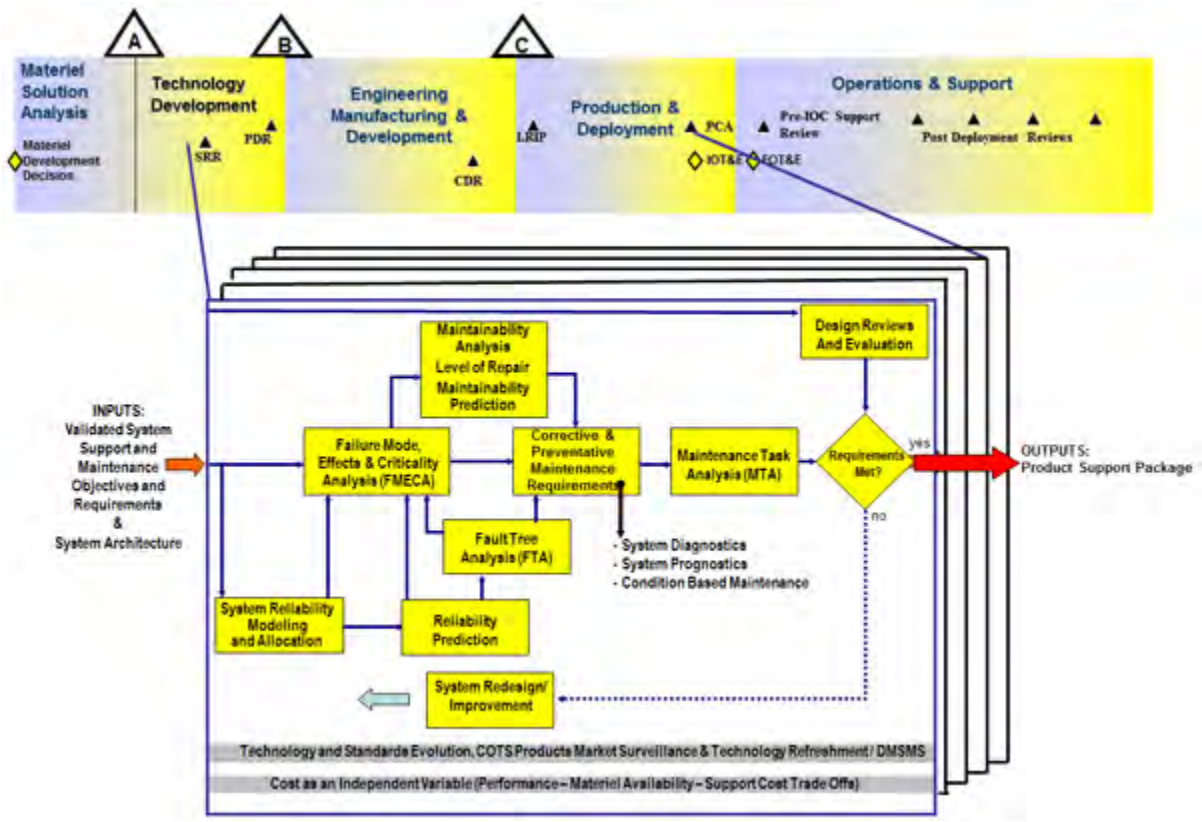
The level of detail performed by the government team will vary by the extent to which performance-based product support contract is used but that will not impact the general process, including the program major events. As a result, the supportability analysis process should take advantage and be an integral part of the major engineering events and processes, including but not limited to the System Requirements Review (SRR) and Preliminary Design Review (PDR).

As illustrated in Figure 5.4.2.5.1.F1, a FMECA helps identify the ways in which systems can fail, performance consequences, and serve as basis in the identification of Critical Safety Items as well as potential areas for preventative maintenance for the system. When conducted in a timely fashion, the FMECA can be used to support trade-offs between performance and life-cycle costs to drive design improvements. A Fault Tree Analysis (FTA) assesses the safety-critical functions within the systems architecture and design. A Maintainability Analysis and Prediction (MAP) assesses the maintenance aspects of the systems architecture, including maintenance times and resources. This analysis identifies strategic opportunities for focused diagnostics, prognostics, and performance monitoring/fault localization, leading to reduced system maintenance times and cost drivers. A level of repair analysis optimally allocates maintenance functions for maximum affordability and materiel availability.

Once FMECA, FTA, and MAP are completed and system design has been established, RCM analysis develops a focused, cost-effective system preventive maintenance program. RCM uses a system based methodical approach to determine causes of

failure, failure consequences, and a logic tree analysis to identify the most applicable and effective maintenance task(s) to prevent failure, if possible. RCM also provides rules for determining evidence of need for condition based maintenance to perform maintenance only upon evidence of need. (DoDI 4151.22, Enclosure 3)

Figure 5.4.2.5.1.F1. Supportability Analysis During Design



A maintenance task analysis identifies detailed logistics and support resource requirements to sustain system readiness. Appropriate use of proactive maintenance technologies embodied in diagnostics and prognostics pays system dividends. Integrating on-board and off-board monitoring, testing, data collection, and analysis capabilities can significantly enhance system maintainability and overall supportability. Typically, practices here include enhanced prognosis/diagnosis techniques, failure trend analysis, electronic portable or point-of-maintenance aids, corrosion mitigation, serial item management, automatic identification technology, and data driven interactive maintenance training. Ultimately, these practices can increase materiel availability and readiness at a reduced cost throughout the life cycle.

The activities shown in figure 5.4.2.5.1.F1 are not necessarily carried out in a linear progression. Design increments and the continuous assessment of test results and in-service system performance will identify needs for system improvements to enhance reliability, maintainability, overcome obsolescence, corrosion, or other sustainment

needs.

Risk Assessments. Risk assessments should be performed to identify and develop design trade-off that mitigates risk. Technology risk considerations should receive intensive consideration as the system concept is developed. Maximum use of low-to-medium risk technology, as indicated in Table 5.4.2.5.1.F2, provides the greatest opportunity to hold to program cost, schedule and performance requirements. Medium-to-high risk technologies should be thoroughly justified and risk mitigation efforts resourced. Use of high-risk technologies should be avoided and be a critical factor in choosing an incremental acquisition strategy.

Once the preferred system, system support concepts and enabling technologies are selected, case scenarios reflecting system support, maintenance, and logistics are refined. These scenarios identify significant system support, maintenance, and logistic requirements and objectives. These are compared to the Sustainment KPP/KSA threshold and objective and expanded in depth as the hardware design matures and the process is iterated until an affordable systems operational effective solution is achieved.

Table 5.4.2.5.1.T1. Technology Risk Considerations

Technology Maturity	Technology Description
Low Risk	Existing Mature Technologies
Medium Risk	Maturing Technologies; New Applications of Mature Technologies
High Risk	Immature Technologies; New Combinations of Maturing Technologies

5.4.2.5.2. Modeling and Simulation

M&S should be used to refine sustainment objectives (this includes the Sustainment KPP and KSAs as well as any other LCC or readiness driver metrics) and identify any constraints based on technology assessments. The technology demonstration results should be modeled to project likely capabilities and the associated confidence levels that enabling technologies will be achievable in the operational environment. It should also be used to develop initial/notional system level product sustainment strategy and maintenance concepts for major sub systems. All of these elements will be used to project the mature Sustainment KPP/KSA values and their associated confidence levels they will be met within the CONOPS.

As the design evolves, modeling and simulation can be used to help keep the product support elements in balance between and within system hardware elements. This is done by allocating the sustainment, LCC or readiness driver metrics to specific subsystems and equipment’s. These requirements are then used to develop the specific system level support strategies and maintenance plans along with their design-to

requirements for both the system and it's logistic support system. Modeling at this level of detail provides more creditability especially relative to the following efforts important in this phase:

- Analyzing the impact of proposed budget alternatives on the Sustainment KPP/KSAs (as well as mission effectiveness).
- Assessing the alternatives affecting the design and deployment of both the end item and it's support system to ensure all metrics and their drivers are considered in parallel and not at the expense of the others.
- Anticipating and resolving potential problems by taking use data and user feedback for similar equipment's and/or sustainment strategies.

5.4.3. Sustainment in the Engineering and Manufacturing Development (EMD) Phase

5.4.3.1. Overview

5.4.3.2. Activities/Processes

5.4.3.2.1. Life-Cycle Sustainment Plan

5.4.3.2.2. Technical Reviews in Engineering and Manufacturing Development

5.4.3.2.2.1. Sustainment Considerations in the Critical Design Review (CDR)

5.4.3.2.2.2. Sustainment Considerations in the Test Readiness Review (TRR)

5.4.3.2.2.3. Sustainment Considerations in the System Verification Review (SVR)

5.4.3.2.2.4. Sustainment Considerations in the Functional Configuration Audit (FCA)

5.4.3.2.2.5. Sustainment Considerations in the Production Readiness Review (PRR)

5.4.3.3. Engineering & Manufacturing Development Phase Results/Exit Criteria

5.4.3.4. Sustainment Considerations in the Engineering and Manufacturing Development Phase

5.4.3.4.1. Sustainment Metrics

5.4.3.4.2. Technology Refreshment and Obsolescence Management

5.4.3.4.3. Sources of Support

5.4.3.1. Overview

The purpose of this phase is to develop a detailed integrated design and ensure producibility and operational supportability. The focus is on producing detailed manufacturing designs, not solving a myriad of technical issues. Prototyping and analysis should have been applied prior to this phase to discover and resolve issues to ensure the design is based on a mature technology and is achievable within cost, schedule and sustainment constraints. From a sustainment perspective this means paying particular attention to reducing the logistics footprint; implementing human systems integration; designing for supportability; and ensuring affordability, integration with the supply chain, interoperability, and safety. All of these factors are used to refine the performance-based support concept and strategy, with the associated requirements, and to identify potential support providers.

5.4.3.2. Activities/Processes

During this phase, the focus is on developing the requirements for the long-term performance-based support concept and the initial product support package. In accomplishing this, life-cycle management documents and analyses are refined as a result of the detailed design process, iterative systems engineering analyses and developmental test results. During this phase, the critical sustainment metrics are also refined and incentives developed for eventual performance-based support contracts and/or performance-based agreements. Stakeholders (including potential support providers) are identified and included in Integrated Product/Process Team (IPT) processes to build an early understanding of and buy-in for sustainment requirements and objectives. Also during this phase, the support concept is refined and potential support providers are identified. Incentives to design for support and to design a cost-effective support concept can, and should, be linked to the support strategy. Identification and involvement of the potential support providers and integrator early during these efforts is essential for program success.

Supportability Analysis. Supportability analysis, modeling and simulation, and life-cycle costing should be applied and integrated with the systems engineering process in increasing levels of detail to determine the relative cost vs. benefits of different support and maintenance strategies; the impact and value of

performance/cost/schedule/sustainment trade-offs; and to create the data required to support and justify the support strategy. During this phase, data will be compiled, refined, and analyzed consistent with acquisition policy and Defense Acquisition Board (DAB) requirements to develop and document a best value long term support strategy. The assessment process determines the right mix between organic and commercial performance-based support and should consider all requirements (including statutory) when determining the best value long term sustainment approach to optimize readiness while minimizing cost. The programs should use accepted decision making tools and processes, such as Business Case Analysis, Economic Analysis, DSOR Analysis, Decision Tree Analysis, and/or other appropriate best value assessments. At this point, no firm source of support decisions should be made until sufficient data is collected and the risks are determined. (Determination of core capability workload requirements should be made after the system passes Critical Design Review (CDR).) As a result, the analysis results should be used and expanded throughout the program life cycle to:

- Assess alternative contracting approaches based on cost, benefit, and performance outcomes
- Establish a strong foundation for budgetary requirements
- Provide the definitive cost and performance base to be used for contract negotiation
- Provide the cost/performance baseline to be used to measure effectiveness
- Quantify the benefit's to be realized

Almost all of the values used during this phase should be based on engineering estimates and actuals or test results. The level of detail performed by the government team will vary by the extent to which industry is used to achieve the materiel availability in a performance-based logistics contract product support package. (The government's detailed supportability analysis requirements decrease in depth as a direct function of the level the performance standards are set in the contract requirements, the portion of the system covered, and the sustainment functions for which the contractor is responsible.)

Regardless of the contracting approach taken, Supportability Analysis will have to be performed even if only to determine the specific metrics and their respective values that will motivate the right behavior, be aligned with the user requirements and to determine a fair and affordable price. Analysis is also needed to ensure any contracted metrics are aligned with portions of the public infrastructure/supply chain that will support the user. See section 5.4.3.5 for a further description of the best practices that should be used in performing a detailed supportability analysis for any parts of the system in which the government will provide the product support package, vice using a contract with materiel availability as the performance measure.

Reliability Growth. A reliability development/growth effort should be undertaken if the assessed reliability of the system or technology is not above threshold with a safe margin to account for the typical drop experienced when a system transitions from a paper design to fielded conditions. Emphasis should be placed on discovering and

mitigating failure modes throughout the system design and development process, since relying solely on testing as a means of improving reliability has been shown to be risky and costly. Consideration should be given to using such practices as physics of failure reviews, environmental stress screening, and highly accelerated life testing. A test analysis and fix program should be implemented to increase reliability and it should be expanded as more of the hardware (including prototypes) is tested and operated by the users. Using this process, failure modes may be found through analysis and testing are then eliminated or reduced by design or process changes as appropriate. Shortchanging this effort early in development, particularly at the subsystem and component level, is a frequent cause of later program delays and cost increases as the flaws inevitably show up in system level performance.

Maintainability Growth. Efforts to improve maintainability and/or validate maintainability metrics are being achieved in the development process should also be considered along with traditional Reliability Growth management efforts. Typically this includes new diagnostics and prognostics technologies, but, the same principles can be applied to other maintainability drivers such as extensive time consuming repair techniques. The specific maintainability growth management efforts are unique to the program but should be considered for maintainability drivers upon which the sustainment KPP/KSA depend.

5.4.3.2.1. Life-Cycle Sustainment Plan

In this phase and in preparing for MS-C, the LCSP focuses on the efforts to manage the sustainment related risk focusing on the implementation of the product support package. This includes the approach for developing and fielding the product support package describing who is doing what, where, and when with the associated budgets. In addition to refining and expanding on the sustainment management approach, schedule and costs aspects, specific attention should be paid to the:

- Product Support Strategy details (including the depot maintenance requirements and the implications of core requirements) and what is expected from each of the stakeholders
- Performance verification methods used in production, fielding and operations. This includes the design characteristics included in the contract, how they will be demonstrated and performance to date
- Outcome based contracts, including the level that will be covered by performance-based incentives tied to metrics
- Assessment results to date and the product support risks
- How major actions/events for the product support package elements fit with the overall program master schedule including the interfaces and dependences between the elements
- Processes to establish the requirements for product support package elements and keep them aligned/balanced as the design and supply chain evolve

5.4.3.2.2. Technical Reviews in Engineering and Manufacturing Development

Regardless of the acquisition strategy chosen relative to PDR timing and prototyping, any remaining initial systems design activities and reviews not finished during the Technology Development phase (i.e., System Requirements Review (SRR), System Functional Review (SFR), or Preliminary Design Review (PDR)) are completed early in the EMD phase. Section 5.4.2.2.3 provides a description of the sustainment aspects that should be considered for each review and is not repeated in this section. If the PDR was not conducted prior to Milestone B, the PM should include the results of the sustainment assessment in the PDR report and Post-PDR Assessment.

5.4.3.2.2.1. Sustainment Considerations in the Critical Design Review (CDR)

The CDR helps to ensure the system can satisfy the CDD requirements within the allocated budget, staffing and schedule. Details can be found in section 4.2.13 , but in summary the CDR results in an initial product baseline for the system, hardware, software, maintainability, supportability, and the product support elements, including support equipment, training systems, and technical data. Subsystem detailed designs and product support elements are evaluated during the review to determine whether they correctly implement system requirements and if the system is mature enough to proceed into fabrication, demonstration, and test.

Product support IPT members, as well as independent sustainment subject matter experts, should participate to ensure the design includes the supportability requirements and the support strategy contained in the Life-Cycle Sustainment Plan (LCSP) are consistent with the product baseline and the projected sustainment metrics (e.g., reliability, maintainability) and other supportability features. The PM should include the results of the CDR sustainment assessment in the Post-CDR report and Post-PDR Assessment. For the system and key product support elements as appropriate, this involves ensuring the:

- Supportability requirement enablers, such as Human Systems Integration (HSI) design features, inclusive of the environment, safety and occupational health risk reduction features, are included in the design.
- Failure Mode Effects and Criticality Analysis have been completed and any remaining subsystem requirements for the product support package elements design are complete.
- Key sustainment characteristic drivers (including critical manufacturing processes to achieve them) have been identified, and an estimate of system reliability based on demonstrated reliability rates and other sustainment drivers are being used in developing the product support package.
- Development testing results are used to update the sustainment metric projection estimates and any planned corrective actions to hardware/software deficiencies have been identified.
- Test success criteria for any remaining development testing and operational testing plans (for testing both operationally effective and suitable) for key

sustainment enablers or drivers requirements are complete. If the test results to date do not indicate the operational test success is likely or risk has increased, new developmental and operational testing criteria and plans should be considered, along with fallback plans.
- Program sustainment development efforts with corresponding schedules, including system fabrication, test, and software critical path drivers, are included in LCSP updates.
- Updated Cost Analysis Requirements Description (CARD) (or a CARD-like document) based on the initial product baseline, captures the key program sustainment cost drivers, development costs, production costs, operation and support costs for all aspects of sustainment and HSI.

5.4.3.2.2.2. Sustainment Considerations in the Test Readiness Review (TRR)

The TRR helps to ensure the subsystem or system is ready to proceed into a formal test. Details can be found in chapter 9 , but in summary it assesses test objectives, test methods and procedures, test scope, and safety confirming test resources have been properly identified and coordinated. Consequently, there are two primary logistics roles in the TRR. One is to help ensure the test is properly planned and resourced (e.g., people, facilities, data systems, support equipment, and any other product support elements) to achieve the test objectives. The second role is to ensure the tests will identify and help control risk by verifying and validating key sustainment drivers are in place to achieve the Sustainment KPP and KSAs. This can be accomplished by building off the system performance tests as well as structuring specific tests and demonstrations focused on sustainment drivers including maintainability. Regardless of stage of development or the level of testing (component, subsystem, or system), the basic tenets contained in section 4.3.3.4.3 apply. This includes, but is not limited to, identifying the:

- Test purpose and exit criteria.
- Expected result, test success criteria, and how the test results will affect the program.
- Risks that will be mitigated by the test and which will remain.
- Fall-back plan should a technical issue or showstopper arise during testing.

5.4.3.2.2.3. Sustainment Considerations in the System Verification Review (SVR)

The SVR is a product and process assessment to ensure the system can proceed into production within cost, staffing, schedule, and other system constraints with an acceptable risk level. Details can be found in section 4.2.14 but in summary the SVR assesses the system functionality, determining if it meets the functional requirements, and verifies final product performance. The SVR is often conducted concurrently with the Production Readiness Review (section 4.2.15) and Functional Configuration Audit (section 4.2.14). Product support IPT members as well as independent sustainment subject matter experts should participate to:

- Address system supportability and, based on developmental testing or analysis whether the sustainment features will satisfy the Capability Development Document/draft Capability Production Document and Sustainment KPP/KSAs.
- Adequate processes are in place so the sustainment performance metrics can be used to help the program to succeed in meeting user needs.
- Ascertain if the system is supportable within the procurement, operations, and support budgets.

5.4.3.2.2.4. Sustainment Considerations in the Functional Configuration Audit (FCA)

FCA is essentially a review of an item's test/analysis data to validate the intended function or performance stated in its specification is met. See section 4.2.14 for additional details. From a sustainment perspective, the FCA should include auditing the testing and analysis performed to date to ensure the results indicate system compliance with the applicable Sustainment KPPs, KSAs, and derived supportability requirements as reflected in the functional baseline. In addition, to help ensure a system will be sustainable, key elements of the product support system should also undergo a FCA.

5.4.3.2.2.5. Sustainment Considerations in the Production Readiness Review (PRR)

The PRR determines whether the design is ready for production and if the producer has accomplished adequate production and product support planning. Details can be found in section 4.2.15 , but in summary it determines if production or production preparations incur unacceptable risks that might breach schedule, performance, cost, or other established criteria thresholds. The review evaluates the full, production configured system to determine if it correctly implements all system requirements, including embedded sustainment enablers. Product support IPT members, as well as independent sustainment subject matter experts, should participate to ascertain that the product support baseline has been established, documented and the:

- Supportability design features are mature enough to be incorporated into the design within the budget, schedule or other design constraints (e.g., weight, size, bandwidth).
- Product support is properly planned and implementation will meet sustainment objectives and requirements.
- System is supportable within the procurement, operations, and support budgets and fielded infrastructure.
- Initial product support package and supply chain are ready to support production output.
- Processes in place are adequate for sustainment performance metrics to help the program succeed in meeting user needs.

5.4.3.3. Engineering & Manufacturing Development Phase Results/Exit Criteria

The focus of this phase is to ensure the system design incorporates the critical supportability/ logistics requirements, develops the product support element capabilities, and demonstrates the key support and sustainment capabilities are mature. Implementing the process contained in figure 5.4.3.2.F1 produces the detailed supportability/logistics requirements and the initial designs. The conclusion of this phase results in the contractual documents required to continue into the Production and Deployment Phase as well as the system prototype logistics equipment and processes. The program should be able to demonstrate acceptable performance in the development, test & evaluation, and operational assessments, to include:

- Demonstrated reliability, availability, maintainability, and sustainment features
- Established and verified product support baselines
- Mature software design
- Acceptable interoperability

Table 5.4.3.3.T1 identifies the most critical documents that should incorporate or address supportability/ logistics considerations. The logistics related data in program deliverables should be updated prior to milestone decisions and to support the various major design reviews (e.g., CDR, and FCA). The key sustainment elements required for low rate initial production systems and initial operational test and evaluation (IOT&E) should be addressed in the LCSP which is summarized in the Acquisition Strategy. Materiel availability enabler driver initiatives should be included in the RFP as well as the Source Selection Plan.

From a logistics perspective, the exit documents should focus on the results of the maintenance planning process, the materiel availability driver initiatives, and their associated metrics. In addition to updating the support strategy, sustainment funding requirements, key logistics parameter and logistics testing criteria, the annual determination of the distribution of maintenance workloads required by statute, an auditable depot level maintenance core capability and workload assessment should be completed bi-annually.

Table 5.4.3.3.T1. Sustainment Considerations in EMD

Entry Documents:
Initial Capabilities Document and Capability Development Document
Acquisition Strategy
Acquisition Program Baseline
Preliminary Design Review Results
Developmental Test and Evaluation Report
Operational Test Plan and Test & Evaluation Master Plan (TEMP)
Life-Cycle Sustainment Plan

Exit Documents:
Update documents from MS B
Capability Production Document
Technical Data Rights Strategy
Approved Maintenance Plans
Life-Cycle Sustainment Plan

5.4.3.4. Sustainment Considerations in the Engineering and Manufacturing Development Phase

5.4.3.4.1. Sustainment Metrics

During this phase, the focus should be on achieving the objective range value estimate for each of the Sustainment KPP/KSAs, along with their supporting driver metrics, and on further analysis (including analysis of the results of any demonstrations that have been performed). The analysis should be performed to:

- Ensure the various metric performance values are consistent with each other as each is refined
- Ensure the design/production process does not degrade the system's ability to meet the sustainment metrics
- Identify the operation impacts the sustainment metrics enablers will have on mission success and materiel availability

The models for establishing and tracking projecting expected values should be refined and the requirements for the metrics should be further allocated to the equipment level. Key metrics data should be collecting and used to validate the models, evaluate technical performance, evaluate system maturity and determine the logistics footprint. The key enabling requirements to achieve the sustainment metrics should be included in the system specification and PBAs. Detailed test criteria should be developed for each metric (including any key dependent enabling technologies) to provide information about risk and risk mitigation as the development and testing continue. The sustainment test strategy/requirements should be documented in the TEMP.

5.4.3.4.2. Technology Refreshment and Obsolescence Management

The extensive life of our systems and rapid technology change has heightened the importance of technology refreshment and obsolescence management. Consequently, successful parts management necessitates the need to address diminishing manufacturing sources and material shortages in the proposal, design, and sustainment phases of a product (to include the systems and support elements). The PM should develop a proactive approach to effectively resolve obsolescence problems before they have an adverse impact on the LCC and system availability. The following are potential

approaches the PM should consider:

- Design features that facilitate change/insertion of new technology.
- Establishing a rigorous change management process for life-cycle support.
- Using performance-based logistics contracts that provide significant latitude to manage technology refreshment. This includes ensuring they are incentivized to maintain currency with state-of-the-art technology and use readily available items to avoid the high cost of diminishing manufacturing sources and materiel shortages over the systems life.

5.4.3.4.3. Sources of Support

DoD Components should operate an integrated, synchronized, total system supply chain to meet user requirements for information and materiel. Competition throughout the life cycle, including during sustainment, is integral to providing best value logistics processes. Consequently, per Public Law 111-23, major weapon systems shall, to the maximum extent practicable and consistent with statutory requirements, ensure maintenance and sustainment contracts are competitively awarded and given full consideration to all sources (including sources that partner or subcontract with public or private sector repair activities).

The Sustainment KPP/KSAs allow the acquisition and sustainment communities to focus their efforts from the users perspective, rather than focusing on any segment of the chain in isolation. This consistent focus on a common outcome (affordable materiel availability) across the supply chain reduces the potential for disconnects during the multiple hand offs across the various links in the supply chain. Consequently, in satisfying the user's needs under the total life-cycle system management approach, the PM is responsible for:

- Determining the appropriate set of metrics to align the various supply chain segments to achieve materiel availability. The specific metrics and their values should be determined regardless of who is executing the action to meet the user needs in the operational environment and be based on the system characteristics.
- Selecting the sources of support to sustain the system. Working with the maintenance community, the PM should use the most effective sources of support that optimize the balance of performance and life-cycle cost, consistent with statutory requirements and required military capability. The sources may be organic or commercial, but the focus should be on optimizing customer support and achieving maximum system availability at the lowest LCC. In making the determination, the PM shall (DoD Instruction 5000.02, Enclosure 8, paragraph 2.d.) work with the manpower community to determine the most efficient and cost effective mix of DoD manpower and contract support.
- Providing the mechanisms and product support elements (including technical data) to implement the source of support decisions. In doing so, the strategy and resources required to implement the strategy should foster and ensure

competition throughout the life of the system.

- Monitoring execution against the metrics to ensure the respective stakeholders are engaged in providing the system support to the user. Effective supply chain management requires data collection and data sharing within and between all elements of the supply chain (public and private). There should be a process to collect data throughout the manufacturing process and operations period so the data may be mined for product and process improvements using trend analysis to effectively communicate/collaborate with a shared understanding of the environment.

User and Provider Collaboration. Implementation of the life-cycle management approach places a premium on collaboration to promote user confidence in the logistics process in building a responsive, cost-effective capacity to ensure users get the materiel they need, when they need it, with complete status information. Supply chain management in particular requires PMs to collaborate with users (e.g., the force providers, the Combatant Commands, and the DoD Components of those commands) to determine optimal logistics strategies tailored to meet the users' needs and expectations and should produce a performance-based agreement codifying the negotiated user requirements and performance expectations (DoD Directive 5000.01). The PM should ensure user support is based on collaborative planning, resulting in realistic performance expectations established through performance-based agreements. These agreements should be negotiated in conjunction with the product support integrator, support providers, and the service providers (e.g., maintenance, supply, distribution centers, transportation providers).

Program managers can contract for performance-based sustainment as part of or as the total sustainment strategy. Contracts can be very powerful tools when support is focused on the customer and entire supply chain thereby mitigating or eliminating conflicting commodity priorities. Any sustainment contracts used should be focused to exploit supply chain processes and systems as well as to provide flexible and timely materiel support response during crises and joint operations. Regardless of the strategy taken, the PM must provide for long-term access to the data required for competitive sourcing of systems support and maintenance throughout its life cycle (see DoD Directive 4151.18 for additional information and guidance). The following major elements of the supply chain should be considered.

5.4.3.4.3.1. Maintenance

Program managers should determine the most effective levels of maintenance and sources based on materiel availability and cost factors. In early deployments the best value may be to use existing contractor capabilities for interim support. However core sustaining workload must be accomplished in Government owned facilities with Government owned equipment and personnel. If it has not already been completed, the PM should perform the analysis discussed in sections 5.2.1.2 and 5.4.2.2.2 to determine the maintenance source that complies with statutory requirements,

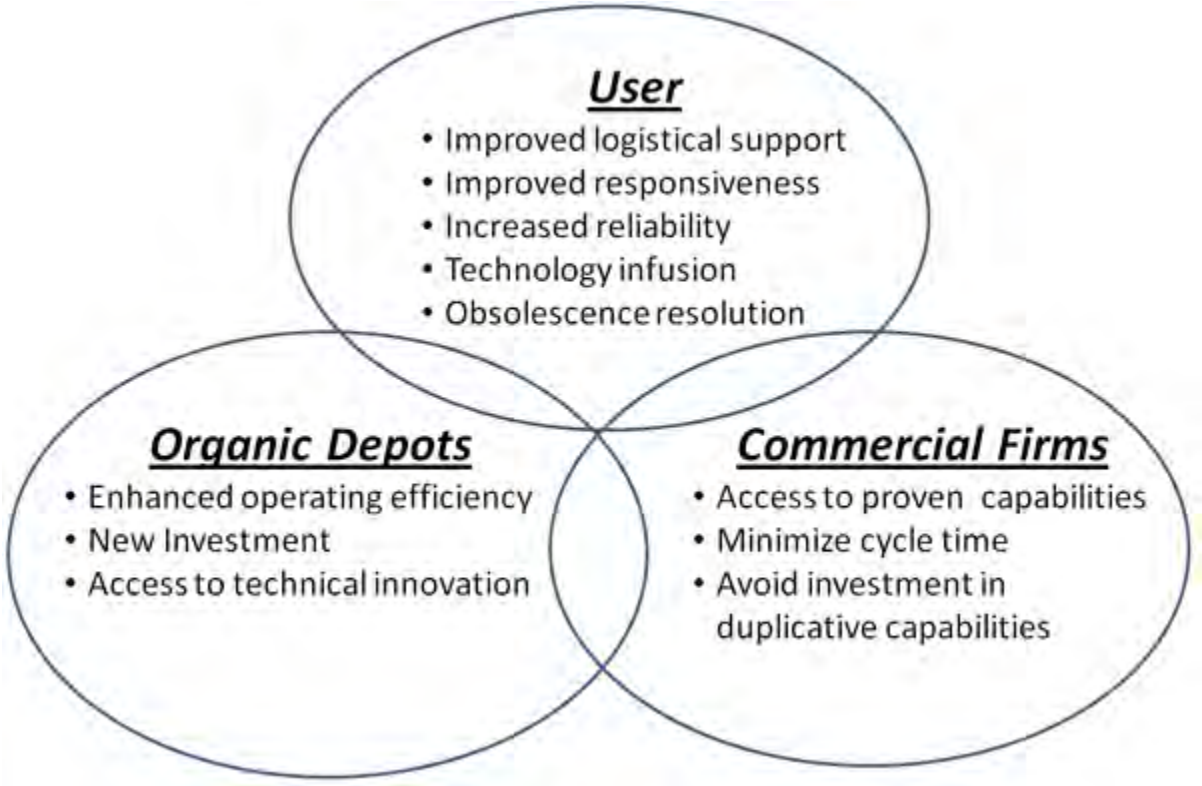
operational readiness and best value for non-core workloads.

Government and Industry Support Partnerships. In meeting the sustainment requirements, maintenance public private partnerships are the preferred arrangements for maintaining and repairing DoD weapon systems, hardware, equipment, and software. Public Private Partnerships can contribute to more effective DoD sustainment operations, can introduce innovative processes or technology, and enable the economical sustainment of organic capabilities. Delineating specific performance objectives in the mutual interests of both sectors, providing financial incentives for attaining the objectives, ensuring responsibilities are clearly assigned across the widest possible segment of maintenance workload requirements can result in:

- Improving DoD depot maintenance operations by combining the best of commercial processes and practices within the Department's own extensive maintenance capabilities
- Industry leveraging the depot's skilled artisans along with best commercial best practices
- Increasing availability at reduced life-cycle costs and increased reliability for new and legacy systems

Figure 5.4.3.4.3.1.F1 depicts some of the key benefits of well-designed public private partnerships. However, care is needed when third parties are involved. For example for information technology/software support some level of organic support needs to be resident and none of the support can be sent to non-approved third party countries (i.e. India, China etc.) without thorough analysis and State Department approval. Further examples and discussion of public private partnerships can be found in DoDI 4151.21 and on the Acquisition Community Connection web site .

Figure 5.4.3.4.3.1.F1. Public Private Partnership Opportunities



5.4.3.4.3.2. Supply

Supply requirements are determined as a part of the maintenance planning process. However, DoD policy gives the program manager latitude in selecting a source of supply support, including support management functions, that maximizes service to the user while minimizing cost. A framework for developing, improving, and conducting supply chain management activities to satisfy support element requirements is a vital link in systems sustainment because skilled labor and advanced technology repair equipment mean little without the right part in the right place at the right time. Consequently, the PM should select a source of supply support that gives sufficient control over financial and support functions to effectively make trade-off decisions that affect materiel availability and cost.

Competitive Process. Supply support may be included as part of the overall system procurement or as a separate competition. The competitive selection process should result in a contract with a commercial source and/or an agreement with an organic source that prescribes a level of performance in terms of materiel availability and cost. The PM may use a competitive process to select the best value supply support provider or include supply support in an overarching performance-based logistics support arrangement. While access to multiple sources of supply may be encouraged to reduce the risks associated with a single source, it is imperative that a single entity be

established as a focal point of responsibility. Particular attention should be given to prime vendor contracts for specific commodities and virtual prime vendor contracts for a wide range of parts support for specific subsystems. Additional guidance appears in DoD Directive 4140.1 and DoD 4140.1-R .

Organic Supply Source of Support. The PM should select organic supply sources of support when they offer the best value. (DoD Directive 5000.01, E1.1.17) When changing the support strategy for fielded equipment from organic to contractor support or from contractor to organic support, DoD owned inventory that is unique to that system should be addressed in the source of support decision.

5.4.3.4.3.3. Transportation

The PM is encouraged to determine the best overall support strategy for the customer to include the use of all available transportation alternatives, including those provided by original equipment manufacturers (OEMs), third party logistics providers, or commercial transportation providers. These alternatives may include the use of commercial transportation services and facilities to the maximum extent practicable; the use of organic transportation consistent with military needs; or the combination of both commercial and organic transportation to support customer requirements. As in supply support, the PM should strive to structure a support arrangement, such as performance-based logistics contracts, that will consolidate the responsibility for transportation in a single entity. Regardless of the approach taken, when making the transportation source decision the PM needs to ensure the entire end-to-end chain is considered including the "last mile" aspects along with any required implementing technology (e.g., IUID).

In considering transportation options, the PM should also plan for transition of the supply and distribution chain from normal operations to expeditionary operations in austere locations that are not served, at least initially, by commercial transportation services and facilities. Transportation alternatives in contractual arrangements must require the contractor to comply with established business rules, when the DoD organic distribution system is used in lieu of or with the commercial transportation service. All contractual arrangements requiring that deliveries be made using door-to-door commercial transportation must include a provision that requires vendors to notify the contracting officer or the contracting officer's designee when they are unable to use door-to-door commercial transportation and to request alternate shipping instructions. The contracting officer or contracting officer's designee must expeditiously provide alternate shipping instructions and make the appropriate contract price adjustments. For additional information, see the on-line Defense Transportation Policy Library .

Arms, Ammunition, and Explosives . PMs should refer to DoD 4500.9-R, Defense Transportation Regulation, Part 2 , and DoD Manual 5100.76-M , Physical Security of Sensitive Conventional Arms, Ammunition and Explosives (AA&E), for transportation and security criteria regarding the movement of arms, ammunition, and explosives. Contract provisions should apply to the prime contractor and all subcontractors.

5.4.3.4.4. Other Considerations

Design Impact . Design alternatives should continue to be considered to help mitigate sustainment risks and reduce LCC and logistics footprint as the design is refined.

Support Strategy . In refining and determining the detailed supportability requirements developed in the earlier phases, the PM should take into consideration the various alternatives that can be cost effectively implemented to achieve the Sustainment KPP and KSAs and to reduce program risks. The following are also aspects that should continue to be considered during this phase in designing and implementing the support strategy:

- **Interservice servicing agreements** to take advantage of joint capabilities by drawing support from other DoD Components and Allies. In developing the support strategy, the long term potential of Acquisition and Cross Servicing Agreements (ACSAs) to help reduce the logistics infrastructure and footprint should be considered. For further discussion including information on the legal authority for the acquisition and reciprocal transfer of logistic support, supplies, and services from eligible countries and international organizations, see section 11.2.3 and DoDD 2010.9 .
- **Adopting DoD Enterprise initiatives** to reduce LCC. For example adopting DoD's enterprise architecture for the information infrastructure, processes, data, data standards, business rules, operating requirements, and information exchanges can facilitate interoperability and LCC.

5.4.3.5. Best Practices during the System Engineering and Manufacturing Development Phase

Modeling and simulation combined with supportability analysis are important best practices to design and develop the individual product support elements required to implement the support strategy. During this phase they are applied to lower and lower levels of detail as the design matures. The supportability analysis should continue to be used to determine the relative cost vs. benefits of different support strategies (including the source of support decisions). The data should be refined and the results included in the LCSP and used to support contract negotiations. Use of Open Source Architecture (OSA) practices is another effective methodology to increase affordability and supportability. Code reuse is a force enabler that provides for more efficient software development programs that can cut across multiple program areas.

Once product support elements are developed and prototyped, modeling and simulation can also be used to provide confidence the sustainment metrics will mature to sufficient levels when the system and supply chain are deployed. This is accomplished with the use of models that take test results and predict likely capabilities. The same concepts are applied to provide confidence levels of what the enabling technologies will be able to achieve in the operational environment and identify any anticipated constraints. All of these factors are then used to project the mature sustainment metric values and their

associated confidence levels for the projected Concept of Operations.

5.4.4. Sustainment in the Production and Deployment Phase

5.4.4.1. Overview

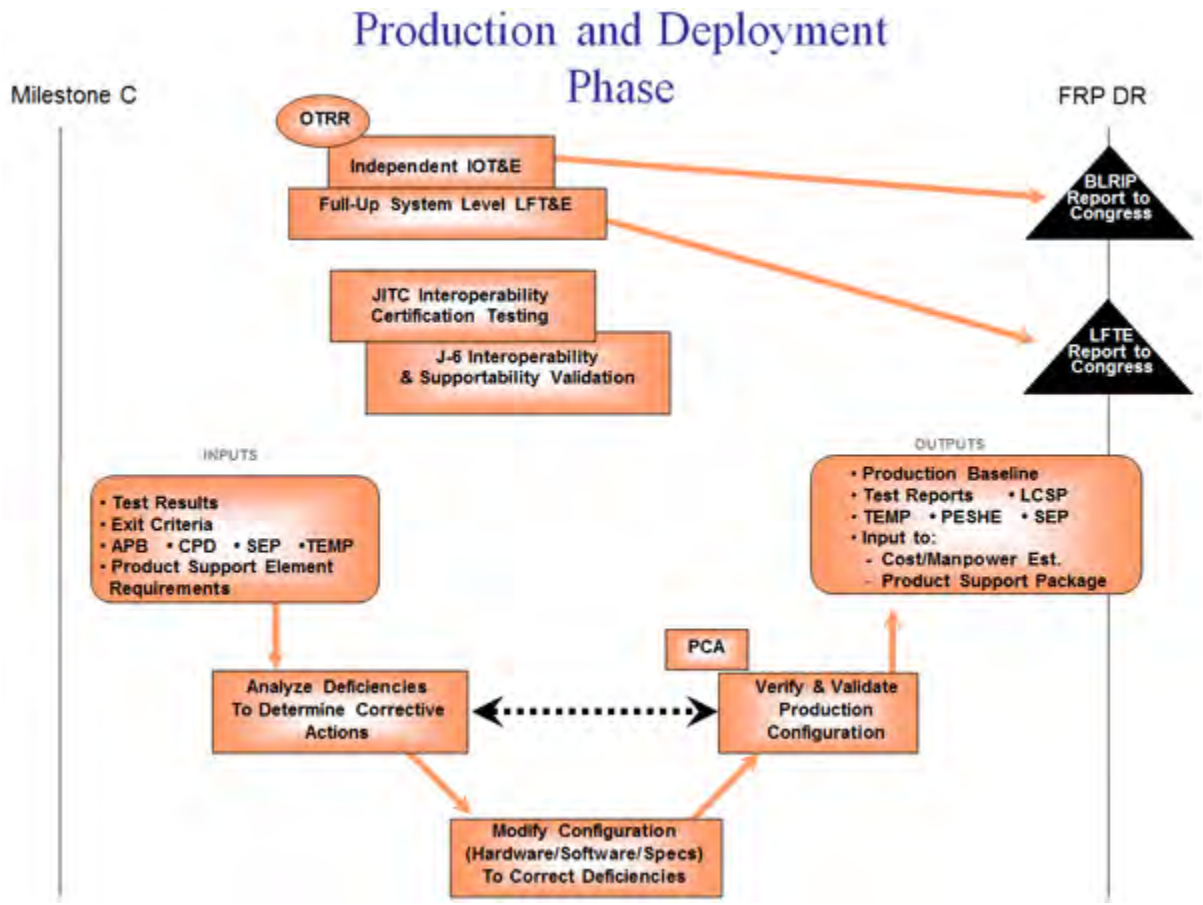
The logistics purpose in this phase is to achieve a materiel availability capability that satisfies mission needs. Milestone C authorizes entry into Low Rate Initial Production, at

which time the design should be mature. The supportability design feature requirements should have been verified and validated as operationally suitable and effective at an affordable cost. At this point, the support requirements should be fully defined and performance-based product support agreements and funding expectations documented and signed. Funding should also be identified and available for testing and implementation of the performance-based strategy. Once operational test and evaluations have determined the effectiveness, suitability, and supportability of the system, the full rate production and deployment decision is made.

5.4.4.2. Activities/Processes

During this phase, the emphasis is on finalizing equipment product support packages/ maintenance plans, managing and deploying the initial sustainment capabilities, and demonstrating the product support capabilities and effectiveness. Once they have been demonstrated, the emphasis is on fully fielding and implementing the sustainment capabilities to provide the users the capabilities identified in their requirements documents. Measuring the product sustainment package's effectiveness (including the associated supply chain) is an important aspect of the management responsibilities in this phase. Figure 5.4.4.2.F1 highlights the key phase activities.

Figure 5.4.4.2.F1. System Support Implications in the Production and Deployment Phase



5.4.4.2.1. Managing Product Support Package Fielding

The following are key program manager responsibilities in this phase:

- Ensuring actions are taken to provide the user support required to sustain the system within the budget provided, including highlighting to senior management the consequences and impacts on the Sustainment KPP/KSAs of budget constraints.
- Coordinating with the contractors, supply chain and operators to ensure each understands and is implementing responsibilities in accordance with the LCSP in an integrated fashion.
- Monitoring any changes to the design, operational environment and supply chain and adjusting the product support elements within the product support package accordingly.
- Looking for improvements to reduce the product support package cost.

During this phase, the reliability of contractor cost and performance data should be verified by monitoring contracts. Increased use of Defense Contract Management

Agency and Defense Contract Audit Agency in overseeing contracts should be considered.

5.4.4.2.2. Maintenance Supportability Considerations

10 USC 2464 requires the establishment of the capabilities necessary to maintain and repair systems and other military equipment required to support military contingencies (i.e., core capabilities) at Government-owned, Government-operated facilities not later than four years after achieving initial operating capability. During the production and deployment phase, it is imperative for the PMs and Program Executive Officers to ensure the prior planning for maintenance support is executed to meet the supportability requirements of the system and/or subsystems. If organic depot maintenance is a portion of the selected supportability strategy, it will require the activation of the requisite organic depot maintenance capabilities.

5.4.4.2.3. Life-Cycle Sustainment Plan

The LCSP should be used to help manage the program's fielding efforts. It should focus on the product support implementation plan and schedule, with emphasis on putting into place the continuous process improvement management structure to review processes and remove bottlenecks or constraints encountered by the user. The following aspects should be emphasized along with the projected sustainment metric values by fiscal year over the FYDP:

- The fielding plan details including any actions to adjust the product support package, ensure competition, and control costs.
- The analytical and management processes for how the sustainment performance will be measured, managed, assessed and reported as well as and achieve and maintain the sustainment requirements.
- The stakeholder roles in executing the sustainment strategy describing the relationships and responsibilities with key players, especially relative to the product support arrangements.

5.4.4.2.4. Measuring Sustainment Effectiveness

Under the total life-cycle systems management concept, the PM is responsible for the timely fielding of an effective product support package, measuring its effectiveness, and taking corrective actions when shortfalls are uncovered. The most effective time to catch problems is before the system is deployed, so including reliability, maintainability and supportability test requirements in the TEMP should be as important as other performance measures. Sustainment KPP/KSA driver metrics should be monitored thought out the test and deployment process to help provide confidence the system will achieve the sustainment objectives in an operational environment.

5.4.4.2.5. Pre-Initial Operational Capability Supportability Review

This review and its associated analysis should be performed at the DoD Component level in conjunction with the OTRR to:

- Confirm design maturity and configuration of the system
- Determine status of correction of any deficiencies identified
- Confirm configuration control
- Certify product support integrator/providers plan to meet user requirements
- Verify product support integrator/provider agreements/contracts and funding are in place

5.4.4.2.6. Technical Reviews in Production and Deployment

Many of the actions and subsequent results in this phase are reviewed during technical reviews and should be accomplished even if the specific referenced reviews do not occur. The actions and results are tied to the reviews to reflect the relative timeframe in which they should be accomplished.

5.4.4.2.6.1. Sustainment Considerations in the Operational Test Readiness Review (OTRR)

The OTRR is a product and process assessment to ensure the system can proceed into Initial Operational Test and Evaluation with a high probability of successfully completing operational testing. (See chapter 9 for additional information.) Many of the same actions used to prepare for the Test Readiness Review (TRR) should be used in preparation for this review. This test is critical because it provides the users the first real hands-on indication as to whether the system is operationally effective and suitable. Consequently, it is important the product support IPT members as well as independent sustainment subject matter experts participate in the review to ensure the test:

- Is properly planned and resourced (e.g., people, facilities, data systems, support equipment, and any other product support elements) to achieve the test objectives. The Pre-Initial Operational Capability Supportability Review should be used to support this process.
- Will verify and validate the key sustainment drivers to achieve the Sustainment KPP and KSAs are included. This should include ensuring system reliability, maintainability, and support performance features are included and demonstrated.
- Is structured to include as much of the product support package that will be used in the operational environment. Where this is not possible, prototypes should be used to gain early user feedback on the product support package.

5.4.4.2.6.2. Sustainment Considerations in the Physical Configuration Audit (PCA)

The PCA examines the end-item actual configuration as defined by the Technical Data

Package and sets the final production baseline under government control. Details can be found in section 4.2.16 , but in summary the audit verifies that design documentation matches the item specified in the contract. In addition to the standard practice of assuring product verification, the PCA confirms that manufacturing processes, quality control system, measurement and test equipment, product support, and training are adequately planned, tracked, and controlled. As such, this review should be used to ensure the "as-produced" system is compliant with sustainment requirements and objectives. To the extent lead times will allow, ordering the product support package elements should be delayed until this review to ensure they are being bought for the right configuration.

5.4.4.3. Production and Deployment Phase Results/Exit Criteria

The focus of this phase is to deploy the initial sustainment capabilities and once the system (both the system and its product support package) are demonstrated to be operationally suitable and effective to then fully deploy the system. This should be demonstrated by:

- The satisfactory achievement of the sustainment criteria in the Initial Operational Test and Evaluation (IOT&E) and other tests.
- Performance-based product support agreements being in place.
- A fully funded sustainment program in the budget.

Implementing the process depicted in figure 5.4.4.2.F1 provides the materiel required to gain full rate production/deployment approval and produce the product support elements to sustain the system. The conclusion of this phase results in a fully fielded and supported system. Table 5.4.4.3.T1 identifies the most critical documents that should address sustainment considerations. Key logistics information complied during this phase should be used to update the acquisition documents, along with the latest sustainment strategy based on the actual technology development progress and/or follow-on increments if an incremental acquisition strategy is used. Also, the sustainment related data and performance-based requirements should continue to be included in product and sustainment contracts and agreements to ensure the system is effectively supported.

Table 5.4.4.3.T1 Sustainment Considerations in Production and Deployment

Entry Documents:
Test and Evaluation Reports
Acquisition Program Baseline
Operational Test Plan and Test & Evaluation Master Plan (TEMP)
Life-Cycle Sustainment Plan
Exit Documents:
Update documents from MS C as appropriate

Physical Configuration Audit Report
Life-Cycle Sustainment Plan
Information Supportability Certification

5.4.4.4. Sustainment Considerations in the Production & Deployment Phase

All the product support elements should be considered and focus should be on refining and fielding them based on their demonstrated success and on confidence that the requirements will be achieved.

5.4.4.4.1. Sustainment Metrics

The results and experience demonstrated in all the tests (including follow-on operational test & evaluation (FOT&E)) and early operations should be considered in refining the metric estimates. This, along with key supply chain performance and effectiveness measures for similar fielded systems, should be used to increase the confidence levels for the PM's estimates. Supply chain performance, Sustainment KPP/KSAs, and key driver metrics should also be considered in the analysis. Special emphasis should be placed on tracking the metrics for the drivers of key enabler technologies that have been developed for the system or are critical for achieving the required materiel availability. Consideration should be given to revising the product support package and it’s agreements if major performance shortfalls are found.

5.4.4.4.2. Configuration Management

Special attention should be placed on configuration and data management, as design changes are made to ensure the product support package is developed and fielded to the same configuration(s) the user will be operating and supporting. Ensuring logistics and sustainment implications are considered and addressed during the Physical Configuration Audit (PCA), Physical Configuration Review, and Operational Test Readiness Review (OTRR) can increase the probability both the system and its support package are deployed in a coordinated fashion.

When multiple production baselines are deployed or if the full product support package is not deployed to support test or operations, the program manager should consider the most effective support method. The alternatives considered can include employing mixes of contractor and organic support over varied performance periods for each configuration. This may result in the consideration of multiple performance agreements and/or support strategies. In determining the best mix, the results from the Production Readiness Review (PRR) and System Verification Review (SVR) should be considered to ensure the product support elements are developed for all configuration / block increments.

5.4.4.4.3. Contractor Logistics Support/Contractors on the Battlefield (CLS/COTB) Integration, In-Theater

Contractors can provide logistics support over a wide range of options, from interim contractor support covering the initial fielding while the product support package is being deployed, to supporting specific limited operations, to full contractor support. When support strategies employ contractors in a battlefield environment, PMs should, in accordance with Joint Publication 4-0 Chapter 5 and DoD Component implementing guidance, coordinate with affected Combatant Commanders. This coordination must be carried out through the lead DoD Component and ensure functions performed by contractors, together with functions performed by military personnel, and government civilians, are integrated in operations plans (OPLANs) and orders (OPORDs). During this process the Combatant Commanders will:

- Identify operational specific contractor policies and requirements, to include restrictions imposed by international agreements;
- Include contractor related deployment, management, force protection, medical, and other support requirements, in the OPORD or a separate annex; and
- Provide this information to the DoD Components to incorporate into applicable contracts.

The intent of the coordinated planning is to ensure the continuation of essential services in the event the contractor provider is unable (or unwilling) to provide services during a contingency operation. Contingency plans are required for those tasks that have been identified as essential contractor services to provide reasonable assurance of continuation during crisis conditions. PMs should also coordinate with the DoD Component manpower authority in advance of contracting for support services to ensure tasks and duties that are designated as inherently governmental or exempt are not contracted.

5.4.4.5. Best Practices during the Production and Deployment Phase

5.4.4.5.1. Supportability Analysis

Supportability Analysis should continue to be expanded in depth and adjusted as necessary based on test results and operational experience. In examining additional information, a conscious decision has to be made as to whether or not the new data warrants a re-examination of previous analyses. Even if the change is not sufficient enough to warrant an adjustment to the support package, an analysis should be performed to assess the risk associated with the new information so key stakeholders can take risk mitigation steps.

Configuration control over the analysis and resulting data becomes important as the design changes. The program should take steps to ensure that as the system changes, the product support package is adjusted to take into account the various configurations

the user will encounter and the product support elements stay in sync.

Even well into operations, programs should evaluate opportunities for transitioning, in whole or part, to performance-based logistics contracts by examining opportunities to leverage public private partnerships. Experience has shown that, even with existing capitalized infrastructure in place, legacy programs can transition to outcome based contracts across the spectrum of subsystem or functional process support segments.

5.4.4.5.2. Modeling and Simulation

M&S continues to support the program improvement efforts by analyzing the impact of proposed design refinement, maintenance processes, and budget alternatives on the sustainment metrics/mission effectiveness. M&S should be used in assessing the alternatives of both the system and its support system (especially the enabling technologies), ensuring all critical metrics are considered in parallel and not at the expense of others. In addition, taking early operational results and predicting likely trends (with confidence levels) can be used to proactively anticipate problems so corrective actions can be taken as the system is fielded to minimize adverse impacts on the users. This also helps to provide confidence the critical sustainment metrics will mature to sufficient levels when the system and supply chain are fully deployed and to identify any anticipated constraints or limitations.

5.4.5. Sustainment in the Operations and Support Phase

5.4.5.5.2. Supportability Analysis

5.4.5.5.3. Modeling and Simulation

5.4.5.1. Overview

In the total life-cycle systems management concept, providing user support and managing the demilitarization/disposal of old systems are the PM's responsibilities. During this phase, the PM is the system focal point to the user and should continually assess the sustainability effectiveness of the fielded systems, adjusting the program as required to support the user.

Users require readiness and operational effectiveness (i.e., systems accomplishing their missions) in accordance with their design parameters in an operational environment. Systems, regardless of the application of design for supportability, suffer varying stresses during actual deployment and use. Consequently, the PM should apply the systems engineering processes used in acquisition throughout the entire life cycle. The difference is that during this phase actual use data including user feedback, failure reports, and discrepancy reports rather than engineering estimates are used.

While acquisition phase activities are important to designing and implementing a successful and affordable sustainment strategy, the ultimate measure of success is supporting the user after the system has been deployed for use. Accordingly, the PM and DoD Components should conduct periodic assessments of system support outcomes comparing actual vs. expected levels of performance and support. The assessments require close coordination with the user, support providers and appropriate systems engineering IPTs. They should be structured to:

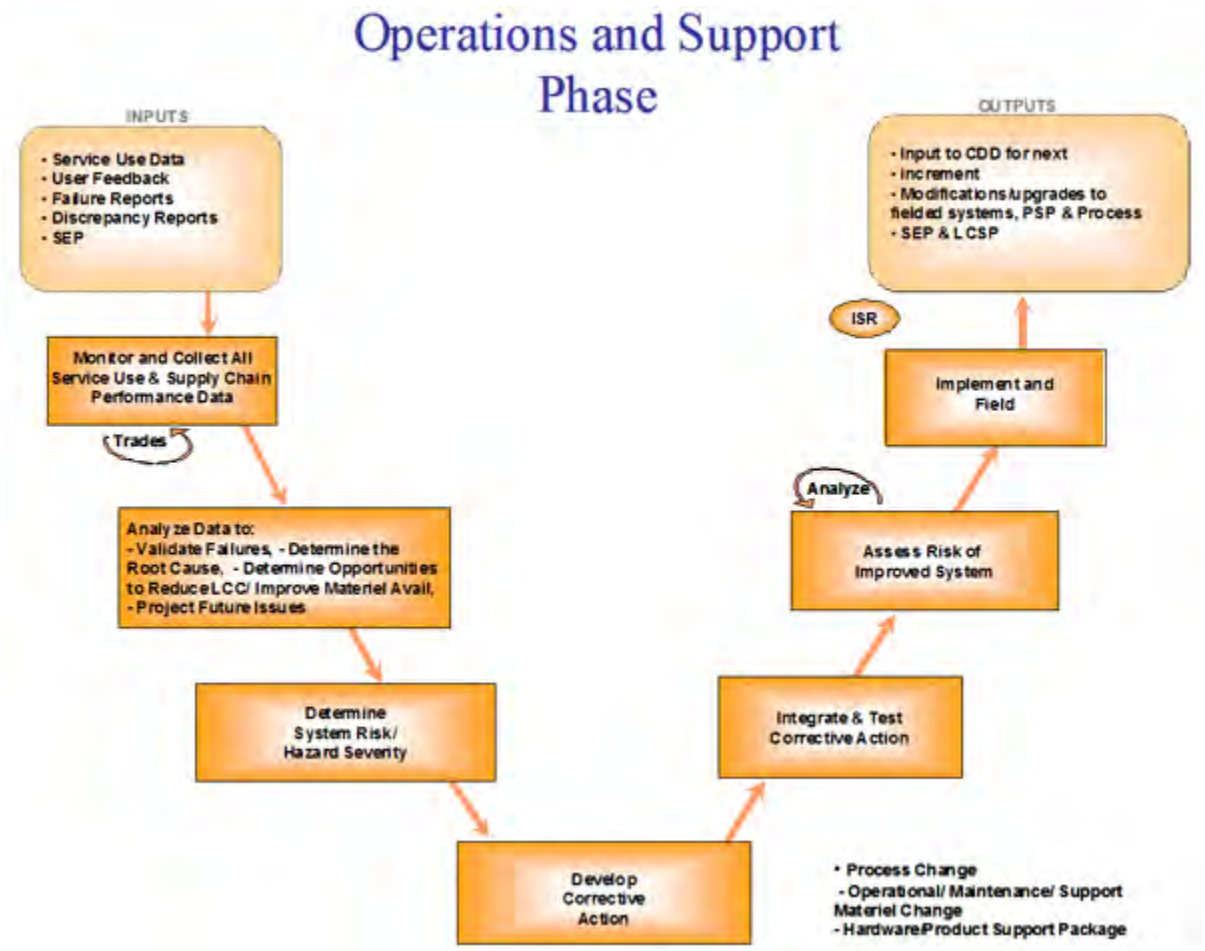
- Monitor system usage and supply chain against design baseline criteria and assumptions.
- Review and triage all use data and supplier data to determine operational hazards/safety risks, as well as readiness degraders.
- Develop alternatives to resolve critical safety and readiness degrading issues.
- Identify sub-optimal performers in the fielded product support system, and correct them through rebalanced product support elements or changes to the maintenance program.
- Enhance the performance and cost-effectiveness of the end-to-end supply chain to ensure materiel readiness continues to meet user needs.
- Identify redesign opportunities to enhance system effectiveness.

5.4.5.2. Activities/Processes

During this phase, the focus is on supporting the user by executing the sustainment program and on making adjustments based on effectiveness and operating conditions using systems engineering principles. However, the PM should not undertake depot maintenance source of support decisions without consultation with accountable military

department logistics officials to ensure the DoD Component depot maintenance 50 percent limitation statutory requirement is being met. Figure 5.4.5.2.F1 highlights the key sustainability and product support activities.

Figure 5.4.5.2.F1. System support implications in the Operations and Support Phase



5.4.5.2.1. Adjusting to meet User Needs

Under the total life-cycle systems management concept, the program manager continually assesses the system performance from the users perspective. The PM should use existing reporting systems and user feedback to evaluate the fielded system, focusing on performance outcomes meaningful to the user. (If existing reporting systems do not provide sufficient information, the PM should augment existing reporting systems by collecting critical data required to assess performance and, where necessary, work with the DoD Components to add the capabilities to the existing reporting systems.) The data should be analyzed, comparing performance expectations against actual performance, root causes of problems identified, and corrective actions

developed.

Potential corrective actions can be implemented through maintenance plan/requirement changes, process changes, modification of performance-based product support agreements, and/or design changes. The final decision for the corrective action selected will be determined by a balance between many factors, including but not limited to risk/safety, costs, schedule, user requirements and probability of success. (During this phase, the solution selected has a higher probability of success because more of the supportability analysis/RCM processes have the benefit of actuals, vice expectations, thereby reducing the amount of unknowns and eliminating many of the unknown-unknowns.) Regardless of the reason for the change (e.g., a required characteristic short fall, obsolescence, safety, changing user requirements or system design changes), the implementation/ fielding process will follow a tailored version of the Defense Acquisition Management System Framework.

5.4.5.2.2. In-Service Reviews (ISR)

The PM should conduct regularly scheduled In-Service Reviews (also known as Post IOC Reviews) with the users, assessing the current status, operational health and corrective actions to satisfy user operational needs based on user feedback and performance metrics. (See section 4.2.17 for additional information.) The ISR is a multi-disciplined product and process assessment to ensure the system is employed with well-understood and managed risk, so timely corrective actions can be taken. Leading into and during the reviews engineering, sustainment stakeholders (e.g., suppliers, representatives from primary supply chain providers, and the comptroller communities) and product support IPT members, as well as independent sustainment subject matter experts, should apply sound programmatic, systems engineering, and logistics management processes to:

- Assess product support performance against requirements and objectives. The focus should be on reliability, maintainability, and support problems (hardware and software) and their impact on safety and operational readiness. It should include an assessment of risk, readiness, and trends in a measurable form.
- Access the status of current system problems, solutions, and performance metrics. The metrics should include material reliability, material availability, mean down time, materiel ownership cost, and any additional useful sustainment metrics to substantiate in-service problems and budget priorities.
- Group system problems, safety, product support, and readiness issues by priority to form an integrated picture of in-service health, operational risk, system readiness, and future sustainment requirements. This information should be used to prioritize budget requirements (execution and out year) and future sustainment planning.
- Quantify and project system operational risk and system readiness levels based on current levels and current procurement, operations, and support budgets.
- Access the status of current initiatives and the program's responsiveness to meeting customer needs, including problem (discrepancy) report inflow,

resolution rate, and trends.

The reviews should be conducted at defined intervals to identify needed revisions and corrections, and to allow for timely improvements in the strategies to meet performance requirements for materiel readiness. At least initially, the In-Service Reviews will focus on the product support package fielding including the product support providers performance against the PBAs and other requirements. Consequently, the reviews with the users and product support service providers should be on a semi-annual basis as the support plans are executed (including transition from organic to contract support and vice versa, if applicable). After the system has been fully deployed, the frequency of these reviews should then be based on system performance (including trends), the pace of technology, obsolescence issues, and safety. The program's In-Service Reviews should be used to prepare for the DoD Component level assessments or reviews.

5.4.5.2.3. Formal DoD Component Post Deployment Reviews

Program assessments encompass and evaluate supportability, logistics, readiness, and sustainment planning and are conducted by each DoD Component to help ensure a solid life-cycle product support program. Assessments independent of the program office are management practices that have proved to be useful in managing product support risks by providing an impartial evaluation of a program's product support and sustainment implementation. The DoD Components have independently established formal assessment processes in DoD Component specific policies and instructions. The process names vary, but all are intended to assist the PM in the successful execution of his/her total life-cycle management responsibilities.

The DoD Components conduct Post Deployment Reviews beginning at Initial Operational Capability (IOC) and then nominally every three to five years or when precipitated by changes in requirements/design or performance problems. These periodic assessments verify whether the fielded system continues to meet or exceed thresholds and objectives for cost, performance, and support parameters approved at the full rate production decision. In addition to comparing actual versus expected levels of performance and support, the reviews should at minimum include:

- Product Support Integrator/ Product Support Provider's performance, including effectiveness of sustained materiel readiness implementation
- Product improvements incorporated
- Configuration control

5.4.5.2.4. Life-Cycle Sustainment Plan

Following the Full Rate Production Decision, the LCSP is the principle program document governing the systems management and execution. It describes the actions to be taken to meet the total system availability requirements based on measured performance in the operational environment. The plan documents the results of the

stakeholder actions and projects outcomes expected based on the budget and real world conditions emphasizing the:

- Sustaining Engineering processes for refining Product Support Package elements based on operation experience to maintain the systems sustainment metrics and control or reduce sustainment costs.
- Results of logistics assessments on how the system and supply chain are performing.
- Adjustments to the product support strategy including any changes to the Program Office or Product Support Arrangements.
- Projected sustainment metric values over the FYDP reflecting the expected results of corrective actions under way.
- Required and anticipated funding levels over the FYDP necessary to ensure acceptable affordability and availability rates to maintain mission capability against the relevant threats.

Once a program has been designated a "replaced system", a Replaced System Sustainment Plan will be generated which will require the program to work closely with the defense acquisition authority and the replacement system program manager. (See section 5.1.2.3)

5.4.5.3. Operations and Support Phase Results/Exit Criteria

Implementing the process depicted in figure 5.4.5.2.F1 results in proactive support to the user focusing optimized resources to meet operational needs. It can also result in new system requirements which would begin the **Life-Cycle Management System** process again.

The conclusion of this phase results in the disposal of the system following statutory regulations and policy. The PM should coordinate with DoD Component logistics activities and DLA, as appropriate, to identify and apply applicable demilitarization requirements necessary to eliminate the functional or military capabilities of assets (DoD 4140.1-R and DoD 4160.21-M-1). The PM should coordinate with DLA to determine property disposal requirements for system equipment, support assets, and by-products (DoD 4160.21-M).

5.4.5.4. Sustainment Considerations in the Operations and Support Phase

DoD Instruction 5000.02, Enclosure 2, paragraph 8 , includes "supply; maintenance; transportation; sustaining engineering; data management; configuration management; HSI; environment; safety (including explosives safety), and occupational health; protection of critical program information and anti-tamper provisions; supportability; and interoperability" within life-cycle sustainment. While not all of these elements are traditional product support elements, all are important considerations for the PM to take into account in supporting the user. Key is ensuring the entire program is assessed and adjustments are made as needed, based on changing user requirements/needs or

system design changes.

When assessing performance and revising agreements or support strategies, the process should encompass all configuration/block increments, and potential redesigns/ECPs to address changes required to address problems encountered in the operational environment. Emphasis should not only be on newly added support requirements, but also on addressing the support strategy in total across the entire platform and range of deployed configurations using the same analytical processes used in earlier phases.

The total life-cycle systems management and performance-based product support concept required by DoD 5000.01 necessitates that managing performance be focused on outcomes vs. segmented functional support organizational outputs. The PM is the focal point for ensuring that all program elements are considered and the respective stakeholders are engaged to support the user.

5.4.5.4.1. Sustainment Metrics

During this phase, the PM should measure, track and report the supply chain performance and its effectiveness, along with the sustainment metric drivers and the root cause of any performance shortfalls. Special emphasis should be placed on tracking the metrics for the drivers for the key enabler technologies that were developed for the system or are critical for achieving the required materiel availability.

5.4.5.5. Best Practices during Operations and Support

The following are important, but not the only, best practices to be used in this phase since the concepts previously spelled out still apply. In each case, the best practices involve Sustaining Engineering where the PM continually comparing performance against expectations using actual equipment and support performance data, to revise, correct and improve product support strategies to meet the users' requirements.

5.4.5.5.1. Continuous Process Improvement (CPI)

Often, due to revisions in funding, mission requirements, or other fact-of-life changes, logistics resources become out of balance or poorly synchronized. Therefore, PM efforts to achieve system availability while reducing costs should include periodic assessments and, where necessary, improvements of the support strategy and processes. While some system deficiencies can be addressed through system design, many can be more effectively resolved by adjusting the support strategy or processes. The continual application of supportability analysis, including condition based maintenance plus concepts, is an effective means of meeting evolving conditions and providing improved materiel availability.

Adjusting the maintenance requirements using RCM and CBM+ principles can be a very effective in optimizing the sustainment KPP and KSAs during the Operating and

Support Phase. Additional approaches useful to the PM in balancing logistics resources, decreasing repair cycle times, and/or improving readiness/availability include:

- Application of Lean, Six Sigma and Theory of Constraints Concepts.
- Updating the supply chain processes based on actuals. This can help balance logistics support through thorough review of readiness degraders, maintenance data, maintenance and support process implementation.
- Implementing properly incentivized performance-based agreements with support providers that encourage product support assessments and improvements based on comparisons between performance expectations against actual performance data.

5.4.5.5.2. Supportability Analysis

During this phase, the supportability analysis continues to focus on design changes regardless of the need for the change (e.g., reliability shortfall, obsolescence issue, safety concern) and adjusting the support package to accommodate the changes. In this process, care should be given to ensure the analysis encompasses all previous configuration/block increments across the entire platform and range of deployed configurations. In doing this, the entire support strategy should be addressed to look for opportunities to reduce the costs and logistics footprint.

Supportability analysis should also be used to adjust the support package based on how it is performing. A wide range of changes (including moving between overhaul and repair, improving off equipment diagnostic capabilities, transitioning to a commercial supply chain management system, etc.) should be considered in determining the best solution. The ability to continually compare performance against expectations using actual equipment and support performance data to drive data analyses and a RCM decision analysis is more efficient and reduces risks.

In both cases, use data is monitored/collected and analyzed using FMECA. Any failure, maintenance or operational issues are verified and root causes, risk and severity are determined. An analysis should then be performed to determine if the most cost effective solution is a:

- Maintenance change (either a preventative maintenance task (including scheduled inspections) or, if it is a non-critical failure, a corrective maintenance task. A Maintenance Plan analysis can help balance logistics support through thorough review of readiness degraders, maintenance data, maintenance procedures and commercial opportunities.
- Supply chain change.
- Product support element change.
- Change in the operations or use of the system (including the timeframe and conditions under which the limitations will be have to remain in effect).
- Design change.

In any proposed solution, the PM should work with the users to determine if the change and the timeframe are acceptable. Once the agreements have been reached, supportability analysis is used to adjust the appropriate product support package elements.

5.4.5.5.3. Modeling and Simulation

During this phase M&S supports the program improvement efforts by analyzing the impact of proposed continuous process improvements, ECPs, and budget alternatives on the sustainment metrics as well as mission effectiveness. M&S can be used in assessing the alternatives affecting the design and deployment of both the end item and it's support system. In addition, it can be used in a proactive mode to anticipate problems by taking use data and user feedback to:

- Project trends (with confidence levels) so actions are taken as conditions deteriorate to minimize adverse impacts on the users.
- Identify areas in the supply chain where performance is adversely affecting materiel availability, increasing LCC, or where there are opportunities for savings/improvements.
- Identify specific risk areas and ways to address/resolve root causes and reduce risk.

5.5. References

5.5.1. Handbooks and Guides

5.5.2. Other References

5.5.1. Handbooks and Guides

Product Support Manager Guidebook . This guide provides the PSM easy reference in addressing key requirements for managing product support across the entire life cycle of the weapon system. It serves as an operating guide to assist the PSM and the Acquisition Community with the implementation of product support strategies in aligning the acquisition and life cycle product support processes.

DoD Product Support Business Case Analysis (BCA) Guidebook. This guide provides overall guidance for conducting a Product Support BCA. It provides a standardized process and methodology for writing, aiding decision making, and providing analytical decision support for a Product Support BCA. The guide should be used in conjunction with other analytical tools and guidance in making product support decisions across the life-cycle.

Performance-Based Agreement Guidance. This guide and the Performance-Based Logistics section of Logistics Community of Practice (LOG CoP) provide guidance, explanations of Performance-Based Agreements, and related concepts for both

Commercial and Organic PBAs. It includes sample Performance-Based Agreements, templates, contractual incentives, a Performance-Based Agreement Toolkit and other resources. It also includes An End to End Customer Support PBA template that provides a common framework and a checklist to consider when undertaking a performance-based type agreement that may involve one or more supply chain support services as well as PBA terms and definitions. (**Note:** This guide is in the update process.)

Operating and Support Cost-Estimating Guide. This guide and DoD Manual 5000.4 , DoD Cost Analysis Guidance and Procedures provide procedures for life-cycle cost estimates. They explain the policies and procedures, focusing on the preparation, documentation, and presentation of cost estimates, and include and Operating and Support Cost element structure.

Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook . This guide consists of a compilation of the best practices for managing the risk of obsolescence. It identifies assorted measurement tools that may useful in analyzing and tracking the effectiveness of DMSMS programs.

CBM+ DoD Guidebook . This guide is an information reference as well as a tool to assist program and logistics managers with CBM+ project development, implementation, and execution. As a supplement to the CBM+ DoD Instruction, the Guidebook illustrates various complementary components of successful CBM+ implementation and describes management actions necessary to integrate technologies in order to increase reliability, availability, operational effectiveness, and maintenance efficiency.

Logistics Assessment Guidebook . This guide provides a structure for conducting Logistics Assessments and helps the DoD Components establish baseline assessment criteria specific to their weapon systems. It serves as an operating guide to put into place assessments that will help ensure there is adequate supportability planning, management, resource identification, and risk mitigation for each program at different life-cycle phases. (**Note:** Statute now requires Logistics Assessments to be independent. How ILAs are conducted is left to the DoD Components, however, pending formal policy, as general guidance, independent can be considered as individuals or organizations outside the line authority of the Program Manager or PMO staff for the program being evaluated.)

5.5.2. Other References

The Acquisition Community Connection (ACC) and the Logistics Community of Practice (LOG CoP) . The Acquisition Community Connection , sponsored by the Defense Acquisition University (DAU), is a tool to facilitate collaboration, sharing, and the transfer of knowledge across the DoD AT&L workforce. ACC is a collection of communities of practice centered on different functional disciplines within the acquisition community. The Logistics Community of Practice , is one of the communities currently

residing within the ACC framework. LOG CoP provides a number of resources for implementing life-cycle logistics. The community space also allows members to share (post to the website) their knowledge, lessons learned, and business case related material, so that the entire logistics community has access and can benefit.

Environment, Safety, and Occupational Health (ESOH) . DoD ESOH Guidance for systems acquisition programs can be found in Chapter 4 Systems Engineering and in the ESOH Special Interest Area on the Acquisition Community.

The DoD Guide For Achieving Reliability, Availability, Maintainability (RAM) . This document helps project managers and engineers to plan for and design RAM into systems. The guide focuses on what can be done in the systems engineering process to achieve effective levels of RAM, successfully demonstrate them during operational test and evaluation, and sustain them through the systems life cycle. It can be used to help capability document requirements writers and engineering organizations think through the top-level sustainment requirements for RAM early in the life cycle to ensure the system is sustainable and affordable throughout its life cycle.

The DoD Reliability, Availability, Maintainability & Cost (RAM-C) Rationale Report Manual . This manual describes the development of the RAM-C Rationale Report. It provides guidance in how to develop and document realistic sustainment Key Performance Parameter (KPP)/Key System Attribute (KSA) requirements and related supporting rationale. It addresses how the requirements must be measured and tested throughout the system life cycle as well as the processes that should be followed when developing the sustainment requirements.

DoD Instruction 4151.20 , Depot Maintenance Core Capabilities Determination Process . This instruction describes the policy, assigns responsibilities, and prescribes procedures to implement 10 USC 2464 and DoD Directive 4151.18 . It identifies the methodology to be used in determining the required core capabilities for depot maintenance and the associated workloads needed to sustain those capabilities.

DoD Instruction 5000.67 , Prevention and Mitigation of Corrosion on DoD Military Equipment and Infrastructure . This instruction establishes policy, assigns responsibilities, prescribes procedures and provides guidance for the establishment and management of programs to prevent or mitigate corrosion of DoD military equipment and infrastructure.

CBM+ Continuous Learning Module (CLL029) . The Condition Based Maintenance Plus (CBM+) module provides the learner with an overview and introduction to Depot Maintenance Management and Operations needed in DoD legacy systems. The module will cover DoD maintenance, CBM+ information and background, essential elements, CBM+ implementation, as well as managing initiatives and measuring success.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 6 - Human Systems Integration (HSI)

6.0. Overview

6.0. Overview

DoD acquisition policy requires optimizing total system performance and minimizing the cost of ownership through a "total system approach" to acquisition management by applying Humans Systems Integration elements to acquisition systems. (DoD Directive 5000.01).

6.0.1. Purpose

While Chapter 4 discusses systems engineering at large, this chapter specifically addresses the human systems elements of the systems engineering process. This chapter provides the Program Manager with the necessary background and understanding to design and develop systems that effectively and affordably integrate with human capabilities and limitations. It also makes the program manager aware of the staff resources available to assist in this endeavor.

6.0.2. Contents

This chapter has six major sections:

- Section 6.1 briefly reviews the total systems approach directed by DoD Directive

5000.01.

- Section 6.2 describes the importance of integration with respect to Human Systems Integration (HSI) implementation and its value in systems integration and risk management.
- Section 6.3 describes each of the domains of HSI: Manpower, Personnel, Training, Human Factors Engineering, Safety and Occupational Health, Survivability (Personnel), and Habitability. Each of these sub-sections contains an overview of the domain, addresses domain requirements, and a discussion of planning considerations.
- Section 6.4 follows with the implementation of HSI, to include formulation of the HSI strategy and the sequencing of expected HSI activities along the timeline of the Defense Acquisition Framework.
- Section 6.5 describes the human considerations associated with resource estimating and planning; it is the HSI complement to Chapter 3.
- Section 6.6 provides two reference lists for additional information .

6.1. Total System Approach

The total system includes not only the prime mission equipment and software, but also the people who operate, maintain, and support the system; the training and training devices; and the operational and support infrastructure. Human Systems Integration (HSI) practitioners assist program managers by focusing attention on the human part of the system and by integrating and inserting manpower, personnel, training, human factors engineering, environment, safety, occupational health hazards, and personnel survivability considerations into the Defense acquisition process. Consistent with DoD Instruction 5000.02, Enclosure 8 , when addressing HSI, the program manager must focus on each of the "domains" of HSI. These domains are outlined and explained beginning in Section 6.3 . The focus on the domains; however, should also include a comprehensive integration within and across these domains as outlined in Section 6.2 .

6.2 HSI - Integration Focus

The key to a successful HSI strategy is comprehensive integration across the HSI domains and also across other core acquisition and engineering processes. This integration is dependent on an accurate HSI plan and includes the comprehensive integration of requirements. The optimization of total system performance and determination of the most effective, efficient, and affordable design requires upfront

requirements analyses. The HSI domains (manpower, personnel, training, environment, safety and occupational health, human factors engineering, survivability, and habitability) can and should be used to help determine and work the science and technology gaps to address all aspects of the system (hardware, software, and human). The program manager should integrate system requirements for the HSI domains with each other, and also with the total system. As work is done to satisfy these requirements, it is vital that each HSI domain anticipate and respond to changes made by other domains or which may be made within other processes or imposed by other program constraints. These integration efforts should be reflected in updates to the requirements, objectives, and thresholds in the Capability Development Document s .

In today's Joint environment, the integration across systems of systems is necessary to achieve a fully networked Joint war fighting capability. The warfighter requires a fully networked environment and must be able to operate efficiently and effectively across the continuum of systems from initial recognition of the opportunity to engage through to mission completion. To accomplish this, HIS domains and human capabilities and constraints, should be considered in analytic assumptions, through system-of-systems analysis, modeling, and testing. This provides opportunities for integration, synchronization, collaboration, and coordination of capabilities to meet human centered requirements. A fully integrated investment strategy with joint sponsorship from the Materiel Development Decision on through the series of incremental developments may be required.

Values for objectives and thresholds, and definitions for parameters contained in the Capabilities Documents, Manpower Estimate , Test and Evaluation Master Plan , Acquisition Plan and Acquisition Program Baseline , should be consistent. This ensures consistency and thorough integration of program interests throughout the acquisition process.

6.2.1. Integrated Product and Process Development (IPPD) and Integrated Product Teams (IPTs)

DoD acquisition policy stresses the importance of IPPD. IPPD is a management technique that integrates all acquisition activities starting with capabilities definition through systems engineering, production, fielding/deployment and operational support in order to optimize the design, manufacturing, business, and supportability processes. At the core of the IPPD technique are IPTs. Human Systems Integration (HSI) should be a key consideration during the formation of IPTs. HSI representatives should be included as members of systems engineering and design teams and other IPTs that deal with human-oriented acquisition issues or topics. The various HSI domain experts should have the opportunity to work in an integrated structure to comprehensively impact the system. Domain experts working separately and in different IPT structures may make significant changes / inputs to the system without fully appreciating effects their changes may have on other domains . Only by working closely together can the HSI practitioners bring an optimum set of human interfaces to the Systems Engineering and Systems Acquisition Processes . HSI participants assist in IPPD as part of the IPTs

by ensuring the following:

- HSI parameters/requirements in the Initial Capabilities Document (ICD) , Capability Development Document , and Capability Production Document are based upon and consistent with the user representative's strategic goals and strategies. These parameters/requirements are addressed throughout the acquisition process starting in the Capabilities Based Assessment CBA and ICD and continuing throughout engineering design, trade-off analysis, testing, fielding/deployment, and operational support;
- Performance and HSI domain issues, identified in legacy systems and by design capability risk reviews, are used to establish a preliminary list for risk management. These issues should be evaluated and managed throughout the systems life cycle at a management level consistent with the hazard;
- The factors, tools, methodologies, risk assessment/mitigations, and set of assumptions used by the acquisition community to assess manpower, personnel, and training requirements, measure human-in-the-loop system performance, and evaluate safety, occupational health hazards, survivability, and habitability are consistent with what the functional communities/user representatives use to evaluate performance and establish performance based metrics;
- The factors used by the acquisition community to develop cost estimates are consistent with the 1) manpower and personnel requirements reported in the Manpower Estimate ; 2) training requirements reported in the DoD Component training plans; and 3) assessments of safety and health hazards documented in the Programmatic Environment, Safety, and Occupational Health Evaluation ; and,
- The Manpower Estimates and training strategies reported during the acquisition milestone reviews are reflected in the manning documents, training plans, personnel rosters, and budget submissions when the systems are fielded.

6.2.2. HSI Strategy, Risk, and Risk Mitigation

The development of an HSI strategy should be initiated early in the acquisition process, when the need for a new capability or improvements to an existing capability is first established. To satisfy DoD Instruction 5000.02, the program manager should have a plan for HSI in place prior to entering Engineering and Manufacturing Development. The program manager should describe the technical and management approach for meeting HSI parameters in the capabilities documents, and identify and provide ways to manage any HSI-related cost, schedule, or performance issues that could adversely affect program execution.

When a defense system has complex human-systems interfaces; significant manpower or training costs; personnel concerns; or safety, health hazard, habitability, survivability or human factors engineering issues; the program manager should use the HSI plan to describe the process to identify solutions. HSI risks and risk mitigation should be addressed in the program manger's risk management program.

The HSI plan should address potential readiness or performance risks and how these risks should be identified and mitigated. For example, skill degradation can impact combat capability and readiness. The HSI plan should call for studies to identify operations that pose the highest risk of skill decay. When analysis indicates that the combat capability of the system is tied to the operator's ability to perform discrete tasks that are easily degraded (such as those contained in a set of procedures), solutions such as system design, procedural changes or embedded training should be considered to address the problem. Information overload and requirements for the warfighter to dynamically integrate data from multiple sources can result in degradation of situational awareness and overall readiness. Careful consideration of common user interfaces, composable information sources, and system workload management will mitigate this risk. An on-board "performance measurements capability" can also be developed to support immediate feedback to the operators/maintainers and possibly serve as a readiness measure to the unit commander. The lack of available ranges and other training facilities, when deployed, are issues that should be addressed. The increased use of mission rehearsal, as part of mission planning, and the preparation process and alternatives supporting mission rehearsal should be addressed in the HSI plan. Team skills training and joint battlespace integration training should also be considered in the HSI plan and tied to readiness. Additionally, HSI issues should be addressed at system technical reviews and milestone decision reviews.

The program manager's Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE) describes the strategy for integrating ESOH considerations into the systems engineering process and defines how PESHE is linked to the effort to integrate HSI considerations into systems engineering. The PESHE also describes how ESOH risks are managed and how ESOH and HSI efforts are integrated. It summarizes ESOH risk information (hazard identification, risk assessment, mitigation decisions, residual risk acceptance, and evaluation of mitigation effectiveness). The HSI Strategy should address the linkage between HSI and ESOH and how the program has been structured to avoid duplication of effort.

DoD Directive 5000.01 prescribes supportability comparable to cost, performance, and schedule in program decision-making. Program managers should establish a logistics support concept (e.g., two level, three level), training plans, and manpower and personnel concepts, that when taken together, provide for cost-effective, total, life-cycle support. MIL-HDBK-29612-1A , -2A , -3A , & -4A may be used as a guide for Instructional Systems Development/Systems Approach to the training and education process for the development of instructional materials. Manpower, personnel, training analyses should be tied to supportability analyses and should be addressed in the HSI plan.

Program risks related to cost, schedule, performance, supportability, and/or technology can negatively impact program affordability and supportability. The program manager should prepare a "fallback" position to mitigate any such negative effect on HSI objectives. For example, if the proposed system design relies heavily on new technology or software to reduce operational or support manning requirements, the

program manager should be prepared with design alternatives to mitigate the impact of technology or software that is not available when expected.

6.3. Human Systems Integration Domains

6.3.1. Manpower

6.3.1.1. Manpower Overview

Manpower factors are those job tasks, operation/maintenance rates, associated workload, and operational conditions (e.g., risk of hostile fire) that are used to determine the number and mix of military and DoD civilian manpower and contract support necessary to operate, maintain, support, and provide training for the system. Manpower officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that optimize manpower and keep human resource costs at affordable levels (i.e., consistent with strategic manpower plans). Technology-based approaches used to reduce manpower requirements and control life-cycle costs should be identified in the capabilities documents early in the process. For

example, material-handling equipment can be used to reduce labor-intensive material-handling operations and embedded training can be used to reduce the number of instructors.

6.3.1.2. Manpower Parameters/Requirements

DoD Directive 5000.01 directs the DoD Components to plan programs based on realistic projections of the dollars and manpower likely to be available in future years. Manpower goals and parameters should be based on manpower studies and analysis. These studies and analyses should ensure that design options that reduce workload and ensure program affordability are pursued, and that lower-priority design features do not take precedence. Throughout the system life cycle, program managers should strive to keep manpower and the associated ownership costs at desired/targeted levels. Program managers should also preserve future-year resources rather than attempting to compete for additional funding later to address Manpower, Personnel or associated Training issues.

When there are Congressional or Administrative caps placed on military end strengths, the introduction of a new system or capability will require compensating reductions (trade-offs) elsewhere in the force structure or in the Individuals Account. Manpower officials should identify areas for offsets, or "bill-payers," for the new system and establish constraints based on available resources. If the new system replaces a system in the inventory, manpower officials should determine whether the constraints placed on the predecessor system also apply to the new system. They should consider the priority of the new system and determine if either additional resources will be provided, or if more stringent constraints will apply. Manpower authorities should consider the availability of resources over the life of the program and weigh competing priorities when establishing manpower constraints for acquisition programs. Reviews should account for all military and civilian manpower and contract support needed to operate, maintain, support, and provide training for the system over the entire life of the program.

Manpower can be a major determinant of program cost and affordability. In translating user requirements into a Defense Acquisition Program and its associated program documents, both the Program Managers and HSI practitioners should ensure that the requirements documents provide sufficient guidance to accurately move forward. The capability documents should identify any manpower constraints that, if exceeded, would require the Department to reconsider the utility of the program. The capability documents should specify the expected location of the system on the battlefield and the expected operational conditions (e.g., a high [or low] likelihood of hostile fire or collateral damage). These specifications affect early cost, manpower mix, training, personnel, and survivability requirements. Absent this guidance, further clarification should be requested from the users.

The capability documents should establish manpower parameters (objectives and thresholds) consistent with existing departmental constraints. If the program is

manpower intensive, it may be prudent to establish a manpower Key Performance Parameter (KPP) early in the acquisition process. Setting a KPP will ensure the system fit's within manpower parameters established by the Department, that agreed-upon resource thresholds are not exceeded, and that the system will not require additional resources from higher priority programs later in the acquisition process. A KPP should only be established if the adverse manpower effect of exceeding the KPP outweighs the overall benefits of the new capability. In all cases, manpower constraints and KPPs must be defendable and commensurate with the priority and utility of the new capability. Program Managers and HSI practitioners should work closely with the users and the sponsoring organization to ensure agreement on the appropriate parameters.

The capability documents should also address specific, scenario-based, factors that affect manpower, such as surge requirements, environmental conditions (e.g., arctic or desert conditions), and expected duration of the conflict. These factors are capability-related and directly affect the ability of the commander to sustain operations in a protracted conflict.

6.3.1.3. Manpower Planning

Manpower analysts determine the number of people required, authorized, and available to operate, maintain, support, and provide training for the system. Manpower requirements are based on the range of operations during peacetime, low intensity conflict, and wartime. They should consider continuous, sustained operations and required surge capability. The resulting Manpower Estimate accounts for all military (Active Reserve, and Guard), DoD civilian (U.S. and foreign national), and contract support manpower.

DoD Instruction 5000.02 requires the program manager to work with the manpower community to determine the most efficient and cost-effective mix of DoD manpower and contract support, and identify any issues (e.g., resource shortfalls) that could impact the program manager's ability to execute the program. This collaboration must be conducted within the Human Systems Integration (HSI) framework to ensure integration with the other HSI domains. The HSI lead for a program / project should be able to draw expertise from the manpower community to provide program assistance. Generally, the decision to use DoD civilians and contract labor in theater during a conflict where there is a high likelihood of hostile fire or collateral damage is made on an exception basis. In all cases, risk reduction should take precedence over cost savings. Additionally, the program manager should consult with the manpower community in advance of contracting for operational support services to ensure that sufficient workload is retained in-house to adequately provide for career progression, sea-to-shore and overseas rotation, and combat augmentation. The program manager should also ensure that inherently governmental and exempted commercial functions are not contracted. These determinations should be based on current Workforce Mix Guidance (DoD Instruction 1100.22).

Consistent with sections E1.1.4 and E1.1.29 of DoD Directive 5000.01, the program

manager must evaluate the manpower required and/or available to support a new system and consider manpower constraints when establishing contract specifications to ensure that the human resource demands of the system do not exceed the projected supply. The assessment must determine whether the new system will require a higher, lower, or equal number of personnel than the predecessor system, and whether the distribution of ranks/grade will change. Critical manpower constraints must be identified in the capability document s to ensure that manpower requirements remain within DoD Component end-strength constraints. If sufficient end-strength is not available, a request for an increase in authorizations should be submitted and approved as part of the trade-off process.

When assessing manpower, the system designers should look at labor-intensive (high-driver) tasks. These tasks might result from accessibility or hardware/ software interface design problems. These high-driver tasks can sometimes be eliminated during engineering design by increasing equipment or software performance. Based on a top-down functional analysis, an assessment should be conducted to determine which functions should be automated, eliminated, consolidated, or simplified to keep the manpower numbers within constraints.

Manpower requirements should be based on task analyses that are conducted during the functional allocation process and consider all factors including fatigue; cognitive, physical, sensory overload; environmental conditions (e.g., heat/cold), and reduced visibility. Additionally, manpower must be considered in conjunction with personnel capabilities, training, and human factors engineering trade-offs.

Tasks and workload for individual systems, systems-of-systems, and families-of-systems should be reviewed together to identify commonalities, merge operations, and avoid duplication. The cumulative effects of system-of-system, family-of-systems and related system integration should be considered when developing manpower estimates.

When reviewing support activities, the program manager should work with manpower and functional representatives to identify process improvements, design options, or other initiatives to reduce manpower requirements, improve the efficiency or effectiveness of support services, or enhance the cross-functional integration of support activities.

The support strategy should document the approach used to provide for the most efficient and cost-effective mix of manpower and contract support and identify any cost, schedule, or performance issues, or uncompleted studies that could impact the program manager's ability to execute the program.

6.3.2. Personnel

6.3.2.1. Personnel Overview

Personnel factors are those human aptitudes (i.e., cognitive, physical, and sensory

capabilities), knowledge, skills, abilities, and experience levels that are needed to properly perform job tasks. Personnel factors are used to develop the military occupational specialties (or equivalent DoD Component personnel system classifications) and civilian job series of system operators, maintainers, trainers, and support personnel. Personnel officials contribute to the Defense acquisition process by ensuring that the program manager pursues engineering designs that minimize personnel requirements, and keep the human aptitudes necessary for operation and maintenance of the equipment at levels consistent with what will be available in the user population at the time the system is fielded.

6.3.2.2. Personnel Parameters/Requirements

DoD Instruction 5000.02 requires the program manager to work with the personnel community to define the performance characteristics of the user population, or "target audience," early in the acquisition process. The program manager should work with the personnel community to establish a Target Audience Description (TAD) that identifies the cognitive, physical, and sensory abilities-i.e. capabilities and limitations, of the operators, maintainers, and support personnel expected to be in place at the time the system is fielded. When establishing the TAD, Human Systems Integration (HSI) practitioners should verify whether there are any recruitment or retention trends that could significantly alter the characteristics of the user population over the life of the system. Additionally, HSI analysts should consult with the personnel community and verify whether there are new personnel policies that could significantly alter the scope of the user population (e.g., policy changes governing women in combat significantly changed the anthropometric requirements for occupational specialties).

Per DoD Instruction 5000.02, to the extent possible--systems should not be designed to require cognitive, physical, or sensory skills beyond those found in the specified user population. During functional analysis and allocation, tasks should be allocated to the human component consistent with the human attributes (i.e., capabilities and limitations) of the user population to ensure compatibility, interoperability, and integration of all functional and physical interfaces. Personnel requirements should be established consistent with the knowledge, skills, and abilities (KSAs) of the user population expected to be in place at the time the system is fielded and over the life of the program. Personnel requirements are usually stated as a percentage of the population. For example, capability documents might require "physically accommodating the central 90% of the target audience." Setting specific, quantifiable, personnel requirements in the Capability Documents assist the establishment of test criterion in the Test and Evaluation Master Plan.

6.3.2.3. Personnel Planning

Personnel capabilities are normally reflected as knowledge, skills, abilities (KSAs), and other characteristics. The availability of personnel and their KSAs should be identified early in the acquisition process. The DoD Components have a limited inventory of personnel available, each with a finite set of cognitive, physical and psychomotor

abilities. This could affect specific system thresholds.

The program manager should use the target audience description (TAD) as a baseline for personnel requirements assessment. The TAD should include information such as inventory; force structure; standards of grade authorizations; personnel classification (e.g., Military Occupational Code / Navy Enlisted Classification) description; biographical information; anthropometric data; physical qualifications; aptitude descriptions as measured by the Armed Services Vocational Aptitude Battery (ASVAB)); task performance information; skill grade authorization; Military Physical Profile Serial System (PULHES); security clearance; and reading grade level.

The program manager should assess and compare the cognitive and physical demands of the projected system against the projected personnel supply. The program manager should also determine the physical limitations of the target audience (e.g., color vision, acuity, and hearing). The program manager should identify any shortfalls highlighted by these studies.

The program manager should determine if the new system contains any aptitude-sensitive critical tasks. If so, the program manager should determine if it is likely that personnel in the target audience can perform the critical tasks of the job.

The program manager should consider personnel factors such as availability, recruitment, skill identifiers, promotion, and assignment. The program manager should consider the impact on recruiting, retention, promotions, and career progression when establishing program costs, and should assess these factors during trade-off analyses.

The program manager should use a truly representative sample of the target population during Test and Evaluation (T&E) to get an accurate measure of system performance. A representative sample during T&E will help identify aptitude constraints that affect system use.

Individual system and platform personnel requirements should be developed in close collaboration with related systems throughout the Department and in various phases of the acquisition process to identify commonalities, merge requirements, and avoid duplication. The program manager should consider the cumulative effects of system-of-systems, family-of-systems, and related systems integration in the development of personnel requirements.

Consistent with DoD Instruction 5000.02, Enclosure 8 , the program manager should summarize major personnel initiatives that are necessary to achieve readiness or rotation objectives or to reduce manpower or training costs, when developing the acquisition strategy. The Life-Cycle Sustainment Plan should address modifications to the knowledge, skills, and abilities of military occupational specialties for system operators, maintainers, or support personnel if the modifications have cost or schedule issues that could adversely impact program execution. The program manager should also address actions to combine, modify, or establish new military occupational

specialties or additional skill indicators, or issues relating to hard-to-fill occupations if they impact the program manager's ability to execute the program.

6.3.3. Training

6.3.3.1. Training Overview

Training is any activity that results in enabling users, operators, maintainers, leaders and support personnel, to acquire, gain or enhance knowledge, skills, and concurrently develops their cognitive, physical, sensory, team dynamics and adaptive abilities to conduct joint operations and achieve maximized and fiscally sustainable system life cycles. The training of people as a component of material solutions, delivers the intended capability to improve or fill capability gaps.

Cost and mission effective training facilitates DoD acquisition policy that requires optimized total system performance and minimizing the cost of ownership through a "total system approach" to acquisition management (DoD Directive 5000.01).

The systems engineering concept of a purposely designed *total system* includes not only the mission system-equipment, but more critically, the people who operate, maintain, lead and support these acquired systems. Including the training, training systems; and the operational and support infrastructure.

The Human Systems Integration (HSI) Training Domain assists program managers throughout the acquired systems life cycle by focusing attention on the human interface with the acquired system, and by integrating and inserting manpower, personnel, training, human factors engineering, environment, safety, occupational health, habitability, and survivability as Systems Engineered elements into the Defense acquisition process consistent with DoD Instruction 5000.02, Enclosure 8

The Systems Engineered practice of continuous *application of human-centered methods and tools ensure* s *maximum operational and training effectiveness of the newly acquired system throughout its life cycle.* Systems Engineering in DoD Acquisition provides perspectives on the use of systems engineered/developed training approaches to translate user-defined capabilities into engineering specifications and outlines the role of the program manager in integrated system design activities.

In all cases, the paramount goal of training for new systems is to develop and sustain a ready, well-trained individual/unit, while giving strong consideration to options that can reduce life-cycle costs and provide positive contributions to the joint context of a system and provide a positive readiness outcome.

6.3.3.2. Regulatory Statutory Basis for Training

In order to achieve intended capabilities of new systems acquisition, enable joint integration, interoperability, testing and insure sustainment goals over the life-cycle of

weapon systems, training of user, operator, maintainer, and leader personnel will be performed. (ref: DoDI 5000.02 Enclosure 2 & 6, Title 10 USC Sections 2433 & 2535)

To facilitate timely, cost effective and appropriate training content, development and planning of training should be performed during the earliest phases (e.g. Material Solution and Technology Development Phases) of the acquisition processes, outlined within the AoA, System Training Plans (e.g. STRAPs, NTSPs or STPs) Acquisition Strategies(AS) and Acquisition Program Baselines (APB). (ref: DoDI 5000.02 Enclosure 4, 7 & 8, Title 10 Sections 2433 & 2435)

To insure appropriate training for new systems acquisition and traceability to life cycle sustainment costs estimates, systems engineering processes should assess training impacts of material decision trades and appropriately document. New Equipment Training (NET) plans (e.g. STRAPs, NTSPs and STPs) should identify service joint warfighting training requirements. Training planning and training cost estimates should be incorporated within the Cost Analysis Requirements Description (CARD) and Life Cycle Sustainment Plans (LCSPs). (ref: DoDI 5000.02 Enclosure 7, DoDD 5000.04-M & 5141.01, Title 10 Sections 2433 & 2435)

6.3.3.3. Training Planning

Training Planning assists the Program Manager in understanding acquisition program (new or upgrade) systems training as a key performance parameter to successfully integrating DoD Decision Support Systems, e.g. the Acquisition System (DoD 5000 Series), the Joint Capabilities Integration and Development System (JCIDS) and the Planning, Programming, Budgeting & Execution (PPBE) Process, and effectively translate joint capabilities into training system design features.

Initially, the JCIDS process should address joint training requirements for military (Active, Reserve, and Guard) and civilian support personnel who will operate, maintain, lead and support the acquired system.

Training programs should employ integrated cost-effective solutions, and may consist of a blend of capabilities that use existing training program insights and introduces new performance-based training innovations. This may include requirements for school and unit training, as well as new equipment training, or sustainment training. This also may include requirements for instructor and key personnel training and new equipment training teams.

Training planning should be initiated early, by the PM in coordination with the training community within the capabilities development process beginning with the Capabilities Based Assessment and Analysis of Alternatives which support development of the Initial Capabilities Document , informing the Material Development Decision to support the Material Solutions Analysis phase, and continues with development of the Capability Development Document .

Training should also be considered in collaboration with the other Human Systems Integration (HSI) domains in order to capture the full range of human integration issues to be considered within the Systems Engineering process.

Early training planning will inform the Capability Development Document and should characterize the specific system training requirements and identify the training Key Performance Parameter :

- Allow for interactions between platforms or unit's (e.g., through advanced simulation and virtual exercises) and provide training realism to include threats (e.g., virtual and surrogate), a realistic electronic warfare environment, communications, and weapons.
- Appropriate embedded training capabilities that do not degrade system performance below threshold values nor degrade the maintainability or component life of the system are preferred.
- That Initial Operational Capability (IOC) is attained and that training capabilities are met by IOC.
- An embedded performance measurement capability to support immediate feedback to the operators/maintainers and possibly to serve as a readiness measure for the unit commander.
- Training logistics necessary to support the training concept (e.g., requirements for new or upgrades to existing training facilities).
- Provide concurrent capability with actual equipment and training devices and systems.

The training community should be specific in translating capabilities into system requirements. They should also set training resource constraints. These capabilities and constraints can be facilitated and worked through system integration efforts in several of the other HSI domains. Examples are:

- The training community should consider whether the system be designed with a mode of operation that allows operators to train interactively on a continuous basis, even when deployed in remote / austere locations.
- The training community should consider whether the system be capable of exhibiting fault conditions for a specified set of failures to allow rehearsal of repair procedures for isolating faults or require that the system be capable of interconnecting with other (specific) embedded trainers in both static and employed conditions.
- The training community should consider whether embedded training capabilities allow enhancements to live maneuvers such that a realistic spectrum of threats is encountered (e.g., synthetic radar warnings generated during flight).
- The training community should consider whether the integrated training system be fully tested, validated, verified, and ready for training at the training base as criteria for declaring Initial Operational Capability.

From the earliest stages of development and as the system matures, the program

manager should emphasize training requirements that enhance the users capabilities, improve readiness, and reduce individual and collective training costs over the life of the system. This may include requirements for expert systems, intelligent tutors, embedded diagnostics, virtual environments, and embedded training capabilities. Examples of training that enhances users capabilities include:

- Interactive electronic technical manuals provide a training forum that can significantly reduce schoolhouse training and may require lower skill levels for maintenance personnel while actually improving their capability to maintain an operational system;
- Requirements for an embedded just-in-time mission rehearsal capability supported by the latest intelligence information and an integrated global training system/network that allows team training and participation in large scale mission rehearsal exercises can be used to improve readiness.

In all cases, the paramount goal of the training/instructional system should be to develop and sustain a ready, well-trained individual/unit/theater/joint, while giving strong consideration to options that can reduce life-cycle costs and provide positive contributions to the joint context of a system, where appropriate.

Training devices and simulators are systems that, in some cases, may qualify for their own set of HSI requirements. For instance, the training community may require the following attributes of a training simulator:

- Accommodate "the central 90 percent of the male and female population on critical body dimensions;"
- Not increase manpower requirements and considerations of reductions in manpower requirements;
- Consider reduced skill sets to maintain because of embedded instrumentation;
- Be High Level Architecture compliant;
- Be Sharable Content Object Reference Model (as in DoDI 13322.26) compliant;
- Be Test and Training Enabling Architecture (overview) compliant;
- Use reusable modeling and simulation devices and architectures.

The acquisition program will be specific in translating new system capabilities into the system and its inherent training requirements.

From the earliest stages of development and as the future system design matures, the program manager should emphasize training requirements that enhance the users capabilities, interoperability, improve readiness, and reduce individual and collective training costs over the life of the system. This may include requirements for expert systems, intelligent tutors, embedded diagnostics, virtual environments, and embedded training capabilities.

6.3.3.4. Development of Training Requirements

When developing the training system, the program manager shall employ transformational training concepts, strategies, and tools such as computer based and interactive courseware, simulators, and embedded training consistent with the programs acquisition strategy, goals and objectives and reflect the tenants outlined in the next generation training strategy.

In addition, the program should address the requirement for a systems training key performance parameter as described in the JCIDS Manual .

The USD (P&R), as a member of the Defense Acquisition Board (DAB), assesses the ability of the acquisition process to support the Military Departments, COCOMs, and other DoD Components acquisition programs from a manpower, personnel, and training readiness perspective.

The acquisition program will characterize training planning, development and execution within the Cost Analysis Requirements Description. Life Cycle Support Plans and Manpower Estimate Reports tailored to each document-type. These training summaries will capture - support traceability of planned training across acquisition and capability documents, and will include logistics support planning for training, training equipment and training device acquisitions and installations

A Special Note on Embedded Training. Both the sponsor and the program manager will provide analysis that demonstrates careful consideration to the use of embedded training as defined in DoD Directive 1322.18 : The sponsor's decisions to use embedded training will be determined very early in the capabilities assessment process. Analysis will be conducted to compare the embedded training with more traditional training media (e.g., simulator based training, traditional classroom instruction, and/or maneuver training) for consideration of a systems Total Operating Cost. The analysis will compare the costs and the impact of embedded training (e.g., training operators and maintenance personnel on site compared to off station travel to a temporary duty location for training).

6.3.4. Human Factors Engineering (HFE)

6.3.4.1. Mandatory Guidance

6.3.4.2. Overview

6.3.4.3. Parameters/Requirements

6.3.4.4. Application of Human Factors Engineering (HFE)

6.3.4.5. General Guidelines

6.3.4. Human Factors Engineering (HFE)

6.3.4.1. Mandatory Guidance

The program manager employs human factors engineering to design systems that require minimal manpower; provide effective training; can be operated, maintained and supported by users; and are suitable (habitable and safe with minimal environmental and occupational health hazards) and survivable (for both the crew and equipment). In

accordance with DoD Instruction 5000.02,

> *"The PM shall take steps (e.g., contract deliverables and Government/contractor IPT teams) to ensure ergonomics, human factors engineering, and cognitive engineering is employed during systems engineering over the life of the program to provide for effective human-systems interfaces and to meet HSI requirements. Where practicable and cost effective, system designs shall minimize or eliminate system characteristics that require excessive cognitive, physical, or sensory skills; entail extensive training or workload-intensive tasks; result in mission-critical errors; or produce safety or health hazards."*

The human factors that need to be considered in the integration are discussed below:

6.3.4.2. Overview

Human factors are the end-user cognitive, physical, sensory, and team dynamic abilities required to perform system operational, maintenance, and support job tasks. Human factors engineers contribute to the acquisition process by ensuring that the program manager provides for the effective utilization of personnel by designing systems that capitalize on and do not exceed the abilities (cognitive, physical, sensory, and team dynamic) of the user population. The human factors engineering community works to integrate the human characteristics of the user population into the system definition, design, development, and evaluation processes to optimize human-machine performance for operation, maintenance, and sustainment of the system.

Human factors engineering is primarily concerned with designing human-system interfaces consistent with the physical, cognitive, and sensory abilities of the user population. Human-system interfaces include:

- Functional interfaces (functions and tasks, and allocation of functions to human performance or automation);
- Informational interfaces (information and characteristics of information that provide the human with the knowledge, understanding and awareness of what is happening in the tactical environment and in the system);
- Environmental interfaces (the natural and artificial environments, environmental controls, and facility design);
- Cooperational interfaces (provisions for team performance, cooperation, collaboration, and communication among team members and with other personnel);
- Organizational interfaces (job design, management structure, command authority, policies and regulations that impact behavior);
- Operational interfaces (aspects of a system that support successful operation of the system such as procedures, documentation, workloads, job aids);

- Cognitive interfaces (decision rules, decision support systems, provision for maintaining situational awareness, mental models of the tactical environment, provisions for knowledge generation, cognitive skills and attitudes, memory aids); and,
- Physical interfaces (hardware and software elements designed to enable and facilitate effective and safe human performance such as controls, displays, workstations, worksites, accesses, labels and markings, structures, steps and ladders, handholds, maintenance provisions, etc.).

6.3.4.3. Parameters/Requirements

Human factors requirements, objectives, and thresholds should be derived from each of the Human Systems Integration (HSI) domains and should provide for the effective utilization of personnel through the accommodation of the cognitive, physical, and sensory characteristics that directly enhance or constrain system performance. In many cases, the interface design limitation may require tradeoffs in several of the other domains and vice, versa.

Cognitive requirements address the human's capability to evaluate and process information. Requirements are typically stated in terms of response times and are typically established to avoid excessive cognitive workload. Operations that entail a high number of complex tasks in a short time period can result in cognitive overload and safety hazards. The capability document s should specify whether there are human-in-the-loop requirements. This could include requirements for "human in control," "manual override," or "completely autonomous operations." Knowledge, skills and abilities for operators, maintainers and other support personnel continuously change with the increasing complexity of emerging systems. These requirements should be cross correlated with each of the HSI domains.

Physical requirements are typically stated as anthropometric (measurements of the human body), strength, and weight factors. Physical requirements are often tied to human performance, safety, and occupational health concerns. To ensure the users can operate, maintain, and support the system, requirements should be stated in terms of the user population. For instance, when the user requires a weapon that is "one-man portable," weight thresholds and objectives should be based on strength limitations of the user population and other related factors (e.g., the weight of other gear and equipment and the operational environment). For example, it may be appropriate to require that "the system be capable of being physically maintained by central 90% of both the male and female population, inclusive of battle dress, or arctic and Mission Oriented Protective Postures-Level 4 protective garments inside the cab," or that "the crew station physically accommodate 90% of the female/male population, defined by current anthropometric data, for accomplishment of the full range of mission functions."

Sensory requirements are typically stated as visual, olfactory (smell), or hearing factors. The Capability Development Document should identify operational considerations that affect sensory processes. For example, systems may need to

operate in noisy environments where weapons are being fired or on an overcast moonless night with no auxiliary illumination. Visual acuity or other sensory requirements may limit the target audience for certain specialties.

6.3.4.4. Application of Human Factors Engineering (HFE)

HFE plays an important role in each phase of the acquisition cycle, to include requirements development, system definition, design, development, evaluation, and system support for reliability and maintainability in the field. To realize the potential of HFE contributions, HFE must be incorporated into the design process at the earliest stages of the acquisition process (i.e., during the Materiel Solution Analysis and Technology Development phases). It should be supported by inputs from the other Human Systems Integration (HSI) domains as well as the other Systems Engineering processes . The right decisions about the human-machine interfaces early in the design process will optimize human and hence, total systems performance. HFE participation continues to each succeeding acquisition phase, continuing to work tradeoffs based on inputs from the other HSI domains and the hardware and software designs / adaptations. The HFE practitioners provide expertise that includes design criteria, analysis and modeling tools, and measurement methods that will help the program office design systems that are operationally suitable, safe, survivable, effective, usable, and cost-effective. In any system acquisition process, it is important to recognize the differences between the competencies (skills and knowledge) required for the various warfighters. Application of HFE processes will lead to an understanding of the competencies needed for the job, and help identify if requirements for knowledge, skills, and abilities (KSAs) exceed what the user can provide and whether the deficiency will lead to a training or operational problem. HFE tools and techniques can be used to identify the KSAs of the target audience and account for different classes and levels of users and the need for various types of information products, training, training systems and other aids. While it is critical to understand the information processing and net-centric requirements of the system, it is equally important to understand the factors affecting format and display of the data presented to the user to avoid cognitive overload. This applies equally to the system being designed as well as to the systems which will interface with the system. The system should not place undue workload or other stress on systems with which it must interface.

6.3.4.5. General Guidelines

Human Factors Engineering (HFE) principles, guidelines, and criteria should be applied during development and acquisition of military systems, equipment, and facilities to integrate personnel effectively into the design of the system. An HFE effort should be provided to: (a) develop or improve all human interfaces of the system; (b) achieve required effectiveness of human performance during system operation, maintenance, support, control, and transport; and (c) make economical demands upon personnel resources, skills, training, and costs. The HFE effort should be well integrated with the other Human Systems Integration domain participation, and should include, but not necessarily be limited to, active participation in the following three major interrelated

areas of system development.

6.3.4.5.1. Analysis

Identify the functions that must be performed by the system in achieving its mission objectives and analyze them to determine the best allocation to personnel, equipment, software, or combinations thereof. Allocated functions should be further dissected to define the specific tasks that must be performed to accomplish the functions. Each task should be analyzed to determine the human performance parameters; the system, equipment, and software capabilities; and the operational / environmental conditions under which the tasks will be conducted. Task parameters should be quantified where possible, and should be expressed in a form that permit's effectiveness studies of the human-system interfaces in relation to the total system operation. Human Factors Engineering high-risk areas should be identified as part of the analysis. Task analysis should include maintenance and sustainment functions performed by crew and support facilities. Analyses should be updated as required to remain current with the design effort.

6.3.4.5.2. Design and Development

Human Factors Engineering (HFE) should be applied to the design and development of the system equipment, software, procedures, work environments, and facilities associated with all functions requiring personnel interaction. This HFE effort should convert the mission, system, and task analysis data into a detailed design and development plan to create a human-system interfaces that will operate within human performance capabilities, facilitate / optimize human performance in meeting system functional requirements, and accomplish the mission objectives.

6.3.4.5.3. Test and Evaluation (T&E)

Human Factors Engineering (HFE) and the evaluation of all human interfaces should be integrated into engineering design and development tests, contractor demonstrations, flight tests, acceptance tests, other development tests and operational testing. Compliance with human interface requirements should be tested as early as possible. T&E should include evaluation of maintenance and sustainment activities and evaluation of the dimensions and configuration of the environment relative to criteria for HFE and each of the other Human Systems Integration domains . Findings, analyses, evaluations, design reviews, modeling, simulations, demonstrations, and other early engineering tests should be used in planning and conducting later tests. Test planning should be directed toward verifying that the system can be operated, maintained, supported, and controlled by user personnel in its intended operational environment with the intended training. Test planning should also consider data needed or provided by operational test and evaluation. (See section 9.5.2).

6.3.4.6. Life-Cycle Sustainment Plan

The program manager should summarize the steps planned to be taken (e.g., government and contract deliverables) to ensure human factors engineering (HFE) is employed during systems engineering over the life of the program to provide for effective human-system interfaces and meet HFE and other Human Systems Integration requirements.

6.3.5. Environment, Safety and Occupational Health (ESOH)

6.3.5.1. Environment, Safety and Occupational Health (ESOH) Overview

Each of the various military departments / services treat the three Human Systems Integration (HSI) domains of Environment, Safety, and Occupational Health differently, based on oversight and reporting responsibility within each of the services. DoD ESOH Guidance for systems acquisition programs can be found in Chapter 4, Systems Engineering, section 4.3.18.9 , and in the ESOH Special Interest Area on the Acquisition Community Connection . What is important to the HSI practitioner and the systems engineer is that these three domains are of vital importance to the HSI effort and must be integrated within the HSI effort. While the ESOH communities have unique reporting requirements that trace to National level mandates, the importance of integrating these domains in the HSI construct cannot be overemphasized. The human aspect brings a host of issues to a system that must be accommodated in each of these three areas and they must each be considered in consonance with the other HSI domains . How they are considered in an integrated manner is left to the Program Manager and Systems Engineering .

Environment includes the natural and manmade conditions in and around the system and the operational context within which the system will be operated and supported. This "environment" affects the human's ability to function as a part of the system.

Safety factors consist of those system design characteristics that serve to minimize the potential for mishaps causing death or injury to operators, maintainers and supporters or threaten the survival and/or operation of the system. Prevalent issues include factors that threaten the safe operation and/or survival of the platform; walking and working surfaces including work at heights; pressure extremes; and control of hazardous energy releases such as mechanical, electrical, fluids under pressure, ionizing or non-ionizing radiation (often referred to as "lock-out/tag-out"), fire, and explosions.

Occupational health factors are those system design features that serve to minimize the risk of injury, acute or chronic illness, or disability; and/or reduce job performance of personnel who operate, maintain, or support the system. Prevalent issues include noise, chemical safety, atmospheric hazards (including those associated with confined space entry and oxygen deficiency), vibration, ionizing and non-ionizing radiation, and human factors issues that can create chronic disease and discomfort such as repetitive motion diseases. Many occupational health problems, particularly noise and chemical

management, overlap with environmental impacts. Human factors stresses that create risk of chronic disease and discomfort overlap with occupational health considerations.

6.3.5.2. Environment, Safety and Occupational Health (ESOH) Hazard Parameters/Requirements

Environment, safety and health hazard parameters should address all activities inherent to the life cycle of the system, including test activity, operations, support, maintenance, and final demilitarization and disposal. Environment, safety and health hazard requirements should be stated in measurable terms, whenever possible. For example, it may be appropriate to establish thresholds for the maximum level of acoustic noise, vibration, acceleration shock, blast, temperature or humidity, or impact forces etc., or "safeguards against uncontrolled variability beyond specified safe limit's," where the Capability Document s specify the "safe limit's." Safety and health hazard requirements often stem from human factor issues and are typically based on lessons learned from comparable or predecessor systems. For example, both physical dimensions and weight are critical safety requirements for the accommodation of pilots in ejection seat designs. Environment, safety and health hazard thresholds are often justified in terms of human performance requirements, because, for example, extreme temperature and humidity can degrade job performance and lead to frequent or critical errors. Another methodology for specifying safety and health requirements is to specify the allowable level of residual risk as defined in MIL-STD-882D, "DoD Standard Practice for System Safety," for example, "There shall be no high or serious residual risks present in the system."

6.3.5.3. Environment, Safety and Occupational Health (ESOH) Planning

6.3.5.3.1. Programmatic Environment, Safety, and Occupational Health (ESOH) Evaluation (PESHE)

The Human Systems Integration Plan should recognize the appropriate timing for the PESHE and define how the program intends to ensure the effective and efficient flow of information to and from the ESOH domain experts to work the integration of environment, safety and health considerations into the systems engineering process and all its required products.

6.3.5.3.2. Health Hazard Analysis (HHA)

Health Hazards Analysis(HHA) should be conducted during each phase of the acquisition process beginning with a review of issues related to predecessor systems. During early stages of the acquisition process, sufficient information may not always be available to develop a complete HHA. As additional information becomes available, the initial analyses are refined and updated to identify health hazards, assess the risks, and determine how to mitigate the risks, formally accept the residual risks, and monitor the effectiveness of the mitigation measures. The health hazard risk information is documented in the PESHE. Health hazard assessments should include cost avoidance

figures to support trade-off analysis. There are nine health hazard issues typically addressed in a health hazard analysis (HHA):

- **Acoustical Energy.** The potential energy that transmits through the air and interacts with the body to cause hearing loss or damage to internal organs.
- **Biological Substances.** An infectious substance generally capable of causing permanent disability or life-threatening or fatal disease in otherwise healthy humans.
- **Chemical Substances.** The hazards from excessive airborne concentrations of toxic materials contracted through inhalation, ingestion, and skin or eye contract.
- **Oxygen Deficiency.** The displacement of atmospheric oxygen from enclosed spaces or at high altitudes.
- **Radiation Energy.** Ionizing: The radiation causing ionization when interfacing with living or inanimate mater. Non-ionizing: The emissions from the electromagnetic spectrum with insufficient energy to produce ionizing of molecules.
- **Shock.** The mechanical impulse or impact on an individual from the acceleration or deceleration of a medium.
- **Temperature Extremes and Humidity.** The human health effects associated with high or low temperatures, sometimes exacerbated by the use of a materiel system.
- **Trauma.** Physical: The impact to the eyes or body surface by a sharp or blunt object. Musculoskeletal: The effects to the system while lifting heavy objects.
- **Vibration.** The contact of a mechanically oscillating surface with the human body.

6.3.6. Survivability

6.3.6.1. Survivability Overview

Survivability factors consist of those system design features that reduce the risk of fratricide, detection, and the probability of being attacked; and that enable the crew to withstand natural and man-made hostile environments without aborting the mission or suffering acute chronic illness, disability, or death. Survivability attributes, as described in the Joint Military Dictionary (JP 1-02) , are those that contribute to the survivability of manned systems. In the HSI construct, the human is considered integral to the system and personnel survivability should be considered in the encompassing "system" context.

6.3.6.2. Survivability Parameters/Requirements

A Survivability / Force Protection Key Performance Parameter should be considered for any "manned system or system designed to enhance personnel survivability" when the system may be employed in an asymmetric threat environment. The Capability Document s should include applicable survivability parameters. This may include requirements to eliminate significant risks of fratricide or detectability, or to be survivable in adverse weather conditions and the nuclear, biological, and chemical (NBC)

battlefield. NBC survivability, by definition, includes the instantaneous, cumulative, and residual effects of NBC weapons upon the system, including its personnel. It may be appropriate to require that the system "permit performance of mission-essential operations, communications, maintenance, re-supply and decontamination tasks by suitably clothed, trained, and acclimatized personnel for the survival periods and NBC environments required by the system."

The consideration of survivability should also include system requirements to ensure the integrity of the crew compartment and rapid egress when the system is damaged or destroyed. It may be appropriate to require that the system provide for adequate emergency systems for contingency management, escape, survival, and rescue.

6.3.6.3. Survivability Planning

The Joint Capabilities Integration and Development System capability documents define the program's combat performance and survivability needs. Consistent with those needs, the program manager should establish a survivability program. This program, overseen by the program manager, should seek to minimize (1) the probability of encountering combat threats, (2) the severity of potential wounds and injury incurred by personnel operating or maintaining the system, and (3) the risk of potential fratricidal incidents. To maximize effectiveness, the program manager should assess survivability in close coordination with systems engineering and test and evaluation activities .

Survivability assessments assume the warfighter is integral to the system during combat. Damage to the equipment by enemy action, fratricide, or an improperly functioning component of the system can endanger the warfighter. The survivability program should assess these events and their consequences. Once these initial determinations are made, the design of the equipment should be evaluated to determine if there are potential secondary effects on the personnel. Each management decision to accept a potential risk should be formally documented by the appropriate management level as defined in DoD Instruction 5000.02 .

During early stages of the acquisition process, sufficient information may not always be available to develop a complete list of survivability issues. An initial report is prepared listing those identified issues and any findings and conclusions. Classified data and findings are to be appropriately handled according to each DoD Component's guidelines. Survivability issues typically are divided into the following components:

- **Reduce Fratricide.** Fratricide is the unforeseen and unintentional death or injury of "friendly" personnel resulting from friendly forces employment of weapons and munitions. To avoid these types of survivability issues, personnel systems and weapon systems should include anti-fratricide systems, such as Identification of Friend or Foe and Situational Awareness systems.
- **Reduce Detectability.** Reduce detectability considers a number of issues to minimize signatures and reduce the ranges of detection of friendly personnel and equipment by confounding visual, acoustic, electromagnetic, infrared/thermal,

and radar signatures and methods that may be utilized by enemy equipment and personnel. Methods of reducing detectability could include camouflage, low-observable technology, smoke, countermeasures, signature distortion, training, and/or doctrine.

- **Reduce Probability of Attack.** Analysts should seek to reduce the probability of attack by avoiding appearing as a high value-target and by actively preventing or deterring attack by warning sensors and use of active countermeasures.
- **Minimize Damage if Attacked.** Analysts should seek to minimize damage, if attacked, by: 1) designing the system to protect the operators and crewmembers from enemy attacks; 2) improving tactics in the field so survivability is increased; 3) designing the system to protect the crew from on-board hazards in the event of an attack (e.g., fuel, munitions, etc.); and, 4) designing the system to minimize the risk to supporting personnel if the system is attacked. Subject matter experts in areas such as nuclear, biological and chemical warfare, ballistics, electronic warfare, directed energy, laser hardening, medical treatment, physiology, human factors, and Information Operations can add additional issues.
- **Minimize Injury.** Analysts should seek to minimize: 1) combat, enemy weapon-caused injuries; 2) the combat-damaged systems potential sources and types of injury to both its crew and supported troops as it is used and maintained in the field; 3) the system's ability to prevent further injury to the fighter after being attacked; and 4) the system's ability to support treatment and evacuation of injured personnel. Combat-caused injuries or other possible injuries are addressed in this portion of personnel survivability, along with the different perspectives on potential mechanisms for reducing damage. Evacuation capability and personal equipment needs (e.g. uniform straps to pull a crew member through a small evacuation port are addressed here.
- **Minimize Physical and Mental Fatigue.** Analysts should seek to minimize injuries that can be directly traced to physical or mental fatigue. These types of injuries can be traced to complex or repetitive tasks, physically taxing operations, sleep deprivation, or high stress environments.
- **Survive Extreme Environments.** This component addresses issues that will arise once the warfighter evacuates or is forced from a combat-affected system such as an aircraft or watercraft and must immediately survive extreme conditions encountered in the sea or air until rescued or an improved situation on land is reached. Dependent upon requirements, this may also include some extreme environmental conditions found on land, but generally this component is for sea and air where the need is immediate for special consideration to maintain an individual's life. Survival issues for downed pilots behind enemy lines should be considered here.

The program manager should summarize plans for survivability in the Life-Cycle Sustainment Plan and address survivability risks and plans for risk mitigation. If the system or program has been designated by Director, Operational Test & Evaluation, for live fire test and evaluation (LFT&E) oversight, the program manager should integrate T&E to address crew survivability issues into the LFT&E program to support the Secretary of Defense LFT&E Report to Congress (10 USC 2366). The program

manager should address special equipment or gear needed to sustain crew operations in the operational environment.

6.3.7. Habitability

6.3.7.1. Habitability Overview

Habitability factors are those living and working conditions that are necessary to sustain the morale, safety, health, and comfort of the user population. They directly contribute to personnel effectiveness and mission accomplishment, and often preclude recruitment and retention problems. Examples include: lighting, space, ventilation, and sanitation; noise and temperature control (i.e., heating and air conditioning); religious, medical, and food services availability; and berthing, bathing, and personal hygiene.

Habitability consists of those characteristics of systems, facilities (temporary and permanent), and services necessary to satisfy personnel needs. Habitability factors are those living and working conditions that result in levels of personnel morale, safety, health, and comfort adequate to sustain maximum personnel effectiveness, support mission performance, and avoid personnel retention problems.

6.3.7.2. Habitability Parameters/Requirements

Habitability is one of several important factors included in the overall consideration of unit mission readiness. Per DoD Instruction 5000.02 , the program manager shall work with habitability representatives to establish requirements for the physical environment (e.g., adequate light, space, ventilation, and sanitation, and temperature and noise control) and, if appropriate, requirements for personal services (e.g., religious, medical, and mess) and living conditions (e.g., berthing and personal hygiene) if the habitability factors have a direct impact on meeting or sustaining performance requirements, sustaining mission effectiveness, or that have such an adverse impact on quality of life or morale that recruitment or retention rates could be degraded. Examples include requirements for heating and air-conditioning, noise filters, lavatories, showers, dry-cleaning and laundry.

While a system, facility, and/or service should not be designed solely around optimum habitability factors, habitability factors cannot be systematically traded-off in support of other readiness elements without eventually degrading mission performance.

6.3.7.3. Habitability Planning

The program manager should address habitability planning in the Life-Cycle Sustainment Plan and identify habitability issues that could impact personnel morale, safety health, or comfort or degrade personnel performance, unit readiness, or result in recruitment or retention problems .

6.4. Human Systems Integration (HSI) throughout the System Life Cycle

6.4.1. Research and Development (R&D), Studies, and Analyses in Support of Human Systems Integration (HSI)

Continuous application of human-centered research data, methods, and tools will ensure maximum operational and training effectiveness of the system. Continual analysis of system functionality provides data to help determine the best allocation of tasks to personnel, hardware, or software. Results guide human workload predictions, man-machine interface requirements, and procedural, software, and hardware innovations needed to ensure that the human element can fulfill and enhance total system performance. Each military department conducts human centered research. The products of this research form the basis for creating and maintaining military standards, design criteria, methodologies, tools, and data bases used when applying HSI to defense systems acquisition. Within each military department, HSI practitioners support ongoing concepts and studies that identify potential HSI impacts on operational effectiveness and resource needs of alternative solutions. Examples of these activities include field assessments, human performance modeling, simulations, and technology

demonstrations.

It is equally important that this research work be rolled into the front end analyses that lead to capability requirements. HSI considerations should be carefully examined during the capabilities-based assessment, and the planning for and execution of the Analyses of Alternatives. Failure to examine the human-centric issues up front may unduly complicate integration in a defined materiel solution.

6.4.2. Human Systems Integration (HSI) in the Capabilities Documents

The Initial Capabilities Document may seek to establish a new capability, improve an existing capability, or exploit an opportunity to reduce costs or enhance performance. The Initial Capabilities Document describes the key boundary conditions and operational environments that impact how the system is employed to satisfy the mission need. Key boundary conditions include critical manpower, personnel, training, environment, safety, occupational health, human factors, habitability, and survivability factors that have a major impact on system performance and life-cycle costs. The Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, or Facilities considerations and implications section of the Initial Capabilities Document should discuss all relevant domains of HSI .

HSI capabilities in the Capability Development Document should be specified in measurable, testable, performance-based language that is specific to the system and mission performance. Analyses and results conducted to determine the HSI requirements should be identified in and governed by other programmatic documentation (e.g., HSI plan, Systems Engineering Plan , Training Systems plan, or Manpower Estimate).

6.4.2.1. Refining Required Capabilities

As plans for the system mature, the capabilities documents should become more specific and reflect the integration of program objectives. The program manager should work with Human Systems Integration (HSI) practitioners and user representatives to translate HSI thresholds and objectives in the capabilities documents into quantifiable and measurable system requirements. The program manager should refine and integrate operational and design requirements so they result in the proper balance between performance and cost, and keep programs affordable. Additionally, system requirements should serve as the basis for developing engineering specifications, and should be reflected in the statement of work, contracts, Test and Evaluation Master Plan , and other program documentation. Over the course of the acquisition process, as trade-offs are made and plans for the system design mature, the capabilities documents should be updated to reflect a more refined and integrated set of parameters.

6.4.3. Engineering and Manufacturing Development Phase

The purpose of the Engineering and Manufacturing Development phase is to develop a

system or an increment of capability; reduce integration and manufacturing risk (technology risk reduction occurs during Technology Development); ensure operational supportability with particular attention to reducing the logistic footprint; implement Human Systems Integration; design for producibility; ensure affordability and protection of critical program information by implementing appropriate techniques such as anti-tamper; and demonstrate system integration, interoperability, safety and utility.

6.4.3.1. Solicitations and Source Selection

Human Systems Integration considerations should be clearly defined and given proper weight in solicitations and proposal evaluation guidelines provided to the government evaluation team. The record of contractors in Human Systems Integration should be an element of bid selection and contract performance criteria.

6.4.3.2. Systems Engineering

Once parameters are established in the Initial Capabilities Document and Capability Development Document , Requirements Definition Package or Capability Drop, it is the program manager's responsibility to ensure that they are addressed during the systems engineering process , included in the Human Systems Integration (HSI) Plan and the Systems Engineering Plan (SEP) , and properly considered during cost/performance trade-off analyses. Consistent with paragraph E1.1.29 of DoD Directive 5000.01 , the program manager applies HSI to optimize total system performance, operational effectiveness, suitability, survivability, safety, and affordability. Program managers should consider supportability, life-cycle costs, performance, and schedule comparable in making program decisions. Each program is required to have a comprehensive plan for HSI. It is important that this plan be included in the SEP or as a stand-alone HSI Plan as the program(s) may require. As required by DoD Instruction 5000.02, the program manager should take steps (e.g., contract deliverables and Government/contractor Integrated Product Teams) to ensure human factors engineering /cognitive engineering is employed during systems engineering. These steps should occur from the Materiel Solution Analysis phase through the life of the program to provide for effective human-machine interfaces, meet HSI requirements, and (as appropriate) support a system-of-systems acquisition approach. The program manager should also ensure that HSI requirements are included in performance specifications and test criteria. Manpower, Personnel, and Training functional representatives, as user representatives, participate in the systems engineering process to help produce the proper balance between system performance and cost and to ensure that requirements remain at affordable levels. Manpower, personnel, training, and supportability analyses should be conducted as an integral part of the systems engineering process throughout the acquisition life cycle, beginning with Materiel Solution Analysis and continuing throughout program development.

6.4.3.2.1. System Design

Human Systems Integration (HSI) plays a major role in the design process. Front-end

analysis methods, such as those described in MIL-HDBK-46855A , should be pursued to maximize the effectiveness of the new system. Initial emphasis should be placed on "lessons learned" from legacy, predecessor or comparable systems to help identify and eliminate characteristics in the new system that require excessive cognitive, physical, or sensory skills or high aptitudes; involve complex fault location or workload intensive tasks; necessitate excessive training; require proficiency training; or result in frequent or critical errors or safety/health hazards. Placing an emphasis on the "human-in-the-loop" ensures that systems are designed to operate consistent with human performance capabilities and limitations, meet system functional requirements, and fulfill mission goals with the least possible demands on manpower, personnel, and training. Moreover, sound HSI applications can minimize added costs that result when systems have to be modified after they are fielded in order to correct performance and safety issues.

6.4.3.2.2. Allocations

During systems engineering , analyses should be performed iteratively to define successively lower functional and performance requirements, to identify functional interfaces, and to allocate functions to components of the system (e.g., hardware, software, and human). Tasks should be allocated to the human component consistent with human attributes (i.e., capabilities and limitations) of the user population as established in the Target Audience Description. Requirements analysis should be conducted iteratively in conjunction with logical analysis to develop and refine system level performance requirements, identify external interfaces, and provide traceability among user requirements and design requirements. Human-systems interfaces should be identified as an outgrowth of the functional allocation process. Another product of the systems engineering process is a list of job tasks with performance/confidence levels. This information is used to further refine manpower, personnel and training requirements.

6.4.3.2.3. Specifications and Standards

It is primarily the responsibility of the program manager, with the assistance of the Integrated Product Teams, to establish performance specifications, design criteria standards, interface standards, and data specifications in the solicitation and resulting contract. Strong consideration should be given to establishing standards when uniform configuration is necessary for ease of operation, safety, or training purposes. For instance, a control panel or avionics suite may need to be standardized to enhance the ability of the user to access information and to respond quickly in an emergency situation. Standard features preclude the need to teach multiple (or conflicting) responses to similar tasks. Standardization is particularly important when a standard performance is required for safety reasons. For instance, rapid ejection from the cockpit should require standard procedures and tasks. If there are unique health hazard or survivability requirements, such as vibration or shock tolerances, extended temperature range, or noise levels, standardization may be the most efficient way to ensure that the system meets those special requirements. Preference should be given to specifications and standards developed under the Defense Standardization Program. Regulatory

occupational exposure standards create performance thresholds. However, use of guidance exposure criteria and ergonomic/Human Systems Integration guidelines should be considered to ensure personnel protection, promote efficiency, and anticipate more stringent standards that are likely to be required during the life cycle of the system.

Performance standards for operators, maintainers, both individual and team, are derived from the performance requirements of the total system. For example, human performance requirements (e.g., completion times or success rates) presumes that in order for the total system to achieve specified performance levels, the human will have to complete tasks or achieve performance objectives within specified confidence levels (usually expressed in terms of per cent of actions completed within a specified time-frame and/or error limit). The training/instructional system should be developed to ensure that operators can meet or exceed the personnel performance levels required to operate/maintain the systems. Additionally, manpower should be determined based on these same performance requirements. Operational tests should also be based on the same criteria.

6.4.4. Production and Deployment

The objective of this phase of the acquisition process is to achieve an operational capability that satisfies mission needs. Operational test and evaluation determines the effectiveness and suitability of the system.

6.4.5. Operations and Support (O&S)

The objective of this phase is the execution of a support program that meets operational support performance requirements and sustains the system in the most cost-effective manner over its life cycle. As required by DoD Directive 5000.01, planning for O&S should begin as early as possible in the acquisition process. Efforts during the O&S phase should be directed towards ensuring that the program meets and has the resources to sustain the threshold values of all support performance requirements. Once the system is fielded or deployed, a follow-on operational testing program, to assess performance, quality, compatibility, and interoperability, and identify deficiencies, should be conducted, as appropriate. Post fielding verification of the manpower, and information resulting from training exercises, readiness reports, and audits can also be used to assess the operational capability of the system. During fielding, deployment, and throughout operational support, the need for modifications to the system should be assessed.

6.5. Manpower Estimates

Manpower Estimate s address manpower affordability in terms of military end strength (including force structure and student end strength) and civilian work years beginning at Milestone B. Additionally, the use of contractor work years support should also be documented, where possible. Consistent with DoD Directive 5000.01 , DoD

Components should plan programs based on realistic projections of the dollars and manpower likely to be available in future years. When major manpower increases are required to support the program, or major manpower shortfalls exist, they will be identified as risks in the Manpower Estimate, and addressed in the risk assessment section of the Acquisition Strategy . Program risks that result from manpower shortfalls should be addressed in terms of their impact on readiness, operational availability, or reduced combat capability.

6.6. Additional References

6.6.1. DoD Publications

6.6.2. Discretionary Practices

6.6. Additional References

6.6.1. DoD Publications

The following DoD Directives and Instructions provide policy and direction:

- DoD Directive 1100.4 , "Guidance for Manpower Programs"
- DoD Directive 1322.18 , "Military Training"
- DoD Instruction 1100.22 , "Guidance for Determining Workforce Mix"
- DoD Instruction 1322.2 6 , " Development, Management, and Delivery of Distributed Learning"
- Training Transformation Implementation Plan
- CJCS Instruction 3170.01 , "Joint Capabilities Integration and Development System"
- The JCIDS Manual , "Operation of the Joint Capabilities Integration and Development System"
- Joint Military Dictionary (JP 1-02) , "Department of Defense Dictionary of Military and Associated Terms"
- AR 602-2 , "Manpower and Personnel Integration (MANPRINT) in the Systems Acquisition Process"

6.6.2. Discretionary Practices

The following military standards (MIL-STD), DoD Handbooks (DOD-HDBK), and Military handbooks (MIL-HDBK) can be used to support Human Systems Integration analysis:

- MIL-STD-882D , "Standard Practice for System Safety"
- MIL-STD-1472 , "DoD Design Criteria Standard: Human Engineering"
- MIL-STD-46855A , "DoD Standard Practice, Human Engineering Requirements for Military Systems, Equipment, and Facilities"
- DOD-HDBK-743 , "Anthropometry of U. S. Military Personnel"
- MIL-HDBK-759 , "Human Engineering Design Guidelines"

- MIL-PRF-29612 , "Performance Specification, Training Data Products"
- "A Guide for Early Embedded Training Decisions," U.S. Army Research Institute for the Behavioral and Social Sciences Research Product 96-06

DEFENSE ACQUISITION GUIDEBOOK
Chapter 7 - Acquiring Information Technology

7.0. Overview

7.0.1. Purpose

The goal of this chapter is to help program managers (PMs) and Sponsors/Domain Owners implement Department of Defense (DoD) policies intended to achieve fundamentally joint, net-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space. This chapter explains how the DoD is using a net-centric strategy to transform DoD warfighting, business, and intelligence capabilities. The chapter provides descriptions and explanations of many of the

associated topics and concepts. This chapter also discusses many of the activities that enable the development of net-centric systems, however, not all activities are the direct responsibility of the PM. Many activities reflect Department-level effort that occurs prior to, or outside of, the acquisition process. The detailed discussions of such a broad set of activities are presented here to help the PM understand the context of the capabilities described in the Joint Capabilities Integration and Development System (JCIDS) documents and required of the system under development.

7.0.2. Contents

This chapter contains ten sections that present the Program Manager with a comprehensive review of topics, concepts, and activities associated with the acquisition of Information Technology (IT), including National Security Systems (NSS).

Section 7.1, "Introduction," explains net-centric information sharing in the context of the discussions and requirements outlined in the various other sections of this chapter.

Section 7.2, "DoD Information Enterprise (DoD IE)," explains several important concepts that provide a foundation for acquiring net-centric Information Technology (including NSS). The overarching concept is that the DoD Enterprise Architecture (DoD EA) is used to describe and document current and desired relationships among warfighting operations, business, and management processes, the entities involved, and the information used. The IT architectures (i.e., IT solutions) are then aligned with the DoD EA.

DoD Architecture Framework (DoDAF) views that comprise architectures that are the DoD EA, and the DoD EA as a whole:

- Describe existing and desired capabilities.
- Provide a basis for interoperability and supportability reviews and certifications.
- Provide required components of the Capability Development Document (CDD) and Capability Production Document (CPD).
- Support portfolio management

The section discusses the DoD IEA and its role in helping PMs and Sponsors/Domain Owners describe their transition from the current environment to the future net-centric environment. Sections 7.3 through 7.10 elaborate on specific areas on which the Sponsors/Domain Owners and PMs should focus as they work to deliver and improve the reach, richness, agility, and assurance of net-centric capabilities.

Section 7.3, "Interoperability and Supportability of Information Technology and National Security Systems," explains interoperability and supportability, outlines the use of the Net-Ready Key Performance Parameter in these processes, and describes the process of building an Information Support Plan.

Section 7.4, "Sharing Data, Information, and Information Technology (IT) Service,"

provides guidance on implementing DoD Net-centric Data Strategy and Goals, and outlines Data, Information, and IT Services Sharing tasks as they relate to the acquisition process.

Section 7.5, "Information Assurance," explains the requirements for Information Assurance (IA) and provides links to resources to assist in developing an IA Strategy.

Section 7.6, "Electromagnetic Spectrum," offers a discussion and explanation of Spectrum Supportability.

Section 7.7, "Accessibility of Electronic and Information Technology," summarizes the requirements of the Workforce Investment Act of 1998, (Section 508 of the Rehabilitation Act (as amended in 1998)), regarding the procurement, development, maintenance, or use of electronics and IT that are accessible to people with disabilities.

Section 7.8, "Clinger-Cohen Act," helps PMs and Sponsors/Domain Owners understand how to implement Subtitle III of title 40 United States Code (formerly known as division E of the Clinger-Cohen Act (CCA) and hereinafter referred to as "Title 40/CCA") and associated regulatory requirements.

Section 7.9, "Post Deployment Reviews," discusses how the Department of Defense (DoD) uses the Post Implementation Review to inform Sponsors of the degree to which their IT/NSS investments closed the needed capability gaps.

Section 7.10, "Commercial, Off-The-Shelf (COTS) Solutions," provides insight into DoD guidance regarding acquisition of COTS software products.

In summary, this chapter should help PMs and Sponsors/Domain Owners understand and apply the tools of the DoD EA so that they can more effectively:

- Describe and measure the degree to which their programs are interoperable and supportable with the DoD IE.
- Ensure their programs employ and institutionalize approaches that make data visible, accessible, understandable, trusted, interoperable and responsive.
- Achieve the Department's objectives for IA.
- Ensure their programs will have assured interoperable access to electromagnetic spectrum.
- Achieve these goals within the constraints of the law and where possible, through the use of commercially available solutions.

7.1. Introduction

7.1. Introduction

The DoD Transformation Planning Guidance (April 2003) defines the desired outcome of transformation as "fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space." The goal of this chapter is to help PMs and Sponsors/Domain Owners implement the DoD policies that are intended to achieve this outcome. This introduction briefly explains net-centricity in context of the requirements outlined in the various other sections of this chapter.

Net-centric information sharing is "the realization of a robust, globally networked environment (interconnecting infrastructure, systems, processes, and people) within which data is shared seamlessly and in a timely manner among users, applications, and platforms. By securely interconnecting people and systems, independent of time or location, net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Users are empowered to better protect assets; more effectively exploit information; more efficiently use resources; and unify our forces by supporting extended, collaborative communities to focus on the mission."

The Department's approach for transitioning to net-centric operations and warfare and achieving the net-centric information sharing vision focuses on five key areas where increased attention and investment will bring the most immediate progress towards realizing net-centric goals:

- Data and Services Deployment
- Secured Availability
- Computing Infrastructure Readiness
- Communications Readiness
- NetOps Agility

This approach uses the Information Enterprise (IE) as "the organizing and transforming construct for managing information technology throughout the Department." It envisions moving to trusted network-centric operations through the acquisition of services and systems that are secure, reliable, interoperable, and able to communicate across a universal Information Technology infrastructure, including NSS. This Information Technology infrastructure includes data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities. The rest of this chapter describes the concepts, topics, and activities to achieve this transformation.

7.2. DoD Information Enterprise

7.2.1. Introduction

To provide a conceptual framework for this change, the Department has defined a Department of Defense Information Enterprise (DoD IE) as an organizing construct. The DoD IE consists of the Department of Defense information assets, processes, activities, and resources required to achieve an information advantage and share information across the Department and with mission partners. The DoD IE includes:

- The information itself, which is a key asset to the Department, and the Department's management over the information life cycle.
- The processes, including risk management, associated with managing information to accomplish the DoD mission and functions.
- Activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise.
- Related information resources such as personnel, funds, equipment, and information technology, including national security systems.

7.2.1.1. Information Enterprise Vision

The DoD IE vision is transforming the Department into an agile enterprise empowered by access to and sharing of timely and trusted information. The net-centric vision of the DoD IE is to function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing:

- A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise.
- An available and protected network infrastructure (the Global Information Grid (GIG)) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.

PMs and Sponsors/Domain Owners should use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global,

robust, survivable, maintainable, interoperable, secure, reliable, and user-driven to be operationally suitable, safe, effective, usable and affordable across the life cycle of the systems.

7.2.1.2. The Information Technology (IT) Infrastructure of the Department

The IT infrastructure of the Department is the GIG. The GIG is the Department's globally interconnected end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

Every DoD acquisition program having an IT component is a participant in the GIG. Each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG. Components, Combat Developers, Sponsors/Domain Owners, DoD Agencies, and PMs should consider the existing and planned capabilities of the GIG that might be relevant as they develop their architectures, JCIDS documentation (see the JCIDS Manual), and related program requirements.

7.2.1.3. The DoD Enterprise Architecture

An Enterprise Architecture describes the "current architecture" and "target architecture," and provides a strategy that will enable an agency to transition from its current state to its target environment. The Office of Management and Budget defines enterprise architecture as the explicit description and documentation of the current and desired relationships among business and management processes and IT. All DoD architectures, including warfighter, intelligence, business, and component enterprise architectures, are part of the DoD EA. The DoD EA is defined as a federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments, and the roadmap for transition to the target environment. As the Secretary of Defense's principal staff assistant for IT and information resources management, the DoD Chief Information Officer (DoD CIO) develops, maintains, and facilitates the use of the DoD EA to guide and oversee the evolution of the Department's IT-related investments to meet operational needs.

7.2.1.4. DoD Information Enterprise Architecture

The DoD Information Enterprise Architecture (IEA) provides a common foundation to support accelerated DoD transformation to net-centric operations and establishes

priorities to address critical barriers to its realization.

The published DoD IEA describes the integrated Defense Information Enterprise and the rules for the information assets and resources that enable it. The DoD IEA unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to existing policy. The DoD IEA highlights the key principles, rules, constraints and best practices drawn from collective policy to which applicable DoD programs, regardless of Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations. The DoD IEA provides information for applying it in architecture development and complying with it.

7.2.2. Mandatory Policies

7.2.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

7.2.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

7.2.2.3. CJCS Instruction 6212.01, "Interoperability and Supportability of Information Technology (IT) and National Security Systems"

7.2.2.4. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

7.2.2.5. DoD Directive 8000.01, "Management of the DoD Information Enterprise"

7.2.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

Extracts:

- *E1.1.9: Information Assurance. Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems.*
- *E1.1.10: Information Superiority. Acquisition managers shall provide U.S. Forces with systems and families of systems that are secure, reliable, interoperable, compatible with the electromagnetic spectrum environment, and able to communicate across a universal information technology infrastructure, including NSS, consisting of data, information, processes, organizational interactions, skills, analytical expertise, other systems, networks, and information exchange capabilities.*
- *E1.1.13: Interoperability. Systems, units, and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units, and forces and shall effectively interoperate with other U.S. Forces and coalition partners. Joint concepts and integrated [solution] architectures shall be used to*

characterize these interrelationships.

7.2.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

Extract:

- *The DoD Enterprise Architecture shall underpin all information architecture development. In accordance with DoD Directive 8000.01. . ., each integrated solution architecture shall have three views: operational, systems, and technical. The standards used to form the technical views of integrated architectures shall be selected from those contained in the current approved version of the DoD IT Standards Registry.*

DoD Instruction 5000.02 requires DoD acquisition programs to demonstrate consistency with GIG policies and architectures, to include relevant standards. (See Enclosure 5, Table 8, Title 40, Subtitle III/CCA Compliance Table) (The table indicates that the Net-Ready Key Performance Parameter in the Acquisition Program Baseline, required at Program Initiation for Ships, Milestone (MS) B, MS C, and the Full-Rate Production Decision Review (DR) (or Full Deployment DR), in part satisfies the requirement. The table also indicates that the Information Support Plan (ISP), in part, satisfies the requirement. An Initial ISP is required at Program Initiation for Ships and at MS B. A Revised ISP is due at the Critical Design Review (unless waived). And the ISP of Record is due at MS C.)

The DoD components under /DoD CIO leadership are required to develop an Enterprise Architecture that aligns with the DoD EA, and use their architecture and the DoD EA to guide the acquisition of IT.

Each IT acquisition program (or set of programs) is also required to develop a solution architecture comprised of DoDAF viewpoints determined to meet the needs of the PM (Fit-for-Purpose) and then use these products over the program life cycle to guide, monitor, and implement solutions in alignment with the DoD Enterprise Architecture as described in the DoD IEA.

Using these architectures and plans, the)/DoD CIO, in collaboration with Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and portfolio managers will conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources throughout the Planning, Programming, Budgeting, and Execution process.

7.2.2.3. CJCS Instruction 6212.01, "Interoperability and Supportability of Information Technology (IT) and National Security Systems"

It is DoD policy that all Information Technology (IT), including NSS, and major

modifications to existing IT will be compliant with the Title 40/CCA, DoD interoperability regulations and policies, and the most current version of the DoD Information Technology Standards Registry (DISR). Establishing interoperability and supportability in a DoD system is a continuous process that must be managed throughout the life cycle of the system. The following elements comprise the Net-Ready Key Performance Parameter (NR-KPP): 1) compliant architecture; 2) compliance with DoD Net-centric Data and Services strategies; 3) compliance with applicable GIG Technical Guidance; 4) verification of compliance with DoD information assurance requirements; and 5) compliance with supportability elements to include spectrum utilization and information bandwidth requirements, Selective Availability Anti-Spoofing Module (SAASM) and the Joint Tactical Radio System, as applicable. (See CJCSI 6212.01, Enclosure A, paragraph 1.e.)

7.2.2.4. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

This Directive defines a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability across the Department of Defense.

Extract:

- *1.3. Establishes the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.*
- *4.2. IT and NSS, of the DoD Global Information Grid (GIG), shall provide for easy access to information, anytime and anyplace, with attendant information assurance. The GIG architecture shall be used as the organizing construct for achieving net-centric operations and warfare.*

7.2.2.5. DoD Directive 8000.01, "Management of the DoD Information Enterprise"

This document reissues and renames DoD Directive 8000.01 and cancels 8100.01. The new DoD Directive 8000.01 requires the following:

- All aspects of the Defense Information Enterprise, including the Global Information Grid (GIG) infrastructure and enterprise services and solutions be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a net-centric environment, as envisioned in the National Defense Strategy, and be capable of effectively and efficiently supporting the Department's outcome goals and priorities.
- Investments in information solutions be managed through a capital planning and investment control process that is performance- and results-based; and provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.

- The capital planning and investment control process interface with the DoD key decision support systems for capability identification; planning, programming, budgeting, and execution; and acquisition.
- Review of all Information Technology (IT) investments for compliance with architectures, IT standards, and related policy requirements.
- Acquisition strategies appropriately allocate risk between the Government and contractor; effectively use competition; tie contract payments to performance; and, where practicable, take maximum advantage of commercial off-the-shelf and non-developmental item technology.
- Information solutions structured in useful segments, narrow in scope and brief in duration; each segment solves a specific part of the overall mission problem and delivers a measurable net benefit independent of future segments.

DoD Directive 8000.01 encourages pilots, modeling and simulation, experimentation, and prototype projects, appropriately sized to achieve desired objectives, and not be used in lieu of testing or acquisition processes to implement the production version of the information solution.

7.2.3. The Use of Architecture

7.2.3.1. Compliance with the DoD Enterprise Architecture (DoD EA)

7.2.3.2. Compliance with the DoD Information Enterprise Architecture (IEA)

7.2.3.3. DoD Chief Information Officer (CIO) Use of the DoD Information Enterprise Architecture (IEA)

7.2.3. The Use of Architecture

1. Architectures are tools to improve the operational processes, infrastructure, and materiel solutions of the Department. Architecture-enabled solutions should facilitate improved interoperability, better information sharing, tighter compliance, leaner processes, reduced costs, and more effective mission accomplishment.
2. The DoD Enterprise Architecture (EA) is a federation comprised of the DoD enterprise and DoD Component level architectures to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the Department of Defense, and provide a sound basis for transition from the existing environment to the future. Solutions should conform to the DoD EA.
3. Solution architectures should be developed for material and non-material initiatives and capabilities that deliver functionality for the DoD information enterprise.
4. All information technology investments, including those related to National Security Systems, should be reviewed for compliance with the DoD Enterprise Architecture and applicable approved solution architectures, and alignment with

the Federal Enterprise Architecture (FEA).

5. An architecture is considered a strategic information asset and should be appropriately secured, shared and made available to any DoD user or mission partner to the maximum extent allowed by law and DoD policy.

7.2.3.1. Compliance with the DoD Enterprise Architecture (DoD EA)

Detailed compliance requirements for the DoD EA are contained in the DoD IEA. To comply with the DoD EA, an information technology (IT)-based initiative or an acquisition program, throughout its life cycle should:

- Follow the DoD Architecture Framework (DoDAF) guidance in creating architectural views. This guidance is met by creating an architecture that captures the specific data needed to support decision making. The specific data is predicated by explicitly identifying the intended use and scope of the architecture in question.
- Meet the DODAF Meta-model (DM2) Physical Exchange Specification (PES) requirements for sharing/reusing architecture data. This requirement is met through the program's creation of XML, based on the PES XSD for the necessary and foundational DM2 concepts and through contributing new reusable architecture data (if any) to the DM2.
- Meet the DoD Information Technology (IT) Standards Registry (DISR) requirements in selecting technologies and standards. This requirement is met by defining and implementing capabilities, based on technologies and standards contained within the DISR. Meeting this requirement should be validated at every milestone. When building systems, requests for proposals and contract statements of work should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents (Intelink account required) are translated into clear contractual requirements. In addition, requests for proposals and contract statements of work should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards and GIG Technical Profiles mandated in DISR.
- Meet the DoD Net-Centric Data Strategy requirements and intent. Make explicit the data that is produced and used by the program's implemented operations. Provide the associated metadata, and define and document the program's data models. This requirement is met by:
    - Describing the metadata that has been registered in the DoD Data Metadata Registry for each data asset used and for each data asset produced (i.e., data for which the program is the Source Data Authority).
    - Providing the documented data models associated with the program.
- Comply with the DoD Information Enterprise Architecture (IEA).
- DTM 09-013, *Registration of Architecture Description in the DoD Architecture Registry System (DARS)* mandates the registration of architectures through the DARS portal so these architectures can be leveraged as information assets.

Architectures developed in the DoD are more easily leveraged when they are widely visible and accessible across DoD. Widely visible and accessible architectures result in increased information sharing, reuse, and a more common understanding of the bigger picture. A fully federated EA can only be realized if all architectures in DoD are properly registered in DARS with appropriate links and relationships. DARS is located at https://dars1.army.mil/IER2/ and includes a tutorial for the registration process.

- Mandatory Core Designated DoD Enterprise Services are common, globally-accessible services designated by the DoD CIO and mandated for use by all programs and initiatives. No capability comparable to the Mandatory Core Designated DoD ES is to be developed unless there is a waiver granted by the DoD CIO.

7.2.3.2. Compliance with the DoD Information Enterprise Architecture (IEA)

The DoD Information Enterprise Architecture (IEA) provides a common foundation to support transformation of the DoD to net-centric operations. The common foundation is presented as a set of Principles and Rules that guide and constrain operations to facilitate a coherent movement towards net-centric operations. Appendix D, *Applying the DoD IEA* , addresses how to apply the DoD IEA. Appendix E describes the compliance areas and content that demonstrates compliance with the DoD IEA.

7.2.3.3. DoD Chief Information Officer (CIO) Use of the DoD Information Enterprise Architecture (IEA)

The DoD CIO uses the DoD Information Enterprise Architecture (IEA) in all three of the major decision processes of the Department.

The DoD CIO uses the DoD IEA throughout the processes included in operating the Joint Capabilities Integration and Development System (JCIDS) to:

- Advise the Joint Requirements Oversight Council (JROC).
- Provide the basis for the development and refinement of joint enterprise and solution architectures by the Joint Staff and other DoD Components in support of the JCIDS.
- Develop assessments and provide recommendations to the Joint Requirements Oversight Council; the DoD IEA, including its concepts, products, data, conclusions, and implications provides a key source for these assessments.

The DoD CIO uses the DoD IEA throughout the Planning, Programming, Budgeting and Execution (PPBE) process to:

- Review and provide recommendations for development of the Guidance for the Development of the Force and the Joint Programming Guidance.
- Provide recommendations to the Senior Level Review Group relating to Information Technology (IT) (including National Security Systems (NSS)),

interoperability, and Information Assurance (IA).
- Review and evaluate Program Change Proposals and Budget Change Proposals relating to IT (including NSS), interoperability, and IA.
- Provide recommendations for Program Objective Memorandum planning and programming advice.

Finally, the DoD CIO uses the DoD IEA throughout the Defense Acquisition Process to:

- Inform and support his recommendations as a member the Defense Acquisition Board and his decisions as the Milestone Decision Authority for delegated acquisition programs.
- Review Information Support Plans and evaluate the interoperability, interoperability key performance parameters, and information assurance aspects of those plans.

7.2.4. Integration into the Acquisition Life Cycle

The following sections outline steps that the DoD Components, Combat Developers, Sponsors, Domain Owners, DoD Agencies, Program Managers, and/or other assigned managers should take to facilitate DoD Information Enterprise Architecture (IEA) compliance and net-centric information sharing when acquiring Information Technology-enabled capabilities that will interoperate within the Global Information Grid.

At Milestones, A, B, and C, architects should assure that any new architectural models they develop conform to the current version of the DoD Architecture Framework (DoDAF). The latest version of the DoDAF is always available on the DoD Architecture Registry System (DARS) website, URL https://dars1.army.mil/. Existing architecture models that require an update for reasons other than a DoDAF version change should include the updates necessary to conform with the most current DoDAF. Stable architecture models that do not otherwise require an update do not need to be updated solely because the DoDAF has changed. Also, IAW DoD policy, all AV-1s must be registered in the DARS. Instructions on how to do this are on the DARS portal.

7.2.4.1. Before Milestone A

Ensure that appropriate steps are taken to prepare or update a concept of operations and an operational view (High-level Operational Concept Description, OV-1) of the integrated (solutions) architecture for key mission areas and business processes using the DoD Architecture Framework (DoDAF) and the guidance in CJCS Instruction 6212.01. The Initial Capabilities Document (ICD) should reflect this architecture work, as prescribed by CJCS Instruction 3170.01 and in the format provided in the JCIDS Manual. It also supports analysis of alternatives, business process reengineering efforts, development of the acquisition strategy and acquisition information assurance (IA) strategy, and provides key artifacts that support development of the Information Support Plan. Ensure that architectures adhere to the DoD net-centric strategies.

Ensure that the mandatory architecture views align with the DoD Information Enterprise Architecture (IEA) and show linkage to parent enterprise architectures, where available, and DoD Component and DoD-level Capability Portfolio Management architecture descriptions as they emerge.

Compliance with the DoD IEA is mandatory for any platform, program of record, system, subsystem, component, or application that conducts communications. Business systems should align with the Business Enterprise Architecture.

Develop an Initial Capabilities Document (Intelink account required) to describe capability gaps identified through analysis of joint concepts and solutions architectures. Use the criteria in CJCS Instruction 6212.01 to ensure the Initial Capabilities Document and supporting OV-1 address required interoperability standards.

7.2.4.2. Before Milestone B

Build or update the architecture and supporting views (All Views, Capability Views, Data and Information Views, Operational Views, Project Views, Services Views, Systems Views, and Standards Views).

Develop a Capability Development Document, as prescribed by CJCS Instruction 3170.01 in the format provided in the JCIDS Manual, and a Net-Ready Key Performance Parameter (NR-KPP) that address the interoperability and Information Assurance requirements described in CJCS Instruction 6212.01. Address issues associated with the updated architecture, the Capability Development Document, and the DoD IEA.

Use the required architecture products to support development of the Information Support Plan.

Begin development of the Information Support Plan for review. Use the criteria in CJCS

Instruction 6212.01 to guide the acquisition of net-centric capabilities.

7.2.4.3. Before Milestone C

Update the architecture and supporting views (All Viewpoint, Capability Views, Data and Information Views, Operational Views, Project Views, Services Views, Systems Views, and Standards Views) and ensure changes are reflected in the Capability Production Document, as prescribed by CJCS Instruction 3170.01 in the format provided in the JCIDS Manual, and in the Net-Ready Key Performance Parameter (NR-KPP). If the program is entering the acquisition process at Milestone C, develop an NR-KPP using guidance in CJCS Instruction 6212.01.

Address any remaining issues associated with Service-Level Agreements. A Service-Level Agreement defines the technical support, business parameters, and/or critical interface specifications that a service provider will provide to its clients. The agreement typically spells out measures for performance parameters and protocols used in interfacing, and consequences for failure.

Ensure the program delivers capabilities responsive to the Capability Production Document and meets interoperability and information assurance requirements reflected in the updated NR-KPP.

Use the criteria in CJCS Instruction 6212.01 to ensure services and data products delivered by the acquisition align with the Department's objectives for net-centricity.

Prepare and submit the Information Support Plan for final review.

Address all information exchange requirements as part of the Information Support Plan and the Information Technology and National Security Systems Interoperability Certification processes.

7.2.4.4. After Milestone C and the Full-Rate Production Decision Review/Full-Deployment Decision Review

Continue life-cycle compliance with the Information Support Plan Interoperability Requirements Certification and the Information Technology and National Security System Interoperability Certification.

Continue life-cycle compliance with Information Assurance Certification and Accreditation .

7.2.5. DoD Enterprise Architecture-Related Guidance

7.2.5.1. DoD Architecture Framework (DoDAF)

7.2.5.2. DoD Information Technology (IT) Standards Registry (DISR)

7.2.5.3. DoD Net-Centric Data and Services Strategy

7.2.5.4. DoD Information Assurance (IA) Strategic Plan

7.2.5.5. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document

7.2.5. DoD Enterprise Architecture-Related Guidance

The following paragraphs describe the major sources of guidance and tools related to the DoD Enterprise Architecture and supporting DoD strategies for implementing the architecture in information technology (including National Security Systems) programs. Program Managers and sponsors/domain owners should use the guidance, tools, and strategies outlined below throughout a program's life cycle to meet a variety of statutory and regulatory requirements.

7.2.5.1. DoD Architecture Framework (DoDAF)

DoDAF has been designed to meet the specific business and operational needs of the DoD. It defines a way of representing an enterprise architecture that enables stakeholders to focus on specific areas of interests in the enterprise, while retaining sight of the big picture. To assist decision-makers, DoDAF provides the means of abstracting essential information from the underlying complexity and presenting it in a way that maintains coherence and consistency. One of the principal objectives is to present this information in a way that is understandable to the many stakeholder communities involved in developing, delivering, and sustaining capabilities in support of the stakeholder's mission. It does so by dividing the problem space into manageable pieces, according to the stakeholder's viewpoint, further defined as DoDAF-described Models.

Each viewpoint has a particular purpose, and usually presents one or combinations of the following:

- Broad summary information about the whole enterprise (e.g., high-level operational concepts).
- Narrowly focused information for a specialist purpose (e.g., system interface definitions).
- Information about how aspects of the enterprise are connected (e.g., how business or operational activities are supported by a system, or how program management brings together the different aspects of network enabled capability).

However, it should be emphasized that DoDAF is fundamentally about creating a coherent model of the enterprise to enable effective decision-making. The presentational aspects should not overemphasize the pictorial presentation at the

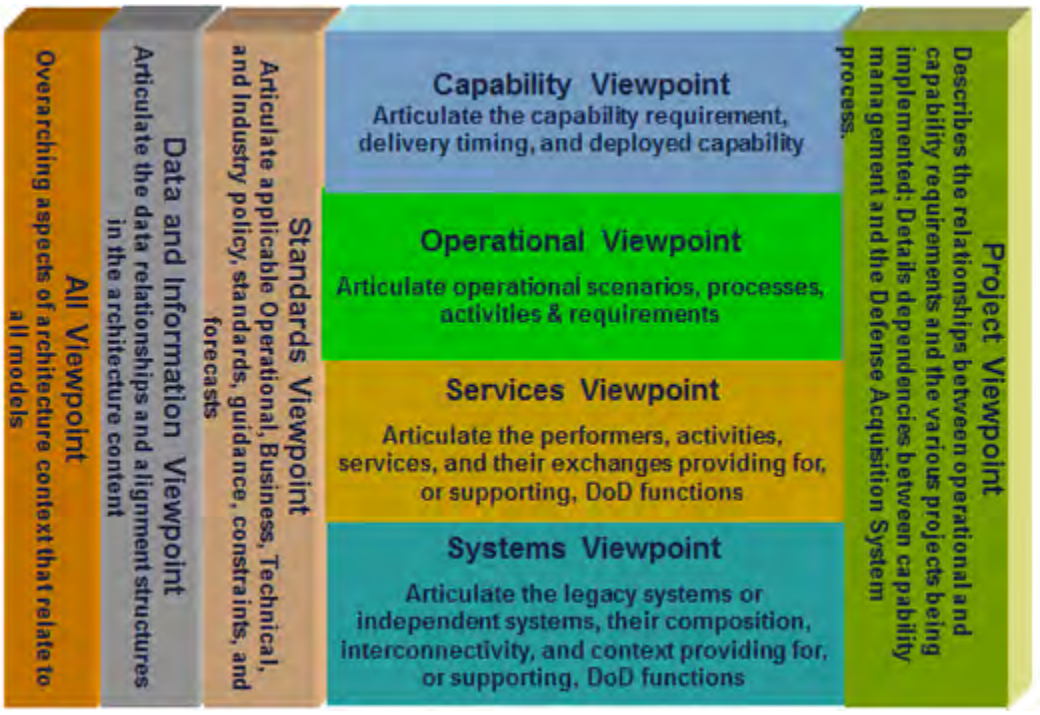
expense of the underlying data.

DoDAF organizes the DoDAF-described Models into the following viewpoints:

- The All Viewpoint describes the overarching aspects of architecture context that relate to all viewpoints.
- The Capability Viewpoint articulates the capability requirements, the delivery timing, and the deployed capability.
- The Data and Information Viewpoint articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.
- The Operational Viewpoint includes the operational scenarios, activities, and requirements that support capabilities.
- The Project Viewpoint describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process. An example is the Vcharts in Chapter 4 of the Defense Acquisition Guide.
- The Services Viewpoint is the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.
- The Standards Viewpoint articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.
- The Systems Viewpoint , for Legacy support, is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.

A presentation of these viewpoints is portrayed in graphic format below:

Figure 7.2.5.1.F1 DoDAF Models Viewpoints



DoDAF Viewpoints

DoDAF V2.0 is a more focused approach to supporting decision-makers than prior versions. In the past, decision-makers would look at DoDAF offerings and decide which were appropriate to their decision process. An example is the JCIDS process architecture requirements inside the JCIDS documentation (ICD, CDD, CPD, etc.). Additionally, older version Architectural Description products were hard-coded in regard to content and how they were visualized. Many times, these design products were not understandable or useful to their intended audience. DoDAF V2.0, based on process owner input, has increased focus on architectural data, and a new approach for presenting architecture information has addressed the issues.

Typically the Combat Developer (or Domain Owner/Sponsor) will be responsible for the architecture description prior to Milestone B with the Program Manager taking on the responsibility subsequent to the approval at Milestone B.

7.2.5.2. DoD Information Technology (IT) Standards Registry (DISR)

The DoD IT Standards Registry is an online repository for a minimal set of IT standards to support interoperability. These standards are used as the "building codes" for all

systems being procured in the DoD. Use of these building codes facilitates interoperability among systems and integration of new systems into the Information Enterprise. In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver net-centric capabilities.

When building systems, requests for proposals (RFPs) and contract statements of work (SOWs) should be reviewed as part of approved acquisition processes to ensure IT standards established in Initial Capabilities Documents, Capability Development Documents, and Capability Production Documents (Intelink account required) are translated into clear contractual requirements. In addition, RFPs and contract SOWs should contain additional requirements for contractors to identify instances where cost, schedule, or performance impacts may preclude the use of IT standards mandated in DISR. Key net-centric elements that program architectures should focus on include:

- **Internet Protocol** Ensure data packets are routed across network, not switched via dedicated circuits. Focus on establishing IP as the convergence layer.
- **Secure and Available Communications** Encrypted initially for core network; goal is edge-to-edge encryption and hardened against denial of service. Focus is on Black (encrypted) Transport Layer to be established through the Transformational Communications Architecture implementation.
- **Assured Sharing** Trusted accessibility to net resources (data, services, applications, people, devices, collaborative environment, etc). Focus on assured access for authorized users and denied access for unauthorized users.
- **Quality of Service** Data timeliness, accuracy, completeness, integrity, availability, and ease of use. This is envisioned as being measured through the Net-Ready Key Performance Parameter. Focus on Service Level Agreements and service protocols with quality and performance metrics.

7.2.5.3. DoD Net-Centric Data and Services Strategy

The DoD Net-Centric Data Strategy provides the basis for implementing and sharing data in a net-centric environment. It describes the requirements for inputting and sharing data, metadata, and forming dynamic communities to share data. Program Managers (PMs) and Sponsors/Domain Owners should comply with the explicit requirements and the intent of this strategy, which is to share data as widely and as rapidly as possible, consistent with security requirements. Additional requirements and details on implementing the DoD Data Strategy are found in section 7.4. (Refer to DoD Net-Centric Data Strategy, May 2003, issued by Assistant Secretary of Defense for Networks and Information Integration (DoD Chief Information Officer (DoD CIO).

The DoD Net-Centric Services Strategy (NCSS) reflects the DoD's recognition that a service-oriented approach can result in an explosion of capabilities for our warfighters and decision makers, thereby increasing operational effectiveness. A service-oriented approach can accelerate the DoD's ongoing effort to achieve net-centric operations by ensuring that our warfighters receive the right information, from trusted and accurate

sources, when and where it is needed.

The DoD NCSS builds upon the DoD Net-Centric Data Strategy's goals of making data assets visible, accessible, and understandable. This strategy establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.

The DoD's vision is to establish a Net-Centric Environment (NCE) that increasingly leverages shared services and Service Oriented Architecture (SOA) that are:

- Supported by the required use of a single set of common standards, rules, and shared secure infrastructure provided by the Enterprise Information Environment Mission Area (EIEMA);
- Populated with appropriately secure mission and business services provided and used by each Mission Area;
- Governed by a cross-Mission Area board, which is chaired by the DoD CIO;
- Managed by Global information Grid (GIG) Network Operations (NetOps).

When this vision is achieved, all members of the DoD will realize significant benefits. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when Military Departments, Agencies, and mission partners create reusable "building blocks" through the use of services. The coordinated management of this environment under GIG NetOps provides the necessary situational awareness for joint forces to use the capabilities that are available. The DoD's commitment to govern this evolution will greatly improve the ability to respond to evolving operations and missions. (Refer to: DoD Net-Centric Services Strategy, Strategy for a Net-Centric, Service Oriented DoD Enterprise, March, 2007, issued by DoD CIO.)

To assist in achieving the net-centric information sharing vision, PMs should be cognizant of the following principles from the DoD Information Enterprise Architecture (IEA) that address the deployment of data and services:

- Data, services and applications belong to the DoD Enterprise. Information is a strategic asset that must be accessible to the people who need it to make decisions.
- Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the underlying implementation. Likewise, data has much greater value if it is visible, accessible and understandable outside of the applications that might handle it.
- Only handle information once (the "OHIO" principle). Information that exists should be reused rather than recreated.
- Semantics and syntax for data sharing should be defined on a community basis.

Information sharing problems exist within communities; the solutions must come from within those communities.

- Data, services and applications must be visible, accessible, understandable, and trusted to include consideration of "the unanticipated user". All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.
- Enterprise Services providing data or information shall be authoritative and, thus, trusted as being accurate, complete and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source.
- Enterprise Services must be hosted in environments that meet minimum GIG computing node standards in terms of availability, support and backup. A small set of Enterprise Services, designated as Core Enterprise Services, are mandated for DoD-wide use by the DoD CIO in order to provide enterprise-wide awareness, access and delivery of information via the GIG.

Refer to: DoD Information Enterprise Architecture (IEA) issued by DoD CIO.

7.2.5.4. DoD Information Assurance (IA) Strategic Plan

The DoD IA Strategic Plan defines an enterprise-wide strategic direction for assuring information and guides planners, programmers, strategists and organizational leaders. The Net-Centric Enterprise IA Strategy serves as an annex to the DoD IA Strategic Plan, and focuses specifically on amplifying the goals and approaches for transforming to the IA essential to safeguarding a net-centric information environment.

The Net-Centric Enterprise IA Strategy is a driver for the IA Component of the Global information Grid (GIG) Architecture. The Net-Centric IA Strategy describes the DoD strategy for integration of IA into the global, net-centric information environment. The end-to-end IA component of the GIG is comprised of a set of informational documents and DoD Architecture Framework (DoDAF) products (tools) that define IA constructs as conceptualized and specified for integration of IA into the net-centric information environment in support of a secure, globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, defense policymakers, and support personnel. The intent of the Net-Centric IA Strategy is to reflect an approach to IA concepts and definitions from a "services" point-of-view instead of a "system" point-of-view, without specifying requirements related to specific implementations or architectures.

For more detail about Information Assurance, see Section 7.5.

7.2.5.5. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document

The GIG ES Capability Development Document is currently focused on nine core enterprise services to be provided by the Net Centric Enterprise Services (NCES) Program. These services are the foundation for the initial net-centric capabilities to be provided by the Defense Information Systems Agency. The Capability Development Document describes the overall set of services in detail.

The NCES program will develop the core enterprise services incrementally. The NCES Program Plan describes the increments and their anticipated schedule. Each program that is dependent upon the core services being developed by the NCES program should address the impact of the incremental NCES schedule on their program.

7.3. Interoperability and Supportability of Information Technology and National Security Systems

7.3.1. Interoperability and Supportability

7.3.1. Interoperability and Supportability

Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information Technology (IT) and National Security Systems (NSS) interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle, and it should be balanced with IA.

Supportability for IT systems and NSS is the ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capabilities .

7.3.2. Mandatory Policies

7.3.2.1. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

7.3.2.2. DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

7.3.2.3. DoD Directive 5000.01, "The Defense Acquisition System"

7.3.2.4. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

7.3.2.5. CJCS Instruction 6212.01, "Interoperability and Supportability of Information Technology and National Security Systems"

7.3.2.1. DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

- Section 4.1 of this Directive requires IT and NSS employed by U.S. Forces to interoperate with existing and planned systems and equipment of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate (based on capability context).
- Section 4.3 requires that IT and NSS interoperability and supportability needs, for a given capability, be identified through:
    - The Defense Acquisition System (as defined in the DoD 5000 series issuances);
    - The Joint Capabilities Integration and Development System process;
    - The Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) change recommendation process.
- Section 4.5 provides that IT and NSS interoperability be verified early, and with sufficient frequency throughout a system's life, or upon changes affecting interoperability or supportability, to assess, evaluate, and certify its overall interoperability and supportability within a given capability. Joint interoperability certification testing shall be as comprehensive as possible, while still being cost effective, and shall be completed prior to fielding of a new IT and NSS capability or upgrade to existing IT and NSS.
- Section 4.8 requires that interoperability and supportability needs be balanced with requirements for Information Assurance (IA).

7.3.2.2. DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

- *E3.1.5. A Net-Ready Key Performance Parameter (NR-KPP), consisting of verifiable performance measures and metrics, shall be used to assess information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. A NR-KPP shall be defined for all IT and NSS defense acquisition and procurement programs and shall be specified to a level of detail that allows verification of interoperability throughout a system's life. The defined NR-KPP shall be developed so that it can be reliably measured, tested and evaluated.*
- *E3.1.6. IT and NSS interoperability and supportability needs shall be managed, evaluated, and reported over the life of the system using an Information Support Plan (ISP). For all DoD ACAT programs and non-ACAT acquisitions and procurements, a ISP shall be produced and used to analyze interoperability and*

supportability requirements specified in the NR-KPP. . . .

- *6.2.3.6.1. All IT and NSS, regardless of ACAT, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC). IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions. Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.*
- *6.2.3.6.2. IT and NSS interoperability testing can occur in multiple stages. Evolutionary acquisitions or procurements, and normal life-cycle modifications, result in a progressively more complete capability. Therefore, there may be instances when it is important to characterize a system's interoperability before all critical interface requirements have been tested and certified. However, all critical interfaces, identified in the NR-KPP, which have been tested, must be successfully certified for interoperability prior to fielding. When appropriate (e.g., between successful completion of OT and the fielding decision), the DISA (JITC) shall issue interim interoperability certification letters specifying which of the system's interoperability needs have been successfully met and which have not. The DISA (JITC) shall issue an overall system certification once the system successfully meets all requirements of the NR-KPP validated by the Chairman of the Joint Chiefs of Staff. The DISA (JITC) shall provide interoperability certification letters to the USD(AT&L), the USD(C)/CFO, the DoD CIO, the DPA&E (now DCAPE), the DOT&E, the Chairman of the Joint Chiefs of Staff, and the Commander, USJFCOM, as well as to the OTA and program manager, as applicable.*

7.3.2.3. DoD Directive 5000.01, "The Defense Acquisition System"

- Paragraph E1.1.10 establishes the requirement to acquire systems and families of systems that are interoperable with other U.S forces.
- Paragraph E1.1.11 states the requirement that test and evaluation shall assess interoperability.
- Paragraph E1.1.16 cites the need to maximize interoperability as a primary reason for acquisition managers to consider and use performance-based strategies for acquiring and sustaining products and services.

7.3.2.4. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

- *Enclosure 6, paragraph 2.c.(8) states: Interoperability Testing: All DoD MDAPs, programs on the OSD T&E Oversight list, post-acquisition (legacy) systems, and all programs and systems that must interoperate, are subject to interoperability evaluations throughout their life cycles to validate their ability to support mission accomplishment. For IT systems (including NSS) with interoperability requirements, the Joint Interoperability Test Command (JITC), regardless of ACAT, shall provide system interoperability test certification memorandums to the Deputy Under Secretary of Defense (Acquisition and Technology)*

(DUSD(A&T)), the DoD CIO, and the Director, Joint Staff J-6, throughout the system life-cycle.

- *Enclosure 6, paragraph 3 states: During DT&E, the materiel developer shall:*
  - d. Assess technical progress and maturity against critical technical parameters, to include interoperability, documented in the TEMP; and
  - h. In the case of IT systems, including NSS, support the DoD Information Assurance Certification and Accreditation Process and Joint Interoperability Certification process; . . .

7.3.2.5. CJCS Instruction 6212.01, "Net Ready Key Performance Parameter (NR KPP)"

This publication provides instruction to develop a NR KPP.

1.a. Defines responsibilities and establishes policy and procedures to develop the NR KPP and NR KPP certification requirement for all information technology (IT) and national security systems (NSS) that contain joint interfaces or joint information exchanges.

7.3.3. Interoperability and Supportability Integration into the Acquisition Life Cycle

7.3.3. Interoperability and Supportability Integration into the Acquisition Life Cycle

DoDD 4630.05, and DoDI 4630.8 as modified by the Interim Guidance for Interoperability of IT and NSS along with the CJCS Instruction 6212.01, provide insights into the relationship between key interoperability and supportability activities and the JCIDS and DAS processes.

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

7.3.4.1. Supporting Architecture Views and Compliance

7.3.4.2. DoD Net-Centric Data Strategy

7.3.4.3. Global Information Grid (GIG) Technical Guidance (GTG)

7.3.4.4. Compliance with DoD Information Assurance (IA) Requirements

7.3.4.5. Compliance with Supportability Requirements

7.3.4. Net-Ready Key Performance Parameter (NR-KPP)

The Net-Ready Key Performance Parameter (NR-KPP) has been developed to assess net-ready attributes required for both the technical exchange of information and the end-

to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving IT (including NSS) interoperability and supportability. The NR-KPP assists Program Managers (PMs), the test community, and Milestone Decision Authorities in assessing and evaluating IT (including NSS) interoperability.

The NR-KPP assesses information needs, information timeliness, Information Assurance (IA), and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. PMs will use the NR-KPP documented in Capability Development Documents and Capability Production Documents to analyze, identify, and describe IT (including NSS) interoperability needs in the ISP and in the test strategies in the Test and Evaluation Master Plan. The following elements comprise the NR-KPP:

- Supporting architecture products, including the Joint Common Systems Function List (JCSFL) required to assess information exchange and operationally effective use for a given capability;
- Compliance with DoD Net-centric Data and Services strategies, including data and services exposure criteria;
- Compliance with applicable Global information Grid (GIG) Technical Guidance, to include DoD IT Standards Registry-mandated GIG net centric IT Standards reflected in the Technical Standards View-1 and, Functional and Technical Implementation of GIG Technical Profiles necessary to meet the net centric operational requirements specified in the architecture system views;
- Verification of compliance with DoD IA requirements; and
- Compliance with Supportability elements to include Spectrum Analysis, Selective Availability Anti-Spoofing Module (SAASM), and the Joint Tactical Radio System (JTRS).

7.3.4.1. Supporting Architecture Views and Compliance

In accordance with the DoD 4630 Series, architecture products or views defined in the DoD Architecture Framework (and related discussion in DoD Instruction 4630.8) shall be used to assess information exchange and use for a given capability. The functional proponent, domain owner, Principal Staff Assistant, and PM use the supporting architecture products or views in developing the NR-KPP and preparing the ISP.

PM compliance with required supporting architecture views is demonstrated through inspection and analysis of developed architecture views to determine conformance with DoD Architecture Framework specifications and that all required views have been produced . CJCS Instruction 3170.01 and CJCS Instruction 6212.01 requirements apply.

7.3.4.2. DoD Net-Centric Data Strategy

Compliance with the DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense" and the DoD Net-Centric Data Strategy is an essential prerequisite of net-centric operations. For a program to gain Interoperability and Supportability Certification, program data and services must be "exposed" by making data elements and provided services visible, accessible, and understandable to any potential user with access to the GIG, both anticipated and unanticipated.

Verification of compliance with the DoD Net-Centric Data Strategy and DoD Net-Centric Services Strategy will be accomplished through the analysis of the sponsor-provided architecture and verification products with accompanying text detailing the program's compliance strategy. Documentation (via architecture products or other forms) must clearly identify all net-centric services and data as adopted from Universal Core, Domain Cores, and COIs.

- In addition to the architecture products, sponsors must complete Data and/or Service Exposure Verification Tracking Sheets to self-evaluate compliance with the direction in the exposure directives.
- The Data and/or Service Exposure Verification Tracking Sheets are required. The preferred method is to use the Enhanced Information Support Tool (EISP) to generate the tracking sheets. Otherwise, the tracking sheets must be filled out manually and submitted to JS J6.
- A guide for selecting which type of Tracking Sheet is required for each program and instructions for the completion of each type is located on the CJCSI 6212 Resource Page.

7.3.4.3. Global Information Grid (GIG) Technical Guidance (GTG)

The GTG is an evolving web enabled capability providing the technical guidance necessary for an interoperable and supportable GIG built on Net-Centric principles. The GTG provides a one-stop, authoritative, configuration managed source of technical compliance guidance that synchronizes previously separate efforts. The GTG is designed to enable users to decide which guidance is applicable and to find detailed information and artifacts needed to meet functional requirements (GIG features and capabilities), DISR-mandatory GIG net-centric IT standards, supporting GIG IT standards, and GIG Technical Profiles (GTPs).

The GTG is the source for all technology guidance and standards implementation information used in describing GTPs necessary to meet the net centric operational requirements specified in the system/service views of an architecture. The GTG contains a program characterization questionnaire and compliance declaration matrix that points to applicable GTPs. The GTPs are built from DISR-mandated IT Standards reflected in a standards profile and include associated implementation guidance, reference architecture and testing criteria necessary to meet all GIG-related requirements characterized in the architecture system/service views. GTG Content

includes:

- The GTG is designed to enable users to decide which guidance is applicable and to find detailed information and artifacts on:
    - Associated technical functional requirements (GIG features and capabilities);
    - DISR-mandated GIG net-centric IT standards;
    - Supporting GIG IT standards;
    - Associated profiles;
    - Reference implementations; and
    - Test criteria.
- The GTPs are aligned with the DoD IEA and are determined based on if following criteria capability:
    - Spans organizational boundaries;
    - Is mandatory or mission critical across the GIG Enterprise;
    - Can be characterized in a GIG Technical Profile;
    - Is essential for resolving GIG end-to end interoperability issues;
    - Enables net centric information sharing for multiple acquisition programs; and
    - Is important from a security perspective.

PM compliance with applicable GTG is demonstrated through inspection of JCIDS documentation and test plans, and during Joint Interoperability Test Command interoperability certification testing (see CJCS Instruction 3170.01 and CJCS Instruction 6212.01 for detailed discussions of the process).

7.3.4.4. Compliance with DoD Information Assurance (IA) Requirements

DoD IA requirements, including IA certification and accreditation, are specified in DoD Directive 8500.01, DoD Instruction 8500.2, DoD Directive 8581.1, and DoD Instruction 8510.01. Satisfaction of these requirements results in system accreditation and the issuance of an authorization to operate. See section 7.5 for details.

7.3.4.5. Compliance with Supportability Requirements

A Program Manager must ensure compliance to spectrum utilization and information bandwidth requirements, Selective Availability Anti-Spoofing (SASSM) and the Joint Tactical Radio System (JTRS), as applicable. See section 7.3.5.5 for details.

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

7.3.5.1. Required Documentation

7.3.5.2. Supporting Architecture Products

7.3.5.3. Global Information Grid (GIG) Technical Guidance (GTG) Compliance

7.3.5.4. Information Assurance (IA)

7.3.5.5. Compliance with Spectrum Supportability

7.3.5. Net-Ready Key Performance Parameter (NR-KPP) Compliance Checklist

The following checklist summarizes the requirements for demonstrating compliance with the NR-KPP and should be useful in preparing for milestone approvals:

7.3.5.1. Required Documentation

Does the capability have the following required documentation?

- Applicable Architecture Products, AV-1, AV-2, OV-1, OV-2, OV-3, OV-4, OV-5, OV-6c, OV-7 (for Final ISP of Record review), SV-2, SV-4, SV-5, SV-6, SV-11 (for Final ISP of Record review), DISR Standards Compliance with TV-1 and TV-2.
- Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, Data Exposure Verification Tracking Sheets.
- Applicable GTG citations, GTG statements, and the corresponding DISR-Mandated GTP IT Standards included in the PMs TV-1 as necessary to meet the net-centric operational characterized in the architecture system views.
- IA requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an accreditation decision by the Designated Approval Authority.
- Applicable Supportability requirements to include SAASM, Spectrum and Joint Tactical Radio System requirements (see section 7.6).

7.3.5.2. Supporting Architecture Products

- Have all architecture products been developed in accordance with the DoD Architecture Framework (DoDAF)?
- Does the AV-1 describe a net centric environment? (**Note:** If this is a non-net-centric environment, i.e., a legacy network, make sure that is noted in the architecture.)
- Has the TV-1 been prepared using applicable information technology standards profiles contained in the DISR?
- Have all the interfaces listed in the OV-2, OV-3, and SV-6 been appropriately labeled with the GIG core enterprise services needed to meet the requirements of the applicable capability architecture?
- Have specific capability architecture OV-6c time event parameters been correlated with GIG architecture OV-6c?

- Have verifiable performance measures and associated metrics been developed using the architectures, in particular, the SV-6?

7.3.5.3. Global Information Grid (GIG) Technical Guidance (GTG) Compliance

The GTG has a compliance regime with granularity appropriate to the Milestone phase or maturity of a program.

- At Milestone B, Capability Development Documents / ISPs will include a preliminary declaration of the functional implementation features and technical capabilities and identify which technical implementation profiles are applicable. Draft TV-1's and TV- 2's will also be included.
- At Milestone C, Capability Production Documents / ISPs and post Milestone C Tailored Information Support Plans (TISPs) will include the final declaration of functional implementation and technical features, identify technical implementation profiles, and complete final TV-1s and TV-2s. The completeness and sufficiency of the program's citing of artifacts drawn from the GTG in determining net readiness will be assessed and certified by Joint Staff in the ISP. A final declaration of selected emerging or maturing standards not found in the DoD Information Technology Standards Registry with rationales and risks will be included along with an approved waiver to use said standards.

7.3.5.4. Information Assurance (IA)

- Have applicable IA requirements of DoD 8500 series issuances and Director of Central Intelligence Directives been identified?
- Is the system level IA design (to include the use of enterprise services) in alignment with the IA component of the GIG architecture?
- Has the applicable capability (system) received an authorization to operate (ATO) from the appropriate Designated Accrediting Authority?

7.3.5.5. Compliance with Spectrum Supportability

Spectrum Supportability Policy and Electromagnetic Environmental Effects (E3) control are contained in DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum."

The spectrum supportability process includes national, international, and DoD policies and procedures for the management and use of the electromagnetic spectrum. The CDD/PD must document the following:

- Permission has been (or can be) obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders; and the newly acquired equipment can operate compatibly with other spectrum-dependent equipment already in the intended operational environment (electromagnetic compatibility).

- All IT, including NSS, must comply with DoD Instruction 4650.01 (see also section 7.6).

7.3.6. Information Support Plan (ISP), Enhanced Information Support Plan (EISP), and Tailored Information Support Plan (TISP)

7.3.6.1. Review of Information Support Plan (ISP)-Specific Mandatory Policies

7.3.6. Information Support Plan (ISP), Enhanced Information Support Plan (EISP), and Tailored Information Support Plan (TISP)

The ISP is intended to explore the information-related needs of an acquisition program in support of the operational and functional capabilities the program either delivers or contributes to. ISPs provide a means to identify and resolve potential information support implementation issues and risks that, if not properly managed, will limit or restrict the ability of a program to be operationally employed in accordance with the defined capability. The ISP focuses on net-readiness, interoperability, information supportability, and information sufficiency concerns. The ISP process is one of discovery, requiring analysis of the program's architecture and processes associated with meeting a capability. This analysis identifies information need, net-centric, interoperability, and supportability issues and assesses compliance with the DoD Chief Information Officers (DoD CIO) stated information policy and goals.

The ISP comes in several forms as a document (ISP or TISP) or as data in the form of an EISP tool (for both ISP and TISPs). The preferred format is using the data-centric EISP tool. The EISP is evolving to become the only acceptable form for ISP content. The ISP provides the PM a mechanism to identify information-related dependencies, to manage these dependencies and to influence the evolution of supporting systems to meet the demands of the system as it evolves to meet the warfighter's needs and capabilities. In the case where the supporting system will not be available, the ISP should provide the PM with awareness of this problem in sufficient time to adjust the program in the most cost effective and operationally efficient manner.

The end-product of the ISP/EISP/TISP is the identified issues and risks associated with information needs and dependencies of the program. Information issues and risks should be treated as any program issue or risk as defined in the AT&L's "Risk Management Guide for DoD Acquisition, Sixth Edition, Version 1, August, 2006." Information issues and risks should be managed as defined in this guide and presented in acquisition decision meetings (such as Overarching Integrated Product Team meetings) by the PM as any other area of issue and risk is presented (e.g., reliability risks).

7.3.6.1. Review of Information Support Plan (ISP)-Specific Mandatory Policies

- DoD Instruction 5000.02, Enclosure 4, Table 3, as amended by the 23 June 2011 PDUSD(AT&L) Memorandum Improving Milestone Process

Effectiveness"Regulatory Requirements Applicable to All Acquisition Programs," requires that all acquisition programs, regardless of acquisition category level, submit an ISP at Pre-EMD Review (Initial ISP), CDR (Revised ISP), Milestone C (ISP of Record, unless waived), at major system or software updates (Updated ISP), and at Program Initiation for ships (Initial ISP).
- DoD Instruction 4630.8, Enclosure 4 provides a ISP content requirements and guidelines..
- CJCS Instruction 6212.01 also provides detailed implementing guidance regarding the ISP and specifically the TISP.
- Intelligence Community Policy Guidance 801.1 provides requirement for Intelligence Community programs to develop an ISP.

7.3.6.2. Information Support Plan (ISP) Integration into the Acquisition Life Cycle

An ISP provides the methodology for meeting a program's information needs and managing the issues and risks associated with those need. It ensures compliance with DoD CIO policy and is used by various other activities to monitor compliance and sufficiency. The Joint Staff utilizes the ISP in the Interoperability and Supportability Certification process; J2 utilizes the ISP for intelligence supportability (CJCS Instruction 3312.01); and the ISP is used as part of Title 40/CCA statutory oversight, oversight of Information Assurance (IA), spectrum supportability, and the National Signature Program.

The ISP is a living document or living data for the EISP, which is developed over the life cycle of a program. At each point of review, the ISP builds and follows the information needs required by a program to meet its intended capability(ies). A completed ISP answers the following seven questions for information needed to support the operational/functional capability(ies) of a system.

- What information is needed?
- How good must the information be?
- How much information (needed or provided)?
- How will the information be obtained (or provided)?
- How quickly must it be received in order to be useful?
- Is the information implementation net-centric?
- Does it comply with DoD information policies?

There are three ISP development approaches during the life cycle:

A traditional ISP Document for Acquisition Category (ACAT) I, IA, and designated ISP Special Interest Programs (see (Office of the DoD CIO Memorandum, Subject: "Information Support Plan (ISP) Special Interest List," located on the JCAPT-E Policy and Guidance website)

1. The Information Needs and Discovery Process will continue to follow the 13 steps in DoD Instruction 4630.8, Enclosure 4 plus the addition of a Net-Ready Key Performance Parameter analysis.
2. A data-centric ISP (EISP) for ACAT I, IA, and designated ISP Special Interest Programs, using an Extensible Markup Language (XML)-based ISP data collection tool provided by DoD CIO and an associated data converter that generates a properly formatted ISP document from the data. This relieves the ISP developer from needing to produce and format a written ISP document and sets the stage for other options of analysis and presentation of ISP data.

An EISP installer, along with the EISP documentation, is available from the JCPAT-E website. In addition to the installer, an EISP Guidebook and technical users guide for the EISP can also be downloaded from the JCPAT-E website. If a user has a problem downloading or installing the EISP, they can contact eisp_help@bah.com.

3. Tailored ISP (TISP) Document for ACAT II and below programs (including ISP Special Interest) and non-ACAT programs that receive Joint Staff (JS) approval may use this method. These programs may tailor the content of their ISP per the procedures in section 7.3.6.9. Authorized programs can obtain a final decision from the JS for their tailored plan to include any special needs identified by the JS for the intelligence and supportability/interoperability certification processes required by CJCS Instruction 3312.01 and CJCS Instruction 6212.01. The final DoD Component approved plan (TISP) will be submitted to DoD CIO ISP document repository (via the DISA-managed JCPAT-E) tool (site requires certificate and/or login)).

The ISP development process serves to guide an ISP throughout a program's acquisition life cycle as opposed to creating a discrete document at each major acquisition decision point. In support of acquisition decisions, the ISP will be submitted for review at four points during the acquisition cycle. Names have been assigned to ISPs for each stage of development (i.e. Initial ISP, Revised ISP, Final ISP of Record,

and Updated ISP). Programs under the various other DoD acquisition lifecycles may follow different milestone events as shown in Figure 7.3.6.2.F1, but also build towards a final ISP of Record.

ISPs for ACAT I, IA programs, and ISPs or TISPs for Special Interest programs will undergo a complete OSD-level review. ISPs or TISPs for all other ACAT II and below programs and Non-ACAT programs will be reviewed using the JSreview process as described in CJCSI 6212.01.

Figure 7.3.6.2.F1, "ISP Submission Timeline," illustrates when ISPs must be submitted to the JCPAT-E tool. It depicts when ISP reviews occur and lists the activities associated with each review. All review timeframes describe the period of time in which the ISP is open for stakeholders comments. All OSD level ISP reviews and JS level ISP reviews will be completed within thirty calendar days of posting with the exception of a final acceptance review by the Joint Staff which will last 15 calendar days. Additional administrative days at the end of the review allow for the Joint Staff and DoD CIO to consolidate and comment matrix or provide appropriate responses. See outline below for the review of time frames and potential responses:

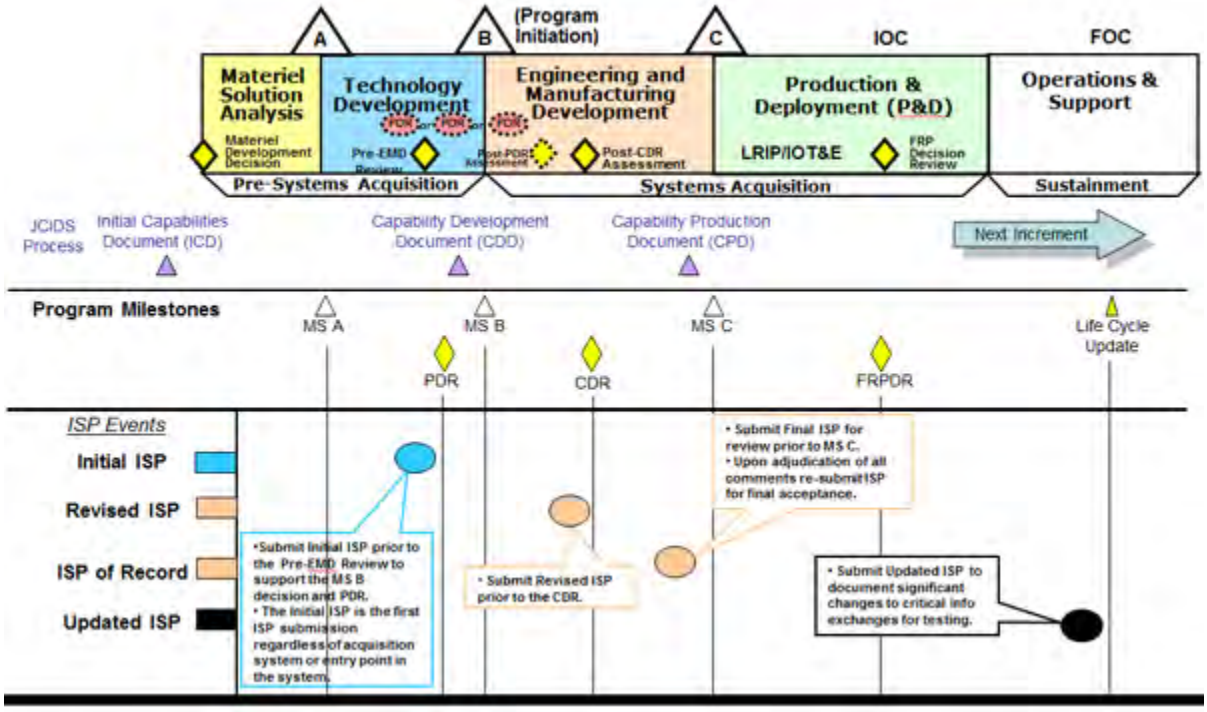
Review time frames:

- 30 Calendar Days: OSD or JS level Review
- N Calendar Days: PM response preparation (N = time determined by PM)
- 15 Calendar Days: Validation of PM responses by OSD/JS for MS C ISP of Record or Updated ISP
- 30 Calendar Days: Submission of ISP of Record signed by Component to JCPAT-E Document Repository

OSD or JS Responses:

- Initial ISP/TISP: Acceptance Memorandum from the DoD CIO or JS for TISP
- Revised ISP/TISP: Acceptance Memorandum from the DoD CIO or JS for TISP
- ISP/TISP of Record: Acceptance of a Component Approved ISP/TISP Memorandum from the DoD CIO and/or JS Interoperability Certification
- Updated ISP/TISP: Acceptance of a Component Approved ISP/TISP Memorandum from the DoD CIO and/or JS Interoperability Certification

Figure 7.3.6.2.F1. ISP Submission Timeline



For a detailed description of the ISP staffing process see the DoD CIO, 26 August 2005 ISP Acquisition Streamlining Pilot Program memo, located within the Policy and Guidance section of the JCPAT-E website.

7.3.6.2.1. Before Milestone A

While the ISP is not required until MS B, early development of the ISP will assist in development of the program's architecture and Concept of Operations discussed in the CJCS Instruction 3170.01. Beginning development of the EISP early will help define information needs and dependencies for the program.

7.3.6.2.2. Before Pre-EMD Review prior to Milestone B (or program initiation for ships)

Define all information needs and related-dependencies according to DoD Instruction

4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to ensure information supportability is addressed in the ISP and Capability Development Document.

- Submit the ISP for formal, coordinated, Initial ISP Review according to DoD Instruction 4630.8 and Pilot Memorandum, DoD CIO, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 as amended by the 23 June 2011 PDUSD(AT&L) Memorandum Improving Milestone Process Effectiveness (Available to users in the JCPAT-E site).

7.3.6.2.3. Before CDR

- Update all information needs and related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to ensure information supportability is addressed in the ISP and Capability Production Document.
- Submit the ISP for formal Review according to DoD Instruction 4630.8 and Pilot Memorandum, DoD CIO, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the JCPAT-E site).
- Results of the Critical Design Review should be used by the PM in making decisions prior to contract award.

7.3.6.2.4. Before Milestone C

DoD Instruction 4630.

- Update all information needs and related-dependencies according to DoD Instruction 4630.8, CJCS Instruction 6212.01, CJCS Instruction 3170.01, and the JCIDS Manual to ensure information supportability is addressed in the Information Support Plan (ISP) and Capabilities Production Document.
- Submit the ISP for formal, coordinated, Final ISP of Record Review according to DoD Instruction 4630.8 and Pilot Memorandum, DoD CIO, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005 (Available to users in the JCPAT-E site).

7.3.6.2.5. After Milestone C

- Submit an updated ISP for each major upgrade (e.g., block or increment).
- Submit the Updated ISP for formal, coordinated, Initial ISP Review according to DoD Instruction 4630.8 and Pilot Memorandum, DoD CIO, "Information Support Plan (ISP) Acquisition Streamlining Pilot Program," August 26, 2005. (Available to users in the JCPAT-E site)

7.3.6.2.6. Interoperability Test Certification

Interoperability Test Certification by Joint Interoperability Test Command will not occur without an Information Support Plan. Exceptions must be approved by both the DoD CIO and Joint Staff.

7.3.6.2.7. Family-of-Systems Information Support Plan (ISP)

A Portfolio ISP should be developed, which at a minimum will identify requirements for support from common GIG infrastructure (e.g., communications). A Portfolio Systems Architecture that conforms to the DoD Architecture Framework is required to guide the integration of the portfolio, as well as a Portfolio Technical Architecture that complies with the Net-Centric criteria. ISPs for families-of-systems or systems-of-systems (i.e., portfolios, enterprises, capability areas, and similar groupings) are encouraged as a way to save time and resources. A platform aggregation of systems as conceptually developed by the Navy is a logical method for implementation. However, this ISP approach requires permission from the office of the DoD CIO and the Joint Staff. The request should define the scope, details and expected process with DoD CIO before the family-of-systems or system-of-systems ISP is initiated. Often the systems within a particular set of systems are out of sync with programmatic acquisition events, particularly in time sequence. Frequently, this situation can be accommodated by creating a "parent" overarching, capstone, portfolio, or enterprise ISP, and adding annexes to the ISP to cover the additional systems. Each time an annex or individual element of the family-of-systems or system-of-systems is addressed, particular care should be taken to include the interactions between the elements making up the overall family- or system-of-systems and the parent operational architecture. The ISP should address any information sharing and/or collaboration.

7.3.6.3. Estimated Information Support Plan (ISP) Preparation Lead Time

7.3.6.4. OSD Review

7.3.6.5. Example/Sample Web Links

7.3.6.3. Estimated Information Support Plan (ISP) Preparation Lead Time

Based on past experience, a small program with few interfaces takes about 6 months to get an ISP ready for review. For most programs, however, ISP preparation for initial review takes about 1 year. Very complex programs, like a major combatant ship, it can take from 18 to 24 months. The length of the process primarily depends on whether a solution architecture exists or requires development.

7.3.6.4. OSD Review

The DoD CIO reviews all ISP documents for Acquisition Category I and IA programs, and for other programs in which DoD CIO has indicated a special interest. This review is performed on the JCPAT-E suite. JCPAT-E provides paperless, web-based support for ISP document submission, assessor review and comment submission, collaborative

workspace, and consolidated review comment rollup. The DISA JCPAT-E functional analyst is available to assist users with JCPAT-E functionality and to establish user accounts. As a best practice, the JCPAT-E includes an ISP repository available for viewing archived and current ISPs.

7.3.6.5. Example/Sample Web Links

Program Managers and other stakeholders will find the links in Table 7.3.6.5.T1 useful for Information Support Plan preparation, program analysis, and oversight.

Table 7.3.6.5.T1. Example/Sample Web Links

• Web Site	
NIPRNET	**SIPRNET**
• Defense Information Systems Agency's Joint C4I Program Assessment Tool	
https://jcpat.csd.disa.mil/JCPAT	jcpat.csd.disa.smil.mil
• Defense Architecture Repository	
https://dars1.army.mil/IER/index.jsp	Not applicable
• DoD Information Technology Standards Registry	
https://gtg.csd.disa.mil/ disronline.disa.smil.mil	
• Global Information Grid (GIG) Technical Direction	
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf	Not applicable

7.3.6.6. Points of Contacts

7.3.6.6. Points of Contacts

Useful points of contact appear in Table 7.3.6.6.T1.

Table 7.3.6.6.T1. Useful Points of Contact

Mission Areas	Phone
Land, Space, Air, Precision Guided Munitions, Command and Control	571-372-4680
Maritime, Missile Defense	571-372-4480

Business Systems, Information Tech Systems, Intelligence	571-372-4471
JCPAT-E Functional Analyst	301-225-7400

7.3.6.7. Information Support Plan (ISP) Content

7.3.6.7.1. Chapter 1. Introduction

Summarize the program's relationships to relevant Joint Operating Concepts (JOCs) and/or Joint Functional Concepts (JFCs) (e.g., focused logistics), as described in the program's JCIDS documents. Provide an OV-1 (High-Level Operational Concept Graphic) for the basic program and descriptive text. For programs not covered by JCIDS, analogous documentation may be used.

- Summarize the program's relationship to other programs.
  - Provide a graphic that shows the major elements/subsystems that make up the system being acquired, and how they fit together. (Provide an Internal SV-1 (System Interface Description)/(e.g., a system block diagram)). Identify the Joint Capability Areas down to three tiers. Use OV-2s in sufficient detail to show each associated area.
  - Analyze threat-specific information that will play a role in capability development, design, testing and operation. This information should be obtained from the appropriate JCIDS documents. Information Operations (IO) threats should be analyzed using the Information Operations Capstone Threat Capabilities Assessment, DI-1577-12-03, August 2003. This is the most comprehensive source available for IO-related threat information.
  - For a weapon system, briefly describe the purpose, design objectives, warhead characteristics, sensors, guidance and control concept (as appropriate), command and control environment, general performance envelope, and primary IT, including NSS, interfaces.
  - For a command and control system, describe the system's function, dependencies and interfaces with other IT (including NSS) systems.
  - For an Automated Information System (AIS), describe the system's function, its mission criticality/essentiality, dependencies, interfaces with other IT (including NSS) systems and primary databases supported.

- Provide the following program data to help the reviewer understand the level of detail to be expected in the ISP:
    - Program contact information (PM, address, telephone, email address, and ISP point of contact).
    - Program acquisition category: Acquisition Category.
    - List Milestone Decision Authority: Defense Acquisition Board, Information Technology Acquisition Board (or component Milestone Decision Authority) or other.
    - Milestone covered by the specific ISP.
    - Projected milestone date.
    - Universal Identifier/DoD IT Portfolio Repository number.
    - Document Type.

7.3.6.7.2. Chapter 2. Analysis

In analyzing a program's information needs and dependencies, the analysis must be considered in the context of the process that is critical to the capability being completed by the system. Look at the critical mission threads associated with the program and compare the operational architecture views to the system architecture views to make sure all information needs and dependencies that are critical to the capability being developed are met. Use in the architectures and consider the following in the analysis:

- Analysis of the qualitative and quantitative sufficiency of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) support (e.g., hardware, software, processes, etc.) should be accomplished in terms of the operational/functional capabilities that are being enabled.
- An understanding of the operational/functional capabilities and the metrics that define whether they are being performed adequately.
- An understanding of what enabling functional capabilities must be performed in order to achieve a higher-level capability (C4ISR functions will almost always be enabling capabilities).
- An understanding of which players (nodes) will direct or perform the missions associated with delivering the capabilities.
- An understanding of DoD Information Policies.
- A definition of the Time Phase in which the analysis is to be accomplished. A user identifies the Time Phase, or Time Phases, the program operates within and defines the Time Phase Name (i.e., increment, block, spiral, et al.), Year, and a Description.
- The information-needs discovery process. For most systems, the steps that follow this list provide an information-needs discovery process that can be used to analyze the system under development. Other approaches for discovering information needs that apply to the intelligence information needs discovery process are:
    - Using the stages of the intelligence cycle (collection, exploitation, dissemination, etc.).

    - Life-cycle stages (Concept Refinement, Technology Development, System Development and Demonstration, etc.).
- The following steps (and notes) are based on using the Architecture developed in accordance with the DoDAF, during the JCIDS process.

Step 1: Identify the warfighting missions and/or business functions within the enterprise business domains that will be accomplished/enabled by the system being procured.

The Mission Threads are based on the last version of the Joint Capability Areas and allow a developer to bin a program's capabilities. A developer selects a Tier 1 Mission Thread in the Enhanced ISP and is then able to select the Tier 2 and Tier 3 mission threads that are children of the chosen Tier 1.

Note: Joint Capability Areas are found at:
http://www.dtic.mil/futurejointwarfare/cap_areas.htm

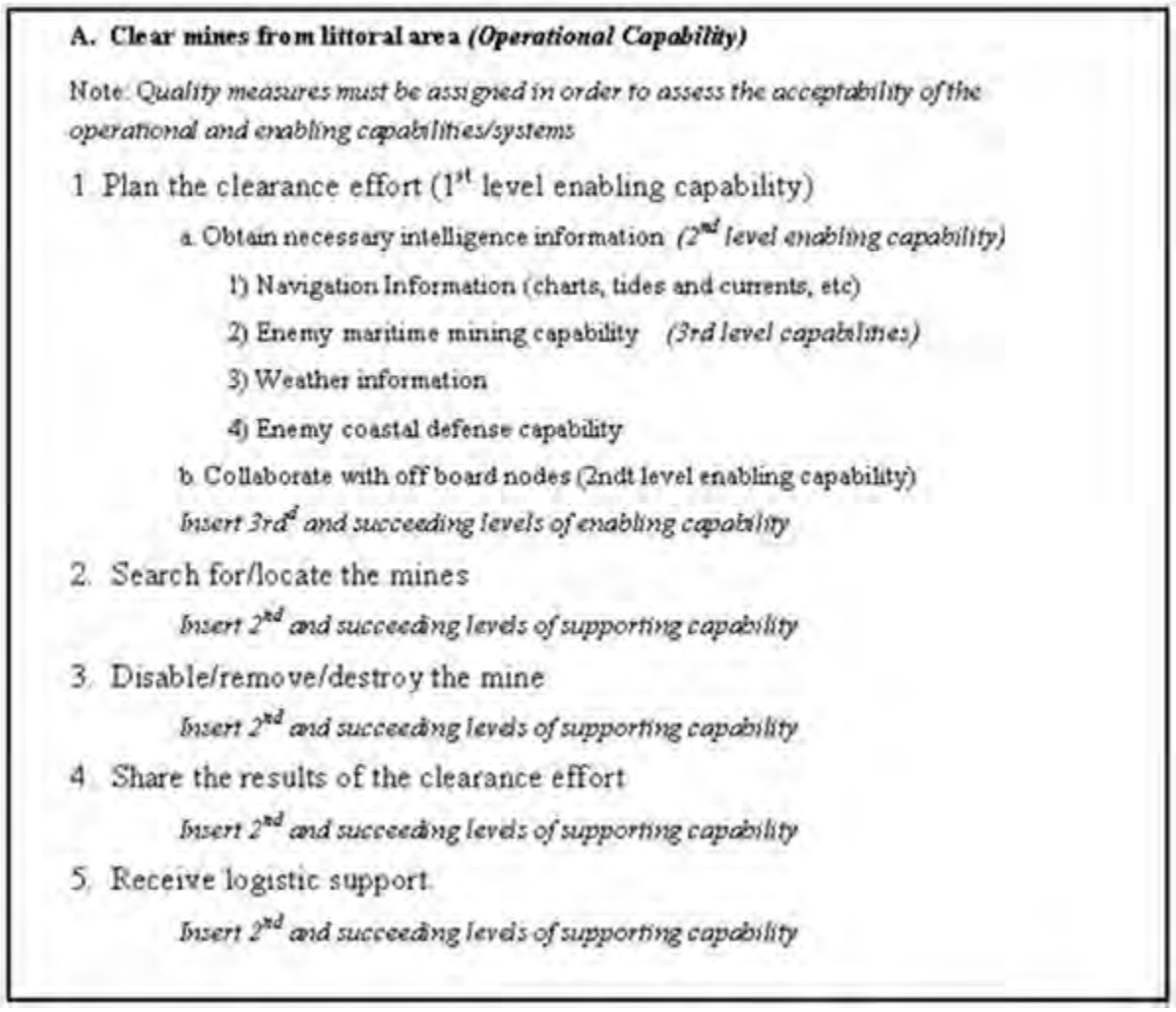
Step 2: Identify information needed to enable operational/functional capabilities for each warfighting mission identified in Step 1 by performing functional capability decomposition.

Note: If a Command and Control capability is the top-level driver of the function breakdown, then the OV-4 (Command Relationships) will be a necessary product to help define the functional capabilities needed. The OV-4 will likely require several OV-5 (Activity Model) functional breakdowns to enable each of the command elements identified.

Note: The architecture product most useful in managing the discovery of enabling/enabled capability relationships for each operational/functional capability is the OV-5 (Operational Activity Model). The OV-5 can be used to show the subordinate capabilities that are necessary to achieve a higher-level operational or functional capability. Notice that the OV-5 focuses on "what" rather than "how." See Example Capability Breakdown, Figure 7.3.6.7.2.F1. This example illustrates specific items to consider for a weapon system that can be used to get the flavor of what is expected in step 2 for a program/system.

Step 2 Example: Clear Mines from Littoral Area

Figure 7.3.6.7.2.F1. Example Capability Breakdown



A. Clear mines from littoral area *(Operational Capability)*

Note: *Quality measures must be assigned in order to assess the acceptability of the operational and enabling capabilities/systems*

1. Plan the clearance effort (1st level enabling capability)
    a. Obtain necessary intelligence information *(2nd level enabling capability)*
        1) Navigation Information (charts, tides and currents, etc)
        2) Enemy maritime mining capability *(3rd level capabilities)*
        3) Weather information
        4) Enemy coastal defense capability
    b. Collaborate with off board nodes (2ndt level enabling capability)
    Insert 3rd and succeeding levels of enabling capability
2. Search for/locate the mines
    Insert 2nd and succeeding levels of supporting capability
3. Disable/remove/destroy the mine
    Insert 2nd and succeeding levels of supporting capability
4. Share the results of the clearance effort
    Insert 2nd and succeeding levels of supporting capability
5. Receive logistic support
    Insert 2nd and succeeding levels of supporting capability

Note: The specific form of this information should capture key information from an OV-5

(Operational Activity Model) and/or other information source (e.g., an outline or hierarchical graph). The important point is that the capability relationships are understood and attributes are identified so that assessments can be made.

Note: Specific items to consider:

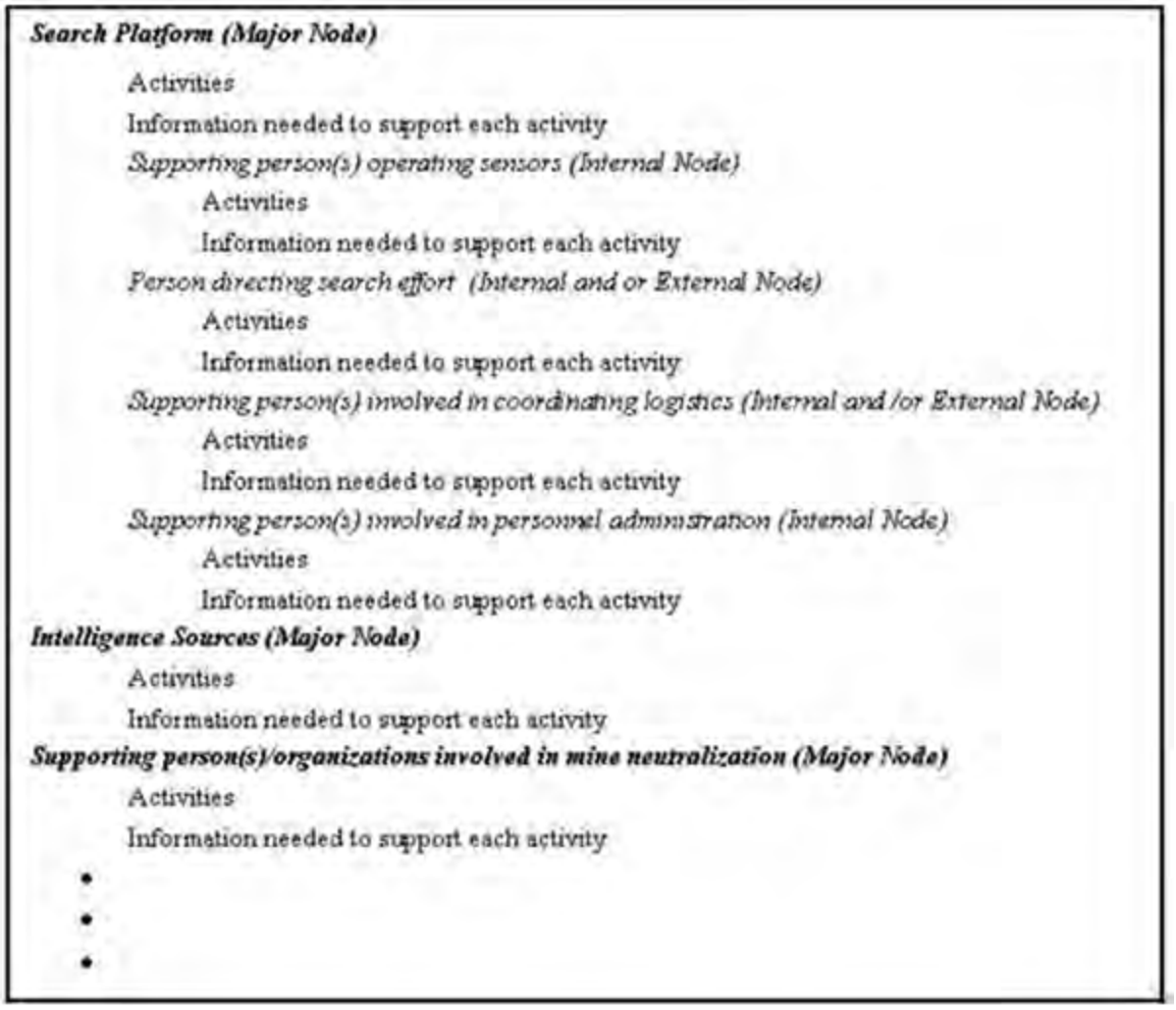
- For satellite systems include: (e.g. Satellite control).
- For communication systems include: (e.g. Net-management).
- For business process systems include: (e.g. information contained in databases, other information sources).
- For weapons systems include: (e.g. Collection Management Support, Threat or signature support, targeting support, Intelligence Preparation of the Battlefield).
- For sensor systems include: (e.g. Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield, and Remote Operations).
- For platforms consisting of a mix of the above include: (e.g., Collection Management support, Threat or Signature support, Targeting support, Intelligence Preparation of the Battlefield.

Step 3: Determine the operational users and notional suppliers of the information needed.

Step 3.a: Provide an OV-2 to identify the operational nodes and elements that drive the communications needed to enable the functional capabilities. For large platforms/systems, this effort should identify the major operational nodes (information drivers) within the platform, as well as nodes that are external to the platform/system with which information will be shared.

Step 3a Example: Clear Mines from Littoral Area

Figure 7.3.6.7.2.F2. Example OV-2 Nodes for Mine Clearance



Step 3.b: Map these nodes (internal and external systems and people) and their activities to the functions identified in OV-5.

Step 4: Establish the quality of the data needed to enable the functions identified in OV-5 and performed by the operational nodes in OV-2 (Operational Node Connectivity).

Note: Establish performance measures and determine the level of satisfaction necessary to make the information useful. (Examples: decimal precision for numerical data, NIIRS for imagery, annotated versus raw data, etc.)

Note: When radio and other information transport systems are identified as providing support, establish transmission quality parameters and then assess whether the programs/systems intended to be used can meet these criteria.

Note: A factor in determining quality is the user (person or sub-system) (i.e., specifically how does the user intend to use the information).

Step 5: Determine if timeliness criteria exist for the information.

Note: To help establish timeliness, use OV-6C (Operational Event Trace Diagram) to establish event sequence. Considerations include:

- Order of arrival of information to enable transaction process(es) (for weapon systems) Latency of data due to speed of flight issues.
- Currency of data in databases to support operations.

Step 6: Determine/Estimate the quantity of information of each type that is needed.

Factors influencing quantity include:

- Frequency of request or transmittal.
- Size of the information requested (packet size, image size, file size etc.).
- Whether data is individual items or a data stream that is provided for a period of time.
- Whether data transmission is "bursty" or continuous over some period of time.
- Whether data transmission is random or occurs at some predictable interval.
- The anticipated spectrum of employment (e.g. Military Operations Other than War or Major Theater of War).

Note: Ultimately this analysis should help estimate the bandwidth needs and should provide an assessment as to whether adequate bandwidth is available. If bandwidth is limited, what actions can be taken to reduce demand or use the bandwidth more efficiently?

Step 7: Discuss the way information will be accessed or discovered.

If data links are involved, identify them and also the message sets that will be implemented.

If an Internet/Web-based (GIG compliant) means of searching for and retrieving posted data is to be used, describe the approach, including compliance with DoD Instruction 8410.01, "Internet Domain Name Use and Approval."

- Data stores must exist for your program.
- The type of searching capability needed.

Note: In many cases, this discussion will involve multiple levels of enabling systems. For example, maybe the enabling system is a Global Command and Control System (GCCS) application. GCCS rides on the Secret Internet Protocol Router Network (SIPRNET). So both levels of this support should be discussed.

Step 8: Assess the ability of supporting systems to supply the necessary information.

Identify the external connections to the system using the system views and identify any synchronization issues associated with schedule and/or availability of external systems.

Note: Supporting systems include collection platforms, databases, real time reports, messages, networked data repositories, annotated imagery, etc.

- Assess the ability to collect, store, and tag the information (to enable discovery and retrieval).
- Assess the ability of networks to provide a means to find and retrieve the necessary data.
- Assess the ability of the information transport systems to move the volume of data needed.
- Assess synchronization in time (i.e., years relative to other system milestones) with supporting programs.
- Whether the information will cross security domains.

Note: If systems will connect to the intelligence Top Secret (TS)/ Sensitive Compartmented Information (SCI) network, Joint Worldwide Intelligence Communications System, or utilize TS/SCI information, they will have to comply with Intelligence Community Directive (ICD) Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" and DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," 18 November 2002.

Note: The number of levels of analysis will depend on the detail required to identify the critical characteristics of the information needed to support the program. This should be accomplished for all phases of the acquisition life cycle.

Note: It is anticipated that other communities such as the intelligence community may have to assist in the determination and analysis of these information needs.

Step 9: Assess Radio Frequency (RF) Spectrum needs.

Note: DoD Instruction 4650.01 establishes spectrum management policy within the Department of Defense. DoD Instruction 4630.8 and CJCS Instruction 6212.01 require Spectrum Supportability (e.g., spectrum certification, reasonable assurance of the availability of operational frequencies, and consideration of Electromagnetic Environmental Effects) to be addressed in the ISP. The Services have additional spectrum management policies and procedures.

To support the Spectrum Supportability process, the ISP should document the following:

- Requirements for use of the electromagnetic spectrum including requirements for wide bandwidths.
- Description of the intended operational Electromagnetic Environment (Allows for realistic test and evaluation).

- Impact of the loss of a planned spectrum-dependent command, control, or communication link as a result of an unresolved spectrum supportability issue. (To be identified in the issue section of the ISP.)

Note: For platforms that employ RF emitters developed by a separate acquisition program, spectrum documentation for those emitters may be cited here as evidence of compliance with Spectrum Supportability regulations.

Step 10. Assess Net-Centricity.

Note: Consider individual Services net-centric policies and procedures that supplement DoD Net-centric policy.

Note: This is an emerging requirement in the analysis required for ISPs. When Net-Centric Enterprise Services (NCES) /Core Enterprise Services (CES) are available, programs will be expected to conduct a detailed analysis of compliance. Programs should be aware of this developing requirement, as it will become an essential part of determining net-centricity and compliance with the DoD Information Enterprise (IE).

Step 10a: Using the information provided as a result of Step 7, the PM should evaluate the program against measurement criteria from the DoD Information Enterprise Architecture (IEA).

Step 10b: Provide an analysis of compliance with the emerging Net-Centric Enterprise Services (NCES)/Core Enterprise Services (CES).

As the DoD IE CES develops, its specifications should be cross-walked with the ISP system's planned network service specifications. Identify the issues associated between the CES service specifications and those of the system that is the subject of the ISP. Compliance would mean that the system would connect seamlessly with the defined DoD-level enterprise services.

Step 10c: Assess use of the following:

- Software Compliant Radios (Joint Tactical Radio System)
- Internet Protocol Version 6.0
- DoD Net-Centric Data Management Strategy
- GIG Bandwidth Expansion relationships
- Net-Centric Enterprise Services linkages

Step 11: Discuss the program's inconsistencies with the DoD Enterprise Architecture and the program's strategy for getting into alignment.

Identify areas where the latest versions of the DoDAF and DoDIEA do not support information needs. (See also DoD Directive 8000.01.)

Step 12: Discuss the program's IA strategy. Also provide a reference to the Program Protection Plan, if applicable.

Step 13: Identify information support needs to enable development, testing, and training.

For development: Weapon systems include information about potential targets that are necessary to support system development. (Example: target signature data)

For testing: Include information support needs critical to testing (Example: Joint Distributed Engineering Plant (JDEP)). Do not duplicate Test and Evaluation Master Plan information except as needed to clarify the analysis. In addition, for information on software safety testing please refer to software test & evaluation.

For training: Include trainers and simulators that are not a part of the program being developed. Include:

- Separately funded training facilities your program intends to use.
- Network support that will be needed to meet the training needs of your program.

7.3.6.7.3. Chapter 3. Issues

- Identify risks and issues (as defined in DoD Instruction 4630.8) in a table similar to Table 7.3.6.7.3.T1 or in an outline containing the same data.
    - Group operational risks and issues under the mission impacted, then under the impacted functional capability (for that mission).
    - When risks or issues involve more than one mission, subsequent missions should be marked with the previous issue number and those fields that remain the same should be so marked.
- Include the following column (or outline) headings:
    - Issue Number
    - Supporting System
    - Source Architectures (e.g., Command and Control (C2), Focused Logistics, Force Protection, Force Application, Battlespace Awareness, Space, etc.)
    - Issue Description
    - Risk/Issue Impact (Use the AT&L "Risk Management Guide for DoD Acquisition" for this assessment)
    - Mitigation Strategy or Resolution Path

Table 7.3.6.7.3.T1. Sample Issue Table Format

Operational Issues
Mission

Functional Capabilities Impacted					
Issue Number	Supporting System	Source Architecture	Issue Description	Issue Impact	Mitigation Strategy/ Resolution Path (and Time-Frame)
Development Issues					
Testing Issues					
Training Issues					

Risks and issues considered critical to the program's success will be briefed by the PM at OIPT meetings. At a minimum, information risks and issues will be incorporated into the PM's risk management program and treated as any other type of program risk and issue.

7.3.6.7.4. Information Support Plan (ISP) Appendices

Appendix A. References. Include all references used in developing the ISP. Include Architectures; other relevant program documentation; relevant DoD, Joint Staff, and Service Directives, Instructions, and Memos; ISPs or ISPs from other programs; any applicable JCIDS documentation; and others as deemed necessary.

Appendix B. Systems Data Exchange Matrix (SV-6).

Appendix C. Interface Control Agreements. Identify documentation that indicates agreements made (and those required) between the subject program and those programs necessary for information support. For example, if System A is relying on information from System B, then this interface dependency must be documented. At a minimum, this dependency should be identified in the ISPs for both System A (the information recipient) and System B (the information provider).

Appendix D. Acronym List: Provide an Integrated Dictionary (AV-2).

Other Appendices. Provide supporting information, as required, not included in the body of the ISP or relevant JCIDS documents. Additional or more detailed information used to satisfy DoD Component-specific requirements should be included as an appendix and not incorporated in the body of the subject ISP. Additional architecture views used in the ISP analysis will be provided in a separate appendix and referenced in the main body of the ISP.

7.3.6.8. Tailored Information Support Plan (TISP) Instructions

7.3.6.8.1. Applicability

7.3.6.8.2. Introduction

7.3.6.8.3. Tailored Information Support Plan (TISP) Process

7.3.6.8.4. Approval of a Tailored Information Support Plan (TISP)

7.3.6.8.5. Tailored Information Support Plan (TISP) Preparation

7.3.6.8. Tailored Information Support Plan (TISP) Instructions

TISP instructions are available from the Joint Staff (CJCS Instruction 6212.01).

7.3.6.8.1. Applicability

The Tailored Information Support Plan (TISP) is designed to improve the Information Support Plan (ISP) process by reducing the number of OSD-level reviews, streamlining the ISP waiver process, and providing a tailored ISP option for ACAT II, III and non-ACAT programs only.

7.3.6.8.2. Introduction

The EISP is designed to accommodate the TISP and is encouraged as the tool for TISP development. ACAT II and below, as well as Non-ACAT programs, may tailor the content of their ISP upon Joint Staff approval. At a minimum, the tailored plan will provide explanation of the programs' Concept of Operations (CONOPS) and will provide IT supportability analysis of the CONOPS. Additionally, the following set of architecture products is required: AV-1, OV-1 (optional), OV-5, OV-6C (optional), SV-1 (optional), SV-5, SV-6, and TV-1.

7.3.6.8.3. Tailored Information Support Plan (TISP) Process

TISP requests shall be requested via email to Joint Staff through the applicable Service/Agency/Joint Forces Command Interoperability Test Panel (ITP) representative. The TISP request form is on the CJCSI 6212 Resources Page. Joint Staff will respond to the TISP request with a "Concur" or "Non-concur" via e-mail.

7.3.6.8.4. Approval of a Tailored Information Support Plan (TISP)

Approval of a TISP will be contingent on the following processes:

- If the mandatory sections of the form are not completed, the request will be returned to the submitter for completion.
- Joint Staff will review submitted TISP applications and will approve or deny entry into the TISP process.
- Applicants, and respective ISP representatives, will be notified via e-mail that a program can precede with development of a TISP.

7.3.6.8.5. Tailored Information Support Plan (TISP) Preparation

- In accordance with DoD Instruction 4630.8, DoD Components/Agencies responsible for ISP development shall comply with applicable portions of the instruction and the procedures outlined in the TISP Program. All TISP requests will be submitted to the appropriate DoD Combatant Command/Service/Agency (C/S/A) Military Communications-Electronics Board Interoperability Test Panel (ITP) Representative using the format available on the ITP web page or CJCSI 6212 Resources Page for either on-line submission or downloading. The appropriate C/S/A ITP Representative shall validate the TISP request.
- Upon DoD Component/Agency approval of using the TISP approach, the TISP will be submitted to Joint Staff via JCPAT-E by submitting their TISP to the appropriate DoD Component/Agency Interoperability Test Panel (ITP) representative point-of-contact for review, approval, and submittal.
- Joint Staff will coordinate with the DoD CIO on all submissions.
- As required, Joint Staff will invite the requesting system's Program Management Office or designated representative to the next scheduled ITP meeting to brief the members concerning the system and their justification for requesting a TISP instead of following DoD Instruction 4630.8 ISP procedures. The ITP will serve as an advisory panel to facilitate Joint Staff determination of system merits and means to mitigate interoperability certification issues.
- The TISP pilot program is intended to accelerate the Joint Interoperability Certification process, programs should make early contact with the Joint Interoperability Test Command to create a testing strategy and gain technical points-of-contact for questions dealing with interoperability and supportability issues .

7.3.6.9. Information Support Plan (ISP) Waiver Process

7.3.6.9. Information Support Plan (ISP) Waiver Process

The requirement for an ISP may be waived when the requirement for JCIDS documentation has been waived, Joint Staff has determined that the Net-Ready Key Performance Parameter or Interoperability Key Performance Parameter are not needed, or the program does not meet any of the criteria identified in paragraphs 2.2.2, 2.2.3, and 2.2.4 of DoD Instruction 4630.8 . Additionally, programs accepted under the Legacy System Interoperability Validation and Certificate Request Process are waived from producing an ISP.

Waiver requirements apply to all Acquisition Category (ACAT) and non-ACAT ISPs. Each DoD Component has an ISP waiver review process. Waiver requests shall be sent via email to DoD CIO by the appropriate DoD Component action officer for coordination prior to approval. The waiver information will include: the program's name, the next milestone, the capability(ies) the program provides, list any external information and related connectivity, and the rationale for the waiver. The ISP waiver application form is available on the CJCSI 6212 Resources Page . DoD CIO will respond to the waiver request via memo indicating approval or disapproval. Waiver authority for non-ACAT ISPs resides with the cognizant fielding authority. Upon final approval by DoD CIO, the DoD Component will be provided a copy of the approved waiver. A test process is now in effect (currently the Navy only) to allow the component some waiver authority. This may be expanded. Legacy Waivers are defined in a DoD CIO memorandum and is being changed as reflected in the text below. As of this guidebook the following will apply for and be changed in future policy for legacy systems.

Fielded Legacy systems, ACAT II and below and non-ACAT programs, that meet all of the conditions outlined below may request a waiver from the DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," dated May 5, 2004, requirement to produce an ISP. In addition to the standard ISP waiver, there are now two categories of legacy waivers with the qualifying conditions shown below by category:

- *Option A* : Permanent Legacy ISP Waiver.
    - Have no current validated Joint Staff requirements documentation;
    - Have no current interoperability test certification;
    - Have no pre-existing interoperability deficiencies identified by the Joint Interoperability Test Command (JITC);
    - Have no plan for funding beyond the Future Years Defense Program (FYDP); and
    - Will be out of the DoD inventory within 5 years.
- *Option B* : Four-year ISP Waiver. (This waiver provides a four-year, ISP waiver for fielded, non-ACAT I programs. At the end of the waiver period, the program may apply for an additional waiver, provided the program continues to meet the three-year waiver requirements.)
    - Have no current validated Joint Staff requirements documentation,
    - Lack a current interoperability test certification,

- Have no major planned updates, incremental changes, spiral development changes planned.
- Have no pre-existing interoperability deficiencies identified by the JITC.
- Be funded beyond FYDP, with no established retirement date, and
- Is currently connected to the Global Information Grid.

Waiver requests will follow the email-based waiver process described in CJCS Instruction 6212.01. When the DoD CIO has electronically approved the request, the fielded legacy system will follow the procedures established by the Joint Staff, for interoperability certification and certificates to operate. Upon granting the waiver, the Joint Staff will inform DoD CIO of the approval.

7.4. Sharing Data, Information, and Information Technology (IT) Services

7.4.1. Implementing the DoD Net-Centric Data Strategy

7.4. Sharing Data, Information, and Information Technology (IT) Services

The DoD policy instruction for sharing data and IT services is contained in the issuance: DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) services in the Department of Defense, March, 2013.

7.4.1. Implementing the DoD Net-Centric Data Strategy

The instruction provides overarching policy, procedures, and responsibilities for sharing data, information, and IT services in the DoD. It is built upon the goals for these respective areas as defined in the DoD Net-Centric Data Strategy (NCDS) (May 9, 2003) and the DoD Net-Centric Services Strategy (NCSS) (May 4, 2007).

The NCDS outlines the vision for managing data in a net-centric information sharing environment. The strategy compels a shift to a "many-to-many" exchange of data, enabling many users and applications to leverage the same data-extending beyond the previous focus on standardized, predefined, point-to-point interfaces. Hence, the objectives are to ensure that all data are visible, available, and usable-when needed and where needed-to accelerate decision cycles. Specifically, the data strategy describes 7 major net-centric data goals as presented in Table 7.4.1.T1, below.

Table 7.4.1.T1. Net-Centric Data Strategy Goals

Goal	Description
Goals to increase Enterprise and community data over private user and system data	

Visible	Users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, no intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.
Accessible	Users and applications post data to a "shared space." Posting data implies that (1) descriptive information about the asset (metadata) has been provided to a catalog that is visible to the Enterprise and (2) the data is stored such that users and applications in the Enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, or security.
Institutionalize	Data approaches are incorporated into Department processes and practices. The benefits of Enterprise and community data are recognized throughout the Department.
Goals to increase use of Enterprise and community data	
Understandable	Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.
Trusted	Users and applications can determine and assess the authority of the source because the pedigree, security level, and access control level of each data asset is known and available.
Interoperable	Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.
Responsive to User Needs	Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

The NCSS outlines a vision to establish Web services (referred to as services hereafter) as the preferred means by which data producers and capability providers make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities. As with data, services are to be made visible, accessible, understandable, and trusted. Specifically, the services strategy describes 3 major net-centric services goals as presented in Table 7.4.1 T2, below.

Table 7.4.1 T2 Net-Centric Services Strategy Goals

Goal	Description

Provide Services	Make information and functional capabilities available as appropriately secure services on the network.
Use Services	Use existing services to satisfy mission needs before creating duplicative capabilities.
Govern the Infrastructure and Services	Establish the policies and procedures for a single set of common standards, rules, and shared secure infrastructure and services throughout the DoD Enterprise to ensure interoperability.
Monitor and Manage Services via GIG NetOps	Implement services in accordance with DoD's GIG NetOps Strategy and concept of operations to ensure situational awareness of the NCE.

7.4.2. Implementing Net-Centric Data Sharing

7.4.2.1. The Roles, Responsibilities, and Relationships of the Community of Interest (COI) in Information Sharing

7.4.2. Implementing Net-Centric Data Sharing

A DoD Guide, DoD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006, stemming from the authority of DoD Directive 8320.02, " Sharing Data, Information, and Information Technology (IT) services in the Department of Defense, March, 2013, provides implementation guidance for the community-based transformation of existing and planned information technology (IT) capabilities across the DoD. The goal of this Guide is to provide a set of activities that members of communities of interest (COIs) and associated leadership can use to implement the key policies of DoD Directive 8320.02 and ultimately increase mission effectiveness across the Department of Defense. The activities presented in this Guide may not apply to all COIs and should be tailored as necessary.

Implementation is largely achieved through activities conducted within Communities of Interests. This guidance covers some of the following key areas:

7.4.2.1. The Roles, Responsibilities, and Relationships of the Community of Interest (COI) in Information Sharing

See Chapter 2 in DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006.

Key COI Attributes

The DoD Chief Information Officer " DoD Net-Centric Data Strategy", May 9, 2003, defines the COI as "a collaborative group of users who must exchange information in

pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." COIs are organizing constructs created to assist in implementing net-centric information sharing. Their members are responsible for making information visible, accessible, understandable, and promoting trust all of which contribute to the data interoperability necessary for effective information sharing. This chapter describes the roles, responsibilities, and relationships of COIs in information sharing.

The focus for COIs is to gain semantic and structural agreement on shared information. For COIs to be effective, their scope-that is, the sphere of their information sharing agreements-should be as narrow as reasonable given their mission. Although the Department of Defense or a Military Department might be considered a collaborative group of users who have a shared mission, and thus a COI, achieving a shared vocabulary across the entire Department of Defense or even across a Military Department has proved to be very difficult to achieve due to the scope and magnitude of the information sharing problem space. COIs represent a mechanism for decomposing the DoD's information sharing problem space into manageable parts that can be addressed by those closest to the individual parts.

COIs may be guided by the DoD's strategic goals, existing policy, and doctrine, or COIs may form on an ad hoc basis to address a data sharing problem among known stakeholders. While DoD Component-specific COIs may exist, COIs are most likely to be functional or joint entities that cross organizational boundaries. Examples of a COI might be a meteorology COI or a joint task force COI. COIs should include producers and consumers of data, as well as developers of systems and applications.

Although COIs may vary, the key attributes (below) should be applicable for the majority of COIs across the Department of Defense.

1. Formed to meet a specific data sharing mission or fulfill a task
2. Composed of stakeholders cooperating on behalf of various organizations, with emphasis on cross-Component activities
3. Members committed to actively sharing information in relation to their mission and/or task objectives
4. Recognize potential for authorized but unanticipated users and therefore, strive to make their data visible, accessible, and understandable to those inside and outside their community

7.4.2.2. Community of Interest (COI) Formation and Execution

7.4.2.2.1. Establish and Evolve a Community of Interest (COI)

7.4.2.2.1.1. Activity Area Overview

7.4.2.2.1.2. Implementation Activities

7.4.2.2. Community of Interest (COI) Formation and Execution

See Chapter 3 in DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006.

This section provides a set of activities to help guide the establishment, evolution, and operations of a COI, as well as the fielding of real information sharing capabilities. Readers new to COIs, in the process of organizing a COI, or belonging to a newly-formed COI should consult this chapter.

COIs may take various forms and are not intended to be "one size fits all." These groups can differ in how they operate, the timelines for their actions, the duration of their existence, how they are governed, and whether or not they demonstrate information sharing capabilities through pilot activities before operational use. As such, COIs should determine what activities, and associated levels of effort, are necessary to ensure sufficient governance and management of the COI.

7.4.2.2.1. Establish and Evolve a Community of Interest (COI)

7.4.2.2.1.1. Activity Area Overview

The COI "Establish and Evolve" activity area focuses on identifying the purpose for a community, identifying the community's needs, and establishing a COI to work toward meeting those needs. The initial step in forming a COI is to identify a potential need for such a group, the mission, and potential membership. In addition, before establishing a new COI, potential members should identify other organizations and/or COIs that may be addressing the same or similar problem area.

If a similar COI exists and there is considerable semantic overlap in the identified problem area, potential members should reach out to the existing COI to leverage its work and investigate opportunities for collaboration. Assuming that a new COI is

required, the process of establishing a new COI will involve the activities below.

7.4.2.2.1.2. Implementation Activities

Identify mission, members, and desired information sharing capabilities. The initial membership of a Community of Interest (COI) will come together around a common information sharing mission that can be addressed as a community. The COI's mission can be formally articulated through a mission statement or charter if the members consider this appropriate. COIs can refer to guidance provided in Chapter 2 of DoD 8320.02-G to identify additional members. The COI should outline the purpose of the community and the scope of its activities, identifying key capabilities that enable the COI to accomplish its mission. Executing these steps ensures that COI agreements reflect end-user needs, that those agreements are technically viable to implement, and that they have the ownership and buy-in necessary to promote changes in operational programs and systems.

Identify related COIs. Communities should use the COI Directory, the DoD CIO will fix or delete to identify related efforts for coordination of governance forums and sharing experiences. This directory maintains a listing of all DoD COIs that register, and provides visibility into their activities. Identification of other COIs can both inform the decision to establish a new COI and identify information sharing possibilities once a new COI has been established.

Prioritize information sharing capabilities. COIs should prioritize key capabilities to focus their efforts based on the potential mission value and feasibility of implementation. In identifying such information sharing capabilities, COIs should consider use of both new and legacy systems. Prioritization should help keep the scope of any COI-identified information sharing capabilities focused and facilitate the implementation of pilots, or initial operational capabilities, as quickly as possible. This enables the COI to contribute to the delivery of real value quickly while providing lessons learned before additional capabilities are developed.

Advertise the COI. To ensure that DoD users can discover the existence and mission of a COI and have the opportunity to participate, a member of the COI should register the COI in the COI Directory. To register, COIs should provide their name, point of contact, mission, status, COI lead, and proposed governing authority.

7.4.2.2.1.3. Forward Planning

Identify measures of success. Communities of interest (COIs) should define COI-specific success measures and measure progress against those criteria. Some measures will be mission specific. For example, success might be defined as reducing the time required to plan strikes as a result of having information available. Other measures of success might be non-mission specific. Non-mission specific measures can provide valuable insight enabling others in the Enterprise to assess data sharing approaches. For example, a COI could measure time saved in fielding new information

sharing capabilities as a result of reusing existing data assets rather than re-creating data. Instituting measures of success helps ensure that the Enterprise continues to invest in those opportunities that provide value to the Enterprise.

Continually gather user feedback. COI members should strive to meet user needs, measure the value achieved through information sharing, and work with stakeholders to identify near-term information sharing capabilities. As the COI evolves, so will stakeholder priorities and needs. Periodically, members should reassess activities to ensure that the COI is continuing to provide value and that it continues to address the COI's mission with needed capabilities. This reassessment would include its support for net-centric information sharing across the Department of Defense. COI members should assess metric results to determine when the COI has achieved its mission and should disband or turn over operations to continuing organizations.

7.4.2.2.2. Community of Interest (COI) Management and Governance

7.4.2.2.2.1. Activity Area Overview

The COI "Management and Governance" activity area focuses on identifying a governing body, communicating with stakeholders, and providing leadership and direction to the COI. COI management and governance activities are integral to ensuring that COIs achieve their mission. Although these activities will be tailored to the individual COI's mission and the membership, there are basic issues that a COI should address. These issues include, but are not limited to, information flow, issue adjudication, prioritization of COI activities, quality assurance, recommendations to portfolio managers, and configuration management of COI products. COI management is responsible for establishing governance processes and structures appropriate to the COI. This effort includes leveraging existing processes and structures where possible and appropriate.

A COI's ability to facilitate cross-Component portfolio management for Information Technology (IT) investments is essential for effective COI management. In IT portfolio management, designated Mission Area and sub-portfolio leads conduct reviews of DoD Component plans and budgets and ensure alignment and efficient use of resources that may advance COI-defined capabilities. As an example, the Intelligence Surveillance Reconnaissance (ISR) COI establishes the expectation that the DoD Components will support inter-Domain/inter-Component information sharing among the Distributed Common Ground System (DCGS) Family of Systems (FoS) program services. The ISR COI provides this direction through the prescribed use of common, shared, or federated information sharing services; specific data implementation strategies and tools, and COI specific agreement on access controls and security mechanisms. For subsequent portfolio reviews, the portfolio manager or identified COI governing authority bases the review on the ISR COI's guidance and works with the DoD Components to validate that each of the DCGS FoS programs are aligned and each has sufficient funding to effectively implement the COI-defined information sharing services and capabilities.

7.4.2.2.2.2. COI Management and Governance Implementation Activities

Identify governing authority. Communities of interest (COIs) should align themselves with an existing governing authority, such as a Mission Area lead, to enable the COI to impact the necessary related systems, programs, and data holdings. Mission Area leads may direct COIs to align themselves with a particular governing authority. Ideally, this governing authority should have flag or general officer level authority, without which the COI might lack the decision-making and resource authority to realize its information sharing goals. The governing authority should be in a position to influence agreements and to help address issues that affect multiple DoD Components.

Select a COI lead. The COI lead is the point of contact and action officer for COI activities. This role differs from that of the governing authority in that the COI lead is responsible for the day-to-day functioning of the COI but should be in a position to influence agreements and to help address issues that affect multiple DoD Components. The COI lead interfaces with the COI governing authority to report status, resolve issues, promote COI agreements, and to make recommendations on DoD Component's plans and schedules. Other responsibilities include leading regular meetings; establishing working groups, as needed; identifying other potential members; acting as a liaison to the portfolio manager or other governing authority; coordinating with the relevant program or system managers; collaborating with other COIs to reuse metadata artifacts; and helping to mitigate any conflict within the COI.

Establish COI-specific governance processes. COIs should develop internal governance processes or leverage existing processes appropriate to the scope and mission of the COI. These activities include appropriate review and adjudication of issues and establishment of Memorandums of Agreement or Memorandums of Understanding as a set of working agreements among participants and their respective organizations. In addition, COI governance processes should enable the establishment of working groups, as needed, to address COI focus areas. For example, the COI might task a data working group with developing COI categorization schemes, thesauri, vocabularies, and taxonomies. COIs should ensure that their working groups operate with defined timelines, focus area(s), and deliverables.

Clarify relationships between groups involved in the COI. Although COI members share a mission, establishing a clear understanding of information sharing relationships among members rather than assuming that such an understanding already exists will help shape COI responsibilities and direction.

Share COI information with all stakeholders. An important aspect of management and governance is transparency of information. COI members should communicate with one another and the governing authority, as well as with their respective organizations. To this end, COIs should track and publicize their activities, schedules, actions, and progress. In addition, COIs should provide stakeholders with the results of specific metrics and measurements (i.e., assessment of performance against metrics) including progress in implementing new information sharing capabilities and progress towards

implementing policy.

This process includes involving stakeholders in the review of documents and specifications developed by the COI and providing the community with mechanisms for user feedback.

Assess reusability of other resources. Using the DoD Data Services Environment (DSE) (CAC-required), communities should identify opportunities for semantic and structural metadata reuse. COIs should also consult other COIs for opportunities to capitalize on operational data access services that can enrich their data sets and, potentially, be integrated into their data sharing capabilities (e.g., a COI can build a new capability using another COI service that is already in place).

Forward Planning. COIs should plan for the long-term maintenance of COI metadata artifacts, including taxonomies and schemas, in consideration of other organizations that have built services that depend on these artifacts. For COIs that are not planned for long-term continuation, the COI should consult with the lead DoD Component organization or governing authority to develop a plan for long-term maintenance, to include configuration management.

7.4.2.2.3. Community of Interest (COI) Capability Planning and User Evaluation

7.4.2.2.3.1. Activity Area Overview

7.4.2.2.3.2. COI Capability Planning and User Evaluation Implementation Activities

7.4.2.2.3.3. Forward Planning

7.4.2.2.3. Community of Interest (COI) Capability Planning and User Evaluation

7.4.2.2.3.1. Activity Area Overview

COIs play a key role in implementing net-centric data sharing across the DoD. The mission-focused and typically joint nature of COIs enable the identification and development of net-centric information sharing capabilities that are of greatest value to DoD users. Through pilots and operational information sharing capabilities, members of COIs can demonstrate the mission value of using cross-Component data sources.

The "Capability Planning and User Evaluation" activity area focuses on defining an information sharing capability that the COI needs, working with DoD Components to implement the capability, and integrating it into ongoing operations. In some cases, COIs, through their members and associated programs, systems, and data sources,

may develop pilot capabilities before engaging in full deployment of a capability. When planning for information sharing capabilities, COI members should define a set of requirements for the capability developers (associated with a program of record or organization with data assets and budget). Associated programs of record inform DoD processes as appropriate when planning for information sharing capabilities. Capability developers are responsible for turning the requirements into a physical implementation of data assets and services in accordance with COI agreements.

The overall goal of these activities is to assist a COI to evolve net-centric information sharing capabilities. Through these activities, COIs should actively identify information sharing needs and to integrate new capabilities supporting known needs of the COI, as well as providing readily discoverable and understandable information to authorized but unanticipated users.

7.4.2.2.3.2. COI Capability Planning and User Evaluation Implementation Activities

Identify the approach for delivering the capabilities. Community of Interest (COI) members must consider the normal certification and test processes when determining whether information sharing capabilities will be piloted or offered for operational use. The COI should base its approach on many factors, including technical and operational risk and the life-cycle stage of the data assets involved. For example, a COI may decide to develop a pilot capability that exposes data from existing systems in order to create a new asset before pursuing operational fielding of the capability. Leveraging exposed data from existing systems (instead of targeting programs in the new cycle), may enable the COI to field a capability faster and provide more immediate benefits to users.

Define measures of success. The COI's members should identify measures of success, including performance and resource-usage improvements. These measures should include metrics that can be used to assess the operational performance as well as provide insight into possible improvements in capability delivery (e.g., time to field, impacts on existing assets). When choosing to implement a pilot capability, it is important to assess whether the pilot effort will generate the intended capability to support the COI's mission, and whether the pilot capability technical solution can be integrated into the operational capability with a minimum of integration difficulty.

Create a capability plan. COIs, in collaboration with the appropriate stakeholders, should develop a capability plan, including a schedule and identification of the data assets of programs, systems, and organizations to be tagged and exposed. Additionally, the plan should include resource requirements; any intermediate demonstrations, pilot efforts, and tests that must be performed; and operational integration tasks. The capability plan should be communicated with the governing authority, system and data asset owners, and other COI stakeholders. Implementation of the plan can then be carried out by participating programs and their respective capability developers. Communications should include measures of success to evaluate capability implementation and user satisfaction.

7.4.2.2.3.3. Forward Planning

Evaluate the capability. During capability execution, Communities of interest (COIs) should extend success criteria to evaluate the overall impact of the information sharing capability on the mission objectives and the overall value of the effort to the Department of Defense. The COI should evaluate capability planning and execution in two ways, which are described above, and then capture lessons learned, also as described above.

Develop measures and metrics. In addition to metrics developed through the capability planning effort, COIs should develop metrics to assess the COI's progress relative to the DoD goals of net-centric information sharing and whether implementation resulted in a meaningful return on investment (ROI). In this instance, ROI indicates that the benefiting DoD Component or program of record has saved money by not having to build a new system to handle and re-create newly shared data. Other measures of ROI could include reduced cycle time and improved legal compliance. The COI should document the costs of implementation to provide a measure of the investment and should include a baseline assessment of relevant data assets to determine future capabilities.

Check user satisfaction. As part of the ongoing feedback loop, COIs should make data regarding the information sharing capability implementation available and accessible to consumers of the community's data, and gather input from these users. Gathering consumer, or user, input will enable the COI to gauge user satisfaction and determine whether the capability meets user needs and expectations.

Capture lessons learned by the COI. Capturing and communicating lessons learned is a key part of the COI's governance responsibilities. Lessons learned provide current and future best practices, baseline financial data, and provide other valuable insight into the fielding of new information sharing capabilities. Although there is no one-size-fits-all approach, COIs should leverage all available resources to avoid repeating past mistakes and duplicating current efforts. COIs should also plan to meet regularly with the appropriate portfolio manager and other stakeholders to review implementation results.

7.4.2.3. Data, Information, and IT Services Sharing Implementation

7.4.2.3.1. Making Data, Information, and IT Services Visible

7.4.2.3.1.1. Implementation Activities

7.4.2.3.1.2. Forward Planning

7.4.2.3. Data, Information, and IT Services Sharing Implementation

See Enclosure 3 DoD Directive 8320.02, " Sharing Data, Information, and Information

Technology (IT) services in the Department of Defense", March, 2013

Making data, information, and IT services visible, accessible, and understandable, and trusted are the cornerstones goals as indicated in the tables above. The creation of duplicative data and redundant capabilities often results from consumers' inability to locate, access, understand, or trust that existing assets meet their needs. Enclosure 3 describes procedures to guide Communities of Interest (COIs) in implementing these cornerstones.

7.4.2.3.1. Making Data, Information, and IT Services Visible

The Data Services Environment (DSE) is an integrated dashboard that brings together the existing capabilities (Metadata Registry [MDR], Net-Centric Publisher [NCP], Service Discovery [SD], Enterprise Authoritative Data Source [EADS] Registry) into a common modular framework. It contains the structural and semantic metadata artifacts critical to successful development, operation, and maintenance of existing and future capabilities that support the DoD Net-Centric Data Strategy and Net-Centric Services Strategy. Its goal is to facilitate information sharing across the DoD, allowing users to publish and discover information resources, data sources, and services. DISA maintains and operates the DSE under the direction and oversight of DoD CIO.

The DoD Data Services Environment contains the structural and semantic metadata artifacts critical to successful development, operation, and maintenance of existing and future capabilities that support the DoD Net-Centric Data Strategy. Its goal is to simplify the publication and discovery of data services that facilitate information sharing across the Department of Defense.

The Data Services Environment provides a one stop access to DoD data source directories to improve search, access, consistency, and integration of data services as well as to increase collaboration amongst data producers and consumers.

DSE promotes this vision by:

- Acting as a key enabler to make data "visible, accessible, and understandable".
- Providing greater data visibility and accessibility by implementing an Enterprise service.
- Streamlining search and access; providing a set of tools to register and discover data services across the Department.

The Data Services Environment is made up of several different components such as Enterprise Service Registry designed to support unique underlying requirements, models, users and workflows. The DSE publish feature provides users a clear set of workflows from a single interface point for publishing, managing and governing their assets that include:

- Semantic metadata artifacts such as service interface specifications, i.e. WSDL

files, supporting message formats, i.e. XML Schemas, as well as descriptive and informative documentation supporting those assets.
- Services and service metadata including service end points, service POCs, and service PMO.
- Authoritative data sources including systems, data stores and capabilities that fulfill particular data needs.
- DDMS records that include the core discovery information required by the DDMS Specification and publish that information to the enterprise catalog.

Users within the DoD Enterprise can discover and leverage various enterprise service offerings, they can discover the authoritative data sources that fulfill their data needs. Developers can locate information in such as service offers, service specifications, and taxonomical information, and they can readily reuse these existing entities to save time and avoid duplication of effort.

Making data, information, and IT services visible focuses on creating discovery metadata and deploying discovery capabilities that catalog these assets for users to find. The overall goal of data, information, and IT service visibility is to enable DoD users to sift through the enormous volume and variety of DoD information holdings and quickly discover assets that pertain to specific subjects of immediate interest. Discovery capabilities providing discovery metadata enable consumers to find out who is responsible for specific assets, where the assets are located, what kind of assets are available, and how to go about accessing them.

The discovery metadata may also include elements defined as COI extensions described in the in the DDMS. These elements are related to the subject matter of the asset, and are necessary for specialist consumers in a particular subject matter to locate relevant data assets.

7.4.2.3.1.1. Implementation Activities

Identify assets to share. Members of the community of interest (COI) should build a prioritized list of the assets it will initially make visible to the DoD via the Data Services Environment (DSE). The list should include descriptive information on each of the identified data assets such as POC information, including email addresses and telephone numbers; name of proposed or existing data access service and any related information resources; and a high-level narrative description. The primary candidates for the initial visibility effort should be the COI's current operational data assets, followed by mature developmental capabilities that are on a rapid deployment track to fill known mission data gaps and information needs. Prioritization occurs at the COI's discretion, taking into consideration organizational preparedness, technical ease of service implementation, law, policy and security classification restrictions, impact of broader access on the COI's operations, and the quantitative and qualitative improvements that might result from making a particular asset visible.

Define and register COI extensions for discovery metadata. One core purpose for

COIs is to foster agreements on the meaning and physical representation of their assets, as packaged and offered in deployed services. This includes the agreement on any metadata necessary to properly describe the community's, information and IT services data assets. The DDMS provides the minimum discovery metadata requirements to support enterprise discovery of these assets and can be extended by COIs to provide additional context that aids in the search for relevant data assets.

- *Enterprise Considerations.* The COI is in the position to anticipate how users might want to find data assets, in part based on the data assets' context or content. Supplementing the rudimentary discovery metadata elements, such as "Creator" or "Classification" found in the DDMS core, the COI extensions detail elements of discovery metadata that aid in enterprise-wide discovery of assets related to that COI.
- *Technical Guidance.* COI extensions to the DDMS may take the form of a data schema, and as such should be registered in the MDR, as part of the COI's set of agreed upon metadata artifacts. Formatting and technical guidance for COI extensions can be found in the DDMS.

Leverage work from other COIs. COIs should leverage the DSE to access guidance on technical, organizational, and procedural approaches to data asset publication. Other available information includes specific DDMS extensions registered by other COIs, data schemas for carrying product payload, taxonomies, and other data engineering artifacts. These models can provide a starting point for the COI efforts to reach agreement on common elements that will be important for users to discover COI data assets. Additional information regarding COIs that have registered metadata in the DoD Metadata Registry may be available in the COI Directory.

Associate discovery metadata with data assets. The association of discovery metadata with data assets is also referred to as "data tagging" within the context of data visibility. Data visibility is enhanced through the use and publication of discovery metadata that describe data assets. The implementation of "data tagging" mechanisms may vary by data asset and granularity of description. COI members should discuss possible methods of associating discovery metadata with capability developers or establish a COI working group to consider the issue and provide recommendations. In this way, the COI can determine the appropriate methods for the types of data assets the COI makes visible.

- *Enterprise Considerations.* Extensible Markup Language (XML)-based discovery metadata is currently the most flexible means of sharing discovery metadata throughout the DoD.
- *Technical Guidance.* To illustrate the distinction between physical and logical tagging and association of metadata, consider the example of a data asset in the form of a single file, such as a DoD Directive. Physically tagging a file would mean placing discovery metadata elements directly into that file, alongside its content. In contrast, logically associating discovery metadata with the file would involve creating a separate file, possibly XML based, containing discovery

metadata that describes the file. Software automation of this task is highly recommended; however, the precise mechanism will depend on the type of data asset and granularity of description. The DDMS provides the minimum required structure and content for discovery-related tags. By adhering to this specification for tagging, the minimum necessary discovery metadata to participate in federated searches will be available.

Create a discovery capability containing discovery metadata. Each COI should consult its governing authority to identify the information and resources associated with providing a discovery capability that the COI can use for its discovery metadata. The purpose of a discovery capability is to provide DDMS-formatted discovery metadata in response to federated searches. Capability developers will then leverage the COI's discovery metadata in the discovery capability, allowing authorized users to discover the COI's data assets.

- *Enterprise Considerations.* Extensible Markup Language (XML)-based discovery metadata is currently the most flexible means of sharing discovery metadata throughout the DoD.
- *Technical Guidance.* COIs can access the Defense Information Systems Agency Net-Centric Enterprise Services visibility guidance, which provides more specific technical guidance for discovery capabilities. COIs should use available and mature federated search specifications to ensure that discovery capabilities interoperate with the Enterprise properly. Enterprise discovery specifications also include requirements for service discovery. Service discovery metadata typically takes the form of a Universal Description, Discovery, and Integration description of a web service. COIs can also consult with other COIs, or other existing resources, for implementations of discovery capabilities and gain insights into the use of similar technology across the Department of Defense.

7.4.2.3.1.2. Forward Planning

COIs should establish, as part of its plan for long-term maintenance of COI metadata artifacts, a plan for maintaining the discovery metadata, the COI extensions to the DoD Discovery Metadata Specification, and the service discovery metadata. The goal is to make data visible as soon as possible and to develop those resources over time. The COI should agree on a schedule and process for how it will maintain the discovery metadata, to ensure that the data is always the most current.

7.4.2.3.1.3. Making Data, Information, and IT Services Accessible

7.4.2.3.1.3.1. Examples of Making Data, Information, and IT Services Accessible

7.4.2.3.1.3.2. Implementation Activities

7.4.2.3.1.3.3. Forward Planning

7.4.2.3.1.3. Making Data, Information, and IT Services Accessible

Making data, information and IT services accessible focuses on offering data assets over the network through commonly supported access methods. While making data, information and IT services visible involves creation and use of discovery metadata, making these assets accessible refers to providing access to the underlying information provided by the asset so that authorized DoD users can make use of it.

This section describes activities that aid in implementing paragraph 4.3 of DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004.

Individually negotiated interfaces between systems are brittle and inflexible; they support only the information transfers anticipated during development, not the "pull-on-demand" transfers that are a key part of net-centric data sharing. While point-to-point interfaces will continue to exist, DoD CIO Memorandum "DoD Net-Centric Data Strategy," May 9, 2003, emphasizes the need to transition those interfaces and implement new interfaces to support many-to-many information exchanges and authorized but unanticipated users. Data, information, and IT service producers should make data assets accessible using web-based approaches, minimizing the need for predefined, engineered point-to-point interfaces wherever operationally and technically possible.

7.4.2.3.1.3.1. Examples of Making Data, Information, and IT Services Accessible

- Providing a website displaying imagery for an Area of Responsibility for humans to use. (This example describes a method through which humans can get information.)
- Providing a web service through which a computer application can obtain imagery data in support of situation awareness. (This example describes a method through which a computer can retrieve raw sensor image data.)
- Providing a web service that an application can use to determine the flight trajectory of a missile. (This example describes a method for computer access to a process or calculation.)

7.4.2.3.1.3.2. Implementation Activities

Understand asset sharing constraints. The COI should identify any existing policies, laws, or data classifications that would restrict access to the data across the Enterprise. Traditional data access mechanisms will contain many implicit rules indicating how systems respond to requests, based on how the requests fall into a predefined process for handling the requests. Therefore, in addition to identifying explicit restrictions on access, the COI should also consider the potential for (and attempt to discern) built-in role-based access control systems. COIs should maintain awareness of evolving DoD information assurance, information security, and information sharing policies, and incorporate them as appropriate into COI activities and implementations.

Discover enterprise resources. The COI should leverage work products of other COIs, operational data access mechanisms that are available, and available net-centric interface standards and specifications.

- *Enterprise Considerations.* The COI can promote access mechanism reuse, and minimize the work required to obtain desired capabilities by collaborating with other COIs. In addition, the COI can make its own data accessible on an enterprise scale by adhering to existing technical standards. Interfaces developed using standard interface specifications enable COI-developed access mechanisms to exchange information readily with enterprise services resulting in wider access to the community's data assets.
- *Technical Guidance.* The Key Interface Profiles are the set of documentation produced as a result of interface analysis that designates an interface as key; analyzes it to understand it's architectural, interoperability, test, and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during analysis.

Identify assets to make accessible. The COI should determine which assets within the associated organizations, programs of record, sub-portfolios, etc., are likely to be of most value to those inside and outside the COI taking into account the potential for authorized but unanticipated users. The assets that the COI makes accessible will typically be a necessary component of the new information sharing capability identified by the COI.

- *Enterprise Considerations.* Part of the value of net-centric information sharing lies in its ability to afford authorized but unanticipated users with access to data, as needed. Taking this into account, COIs should assess information sharing options with the understanding that there might be other consumers in the DoD, external to the COI, who could make valuable use of the COI's data.

Define requirements for access mechanisms. The COI should define the priority of and functional requirements for data access mechanisms. Depending on the situation, the COI may base these requirements on an existing data access mechanism or establish them as part of an ongoing implementation plan. In setting requirements for data access mechanisms, the COI should take into account the type of assets; the security, license, and privacy considerations; and the static, dynamic, or streaming nature of data change. The data access mechanism specifications should conform to any agreements put forward by the stakeholders and the COI.

- *Technical Guidance.* The specific technology architecture for access mechanisms will depend on a number of factors, including the nature of the underlying asset, whether humans or machines will consume the asset, and the operational scenarios that surround the asset's use. Preferred architectures will use web-based technologies based on open standards, such as web services, portals, and web pages using Hypertext Markup Language and common web display standards. The DoD Information Technology (IT) Standards Registry

(DISR), according to DoD Directive 4630.05, provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The standards and guidelines in the DISR are stable, technically mature, and available via DISRonline.

Post descriptions of access mechanisms. Capability developers in the COI should publish metadata for any data access mechanisms the DSE and any other to available service registries, so that both known and authorized but unanticipated users may discover the service and understand how to interact with it.

- *Enterprise Considerations.* Publication of access mechanisms has two enterprise benefits: the first is enabling unanticipated users to find the service; the second is providing all background information necessary to reuse the service, deterring the development of redundant services.
- *Technical Guidance.* In the case of web services, enterprise specifications should be consulted for the minimum service discovery requirements to enable enterprise-wide discovery of COI data services. For instance, additional information in the form of a Universal Description, Discovery, and Integration description may be required to enable federated discovery and greater understanding of data services.

7.4.2.3.1.3.3. Forward Planning

Review systems for operational impact and scalability. Communities of interest should not degrade system performance for critical operational users to make data accessible. In addition, access mechanisms should be engineered for maximum scalability.

Develop expandable systems. Although such mechanisms need not immediately support the entire set of DoD users, they must be expandable to meet growth in demand.

7.4.2.3.1.4. Making Data, Information, and IT Services Understandable

7.4.2.3.1.4.1. Implementation Activities

7.4.2.3.1.4.2. Forward Planning

7.4.2.3.1.4. Making Data, Information, and IT Services Understandable

Making data, information and IT services understandable focuses on reaching agreement on the meaning of information provided by data assets and making that understanding available to consumers through the DSE. Data that is visible and

accessible is still not usable unless it is understandable. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum " DoD Net-Centric Data Strategy," May 9, 2003, provides for the existence of expedient communities of interest (COIs) that may have diverse needs, based on operational requirements. It is therefore not always safe to assume that consumers will be familiar with what a COI's data, information and IT services means, the way it is structured, or particularly how it fits into the COI's operational context. Most important, it is not necessarily the case that all consumers will be using these assets in the same way or for the same purpose. For example, "a tank" in the Army might refer to an armored vehicle, whereas "a tank" in the Navy might refer to a storage device for fluids. Although the data producer's perspective might be reasonable within the producer's context, the consumer might have a very different purpose in mind.

7.4.2.3.1.4.1. Implementation Activities

Discover enterprise resources. As part of developing a shared understanding of the community of interest's (COI) data, the COI should discover existing enterprise resources in order to maximize reuse of existing metadata artifacts.

Gather existing semantic metadata. The DSE will contain vocabularies, taxonomies, ontologies, conceptual data schemas, and other forms of semantic metadata from other COIs upon which the COI might base development of its own semantic metadata. In addition, the COI should discover existing semantic metadata among its members. In this way, the COI can start the process with a foundation in related semantics.

Gather existing structural metadata. The DSE also contains logical and physical data schemas that could aid the COI in forming structural representations that would be understandable to end-users. Data asset structure (such as whether dates are represented as normal, or as Julian dates) is an important aspect of understanding. By using the DSE and consulting COI members, the COI start the process with a foundation in related structures.

Develop a shared understanding of COI data made visible. COI members, pooling subject matter expertise, should collaborate on several semantic metadata artifacts that are crucial for providing context and meaning to any COI data that is made visible and accessible.

Agree on a shared vocabulary. The COI should use its own extensions to the DDMS as a starting point for the shared vocabulary. As a set of terms and definitions, the shared vocabulary should include any term used in the COI extensions, along with definitions that put these and other terms into proper COI context.

Agree on a conceptual data schema. The conceptual data schema indicates high-level data entities. Its coverage includes any entities in visible COI data assets, as well as the relationships between those data entities. The conceptual schema's coverage area may include multiple data assets, requiring that the COI come to an agreement on

how members will collaborate, possibly through a COI data working group, to develop the conceptual schema.

Agree on a COI taxonomy. A COI taxonomy is a categorization hierarchy indicating generalization and specialization relationships between terms; a submarine is a kind of sea-based asset, and an Abrams M1A1 is a kind of tank.

- *Enterprise Considerations.* Metadata artifacts such as the shared vocabulary, conceptual data schema, and taxonomy will be necessary for data consumers to understand a COI's data and to relate concepts within it. These artifacts will play a vital role in allowing mediation between COIs. The conceptual data schema indicates the general data subject area for consumers who are attempting to discover data assets relevant to their purpose.

Associate format- and content-related metadata. Content-related metadata is specifically aimed at providing content details, such as topics, keywords, context, and other information. Format-related metadata refers to how the data, information or IT service asset is formatted or represented. It is important that data assets use formats that are understandable to data consumers. The COI should agree on how these metadata elements will be associated with these assets, using the DDMS as the specification for guidance on specific elements that will be associated with data assets.

- *Enterprise Considerations.* Content metadata provides a basis for search engines to locate data assets by keyword or topic, and improves the human understandability of the data. Format-related metadata enables consumers to determine whether or not they can consume a data asset. COIs should avoid the use of less well known publication formats that require special software. A good, understandable publication format will be one that is widely known and for which no additional software for conversion to a more widely known format is required.
- *Technical Guidance.* For content-related metadata, relevant DDMS elements are located in the Subject category. For format-related metadata, recommended formats are typically open and common throughout the enterprise, such as Joint Photographic Experts Group imagery, MP3 audio files, Apple Quick Time videos, and Microsoft Office document formats.

Register the Metadata Artifacts. Registration of semantic and structural metadata within the DSE enables all users both anticipated and unanticipated to discover their existence, access them, and establish an understanding of the meaning and context of COI data.

- *Enterprise Considerations.* Registration of metadata artifacts enables unanticipated users and those outside the COI to discover the meaning and context of COI data and facilitates their reuse across the Department of Defense.
- *Technical Guidance.* Registering these artifacts means posting them to the DoD Metadata Registry. The COI can accomplish this by accessing the DoD Metadata

Registry and following the instructions for submission.

7.4.2.3.1.4.2. Forward Planning

Determine how the community of interest (COI) will maintain metadata artifacts. As the COI develops over time, the shared vocabulary, COI taxonomy, and other metadata artifacts that enable understandability should remain synchronized with the subject area they represent. To help it attain this objective, a COI could institute rules relating to how shared vocabulary updates occur. In addition, COI governance should be consulted for configuration management standards and related maintenance schedules.

- *Enterprise Considerations.* Unanticipated users will require and rely on up-to-date metadata artifacts to help them understand the context of discovered data assets and properly assess their relevance to their current mission.

Improve the understandability of the data, information, or IT service. The first iteration of metadata artifacts for understandability need not be ideal, since the goal is to make these assets available as soon as possible, rather than to have a perfect vocabulary on the first try. COIs should plan on improving their artifacts over time. Understandability is improved by providing more and better semantic metadata artifacts that capture and convey the knowledge consumers require to correctly use the asset.

Anticipate future mediation needs. Mediation is the process of reconciling one vocabulary with, or translating one vocabulary to, another. The need for such mediation is inevitable in an environment with many different systems and representation languages. By tracking which types of mediation occur or will occur most frequently, the COI can aggregate best practices surrounding the mediation of its data with other sources, as well as gain an understanding of what format and structural issues may exist. The COI should register metadata artifacts necessary for mediation in the DSE, which will facilitate their discovery and usage.

Ensure that data structure meets the consumers' needs, including those of unanticipated users. The physical structure of the data affects how the consumer will understand and utilize the data. Because it is not possible to know the unanticipated uses and needs of the data, COIs can engage in ongoing planning to change the structure of the data as it is exposed to the consumer via the access mechanism. Note that this sort of change represents a change to the access mechanism, not necessarily a change to the underlying data asset. Such changes can be meaningful only if they are made with consideration for user feedback.

7.4.2.3.1.5. Promoting Trust

7.4.2.3.1.5.1. Implementation Activities

7.4.2.3.1.5.2. Forward Planning

7.4.2.3.1.5. Promoting Trust

A consumer that can locate, access, and understand a particular data, information or IT service asset, will want to assess the authority of the that asset to determine whether the contents can be trusted. Promoting trust focuses on identifying sources clearly and associating rich pedigree and security metadata with the assets to support the consumer's trust decision.

While COIs can promote trust through implementation of the activities described in this section, this Guidebook does not provide COIs the authority to share information in any way that is prohibited by law, policy, or security classification.

7.4.2.3.1.5.1. Implementation Activities

Identify authoritative data sources. The community of interest (COI) should make every effort to identify data assets that are authoritative sources for data, as well as identifying in what contexts the data is authoritative. In situations where there is more than one authoritative source, depending on how the data is used, the COI should indicate the business process for which the authority is valid.

- *Enterprise Considerations.* The COI should consider the ownership and stewardship of data sources when determining authoritativeness. Active stewardship in the ADS Registry of the DSE will help maintain the quality and relevance of authoritative data sources for those internal and external to the COI.
- *Technical Guidance.* Authoritative sources may vary by COI (e.g., one community may define an authoritative source for location data to be the United States Postal Service, whereas another community might define an authoritative source for location data to be an intelligence database). In addition, a community might define more than one authoritative source for a particular type of data (e.g., a budget and planning community might have an authoritative source for budget data for each Military Department).

Associate trust discovery metadata with data, information, and IT service assets. The COI should include trust discovery metadata to support data consumers' decisions on which assets are appropriate for their use. There are three categories of trust discovery metadata. These are discussed in the following subparagraphs.

- *Asset pedigree metadata.* The source and lineage of an asset are its pedigree. The purpose of the pedigree is to enable consumers to determine whether the asset is fit for their intended use and to enable them to track the flow of information, its transformations, and modifications, through assets. Notional metadata describing an asset's pedigree would include creation date, modification date, processing steps (including methods and tools), source and author (if known) status, and validation results against a published set of

constraints.

- *Security labels.* Security labels provided in discovery metadata enable services to restrict access to data assets on the basis of a COI's identified parameters, including classification and dissemination controls. Preventing unauthorized access to data assets is important to promote trust in the data among authorized users.
- *Associate rights protection metadata.* Rights protection metadata refers to metadata that indicates any copyright, trade secret, trademark, licensing, proprietary information, Privacy Act, or other usage restriction. As such, it may not be appropriate for all assets. Nevertheless, where this metadata does apply, it is important that it be provided. Consumers and data access services can only protect data against inappropriate use if they are informed of restrictions.
- *Technical Guidance.* The DoD Discovery Metadata Specification (DDMS) references the security elements found in the Intelligence Community Metadata Working Group document, specifying 18 attributes that can be used for information in classification and controls marking. The DDMS category named "Security" contains relevant elements addressing classification and dissemination. The "Source" category contains elements for asset pedigree metadata, and the "Rights" category contains applicable elements for rights protection metadata. The COI can obtain background on security tagging by checking the Intelligence Community Metadata Standard for Information Security Markings and accessing the Data Element Dictionary.

7.4.2.3.1.5.2. Forward Planning

Because a data asset can be trusted only if its contents are sufficiently accurate and of sufficiently reliable quality, assessing and improving data asset quality is important. Quality assertions about data include information on its accuracy, completeness, or timeliness for a particular purpose. For example, consumers might need to know the age of the data to determine whether it is trustworthy, or they might need to know how accurate estimates and figures within the data asset are. Typically, such metadata results from a separate data quality analysis of an asset. The community of interest (COI) may develop an ongoing process for auditing the quality of data assets that are made visible and accessible. This process should be designed in concert with the COI leadership's ongoing quality assurance and configuration management efforts .

7.4.3. Integrating Net-Centric Information Sharing into the Acquisition Life Cycle

7.4.3.1. Data, Information, and IT Services Planning Activities

7.4.3.2. Data, Information, and IT Services Planning

7.4.3.3. Manage Data Infrastructure [Determine Infrastructure Requirements]

7.4.3.4. Provide Enterprise Data Assets

7.4.3.5. Govern Data Activities

7.4.3. Integrating Net-Centric Information Sharing into the Acquisition Life Cycle

A description of the program's approach for ensuring that information assets will be made visible, accessible, and understandable to any potential user as early as possible (DoD Directive 8320.02, "Sharing Data, Information, and Information Technology (IT) services in the Department of Defense, March, 2013"). Recommended scope of data, information and IT services activities follow:

7.4.3.1. Data, Information, and IT Services Planning Activities

Define Net-Centric Data, Information, and IT Services Sharing Plan

This activity relates to the development of a comprehensive net-centric plan to share data assets within your program/organization and to the Enterprise. This includes metadata catalog plans, registry plans, interoperability plans, etc. In essence, this Net-Centric Data Sharing Plan should be the program's/organization's plan to accomplish the goals of the DoD Net-Centric Data Strategy. This is a key product and will drive most data activities and architectures.

Responsibilities: Sponsor/Domain Owners should develop these plans at a broad, strategic level to ensure that architectures for programs and sub-organizations associated with the Domain include net-centric data components. Depending on the scale of the program or system, Program Managers (PMs) should develop a more detailed plan that outlines how their information architecture(s) make their assets and processes discoverable, accessible, and understandable to both known and unanticipated users. These program sharing plans should ensure that they align with and make use of enterprise net-centric data, information and IT services sharing capabilities such as those envisioned/planned under core enterprise services.

Define Data Guidance

Evaluate information from sources such as compliance reports, incentive plan reports, policy, and user needs to create net-centric data, information and IT services guidance documents. This guidance is the policy, specifications, standards, etc., used to drive activities within the program/organization. It differs from a net-centric data or services plan in that the plan is more strategic in nature. Data guidance may be a subset of an overall net-centric data sharing plan.

Responsibilities: Sponsor/Domain Owners should develop appropriate issuance and standards to ensure that incentives, metrics, and direction are in place to drive the transition to net-centricity. Sponsor/Domain Owners should establish policy and governance to ensure that the Domain's Programs and sub-organizations have a voice in the development of standards, specifications, and processes (e.g., empowering a

Program to insert its metadata requirements into an overall Domain metadata model).

Define Data, Information, and IT Services Sharing Data Architectures

Build upon existing and revised architectures and plans to describe the architecture to support data sharing objectives. The architecture should depict components that emphasize the use of discovery, services-based approach to systems engineering, use of metadata to support mediated information exchange, web-based access to data assets, etc.

Responsibilities: Both Sponsor/Domain Owners and PMs should include net-centric concepts, activities, and processes into their architectures. Sponsor/Domain Owners should ensure that their Domain-level architectures are developed in a manner that is appropriate for governing under a capabilities-based portfolio management process. PMs should ensure that net-centric components are integrated into their program architecture products.

7.4.3.2. Data, Information, and IT Services Planning

Identify Data Assets

Determine what data assets (documents, images, metadata, services, etc.) are produced or controlled within a program or organization. This is primarily an inventory of data assets, which should include both structured and unstructured data sources as well as IT services.

Responsibilities: Sponsor/Domain Owners should identify major data assets created or managed within their Domain. This asset listing will assist in the development of visibility, accessibility, and understandability strategic plans (i.e., based on the composition of the major data assets within the Domain, the planning products can reflect the most appropriate approach in supporting net-centric information sharing data strategy goals). Likewise, Program Managers (PMs) should inventory the data assets created or managed by the program and use this asset listing to plan their strategy and implementation approach for making these assets net-centric.

Prioritize Data Assets

Assess the data asset inventory to identify key data products that are of greatest value to known users and are likely to be of value to unanticipated users. This list should be used to determine data assets a program/organization should make initial efforts at exposing as enterprise data assets.

Responsibilities: Both Sponsor/Domain Owners and PMs should analyze and prioritize which data assets are most valuable, initially, to be exposed as enterprise data assets.

Define Communities of Interest (COIs)

Identify appropriate groups of people who should come together to support common mission objectives. COIs are an appropriate construct for defining information exchange formats and metadata definitions as well as vocabularies used to communicate within the COI. This activity does not include the establishment of actual COIs. This is simply the process of identifying COIs that exist or should exist.

Responsibilities: Sponsors/Domain Owners should define major COIs that could benefit missions within the Domain (and across Domains). PMs should identify other COIs that serve the goals of the program and its associated functional areas.

7.4.3.3. Manage Data Infrastructure [Determine Infrastructure Requirements]

Manage Discovery Metadata Catalog(s)

Identifying/establishing and maintaining searchable catalogs used to locate data assets within the program, organization, or enterprise. Metadata stored within these catalogs facilitates discovery and includes descriptive information about each shared data asset.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata catalogs that allow for the search of data assets across the Domain. Distributed, federated approaches should be used in developing this capability. Program Managers (PMs) should ensure that their data is tagged and posted to metadata catalogs that are tied into the Domain metadata catalog.

Manage Metadata Registry(s)

Identifying and/or establishing metadata registries that can be used to maintain, manage, and/or search for metadata artifacts such as schema and data definitions. Metadata stored in metadata registries are typically for developers, business analysts, and architects. Metadata registries are a type of metadata catalog specifically designed to support developers/business analysts.

Responsibilities: Sponsor/Domain Owners should ensure that metadata products within their Domain (including associated programs and sub-organizations) are registered into the DoD Metadata Registry. Domain Communities of Interest (COIs) are likely to be structured around the functional areas for which metadata is registered. PMs should ensure that program metadata is registered in the DSE and is maintained.

Manage Service Directory(s)

Identifying and/or establishing service directory(s) that can be used to maintain, manage, and/or search for callable, reusable services from which net-centric capabilities are built. Metadata stored in service directories gives information as to the services available, how to call them, and possibly, expected service levels. Service

directories include Universal Description, Discovery, and Integration Directories used to maintain Web Services information. This is a key component of establishing a services-based architecture that supports net-centric data tenets.

Responsibilities: Sponsor/Domain Owners should ensure that services created or managed within their Domain (including associated programs and sub-organizations) are registered into the DoD Data Services Environment (DSE) maintained by the Defense Information Systems Agency. PMs should ensure that program services are registered in the DSE.

Manage Interoperability Components

Development of metadata artifacts used to enable the interchange of data and information including document vocabularies, taxonomies, common data models, schema, formats, mediation components, and interface specifications.

Responsibilities: Sponsor/Domain Owners should establish Domain-level metadata models to facilitate the loosely-coupled exchange of information between systems. PMs should develop metadata models (e.g., data structures, schema, etc) pertinent to their program. This includes tagging models, service schema, and mapping models to the Domain metadata model.

Develop/Acquire Data Access Mechanism(s)

Post data assets to an information sharing application (e.g., end-user web site, a file system, a document repository) or through the use of web services to provide system-to-system access, etc.

Responsibilities: Sponsor/Domain Owners should establish shared space, as necessary, to support Program's within its scope. PMs should ensure that web-enabled services provide access to valuable systems data and processes.

Manage COIs

This activity encompasses establishing Mission Area sponsored COI(s), registering COI(s) in the Enterprise COI Directory, and COI participation. The outcomes of this activity will ensure that COI(s) can be located and managed throughout the enterprise.

Responsibilities: Both Sponsor/Domain Owners and PMs should establish, register, and maintain identified COIs.

7.4.3.4. Provide Enterprise Data Assets

Provide Discovery Metadata

Associate or generate discovery metadata for data assets. This activity is the 'tagging'

of data assets to provide value-added information about data assets that can be used to support discovery, accessibility, information assurance, and understandability.

Responsibilities: Program Managers (PMs) should ensure that discovery metadata is provided for all data assets created/managed by the Program.

Post Discovery Metadata

Providing, or posting, discovery metadata to catalogs, registries, etc., that can be searched. It is through 'posting metadata' that metadata catalogs are populated. This activity allows data assets to be discovered (but does not guarantee access to the data asset).

Responsibilities: PMs should ensure that discovery metadata associated with each data asset is posted to searchable metadata catalogs (established by the Domain and by Programs).

7.4.3.5. Govern Data Activities

Participate in DoD Information Enterprise (DoD IE) Governance

Participate in governance activities that enable net-centric data asset sharing. This includes participation in DoD IE Enterprise Service efforts, net-centric architectural compliance, Capabilities Portfolio Management for net-centric information sharing, etc.

Responsibilities: Sponsor/Domain Owners should participate in DIE governance activities to ensure the proper processes are followed and executed within their Domain to enable the net-centric Domain environment.

Enforce Data Guidance

Participate in enforcement/compliance activities that assess net-centric architectures against Net-Centric Data Guidance that was developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and PMs should enforce established data guidance (including conformance to standards and adherence to DoD/Domain issuances).

Advocate Data Strategy(s)

This activity involves vetting, publicizing, and institutionalizing the Net-Centric Data Sharing plans and guidance developed in the Data Planning process.

Responsibilities: Both Sponsor/Domain Owners and PMs should advocate the DoD Net-Centric Data Strategy and Domain-established data guidance.

7.4.4. Supporting Language for Information Technology (IT) System Procurements

7.4.4. Supporting Language for Information Technology (IT) System Procurements

To ensure support of the goals of *NCDS*, the Program Manager (PM), through his or her contracting specialists, should include the following sections, as appropriate, in Request for Proposal (RFP)/Request for Quotation (RFQ) language for the procurement of IT systems.

The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the Defense Information Enterprise Architecture 1.1, dated May 27, 2009, and its subsequent official updates and revisions. The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of the DoD Net-Centric Data Strategy dated May 9, 2003, and comply with the Department's data strategy as defined in DoD Directive 8320.02, Sharing Data, Information, and Information Technology (IT) services in the Department of Defense", March, 2013. The contractor shall ensure that any IT systems covered in this procurement or identified in this RFP/RFQ support the goals of DoD Net-Centric Services Strategy, Strategy for a Net-Centric, Service Oriented DoD Enterprise, March, 2007.

Also, the contractor must ensure that any IT systems covered in this procurement or identified in this RFP/RFQ meet the requirements detailed below. Additionally, it is acceptable for vendors and/or integrators to provide functionality (via wrappers, interfaces, extensions) that tailor the COTS system to enable these requirements below (i.e., the COTS system need not be modified internally if the vendor/integrator enables the requirements through external or additional mechanisms. In this case, these mechanisms must be acquired along with the COTS system procurement).

- Access to Data: *The contractor shall ensure that all data managed by the IT system can be made accessible to the widest possible audience of DIE users via open, web-based standards. Additionally, the system's data should be accessible to DIE users without 1) the need for proprietary client-side software/hardware, or 2) the need for licensed user-access (e.g. non-licensed users should be able to access the system's data independent to the licensing model of the COTS system). This includes all data that is used to perform mission-related analysis and processing including structured and unstructured sources of data such as databases, reports, and documents. It is not required that internal, maintenance data structures be accessible.*
- Metadata: *The contractor shall ensure that all significant business data made accessible by the IT system is tagged with descriptive metadata to support the net-centric goal of data visibility. Accordingly, the system data shall be tagged to comply, at a minimum, with the DoD Discovery Metadata Specification (DDMS). This specification is available at: http://metadata.ces.mil/dse/irs/DDMS/ . The*

system should provide DDMS-compliant metadata at an appropriate level based on the type of data being tagged. It is not required that individual records within databases be tagged; rather it is expected that the database itself or some segment of it is tagged appropriately. Additionally, the contractor shall ensure that all structural and vocabulary metadata (metamodels, data dictionaries) associated with the exposed system data be made available in order to enable understanding of data formats and definitions. This includes proprietary metadata if it is required to effectively use the system data.

- Enterprise Services/Capabilities: *The contractor shall ensure that key business logic processing and other functional capabilities contained within the IT system are exposed using web-based open standards (e.g., application programming interfaces provide for Web Services-based access to system processes and data). The level of business logic exposure shall be sufficient to enable reuse/extension within other applications and/or to build new capabilities. The contractor shall provide an assessment of how any licensing restrictions affect or do not affect meeting the goals of re-use and exposure as DoD Information Enterprise-wide enterprise services.*

Optional Components/Modules: *The contractor shall ensure that all standard and/or optional components of the IT system are identified and procured in a manner that ensures the requirements outlined in this document are met.*

7.5. Information Assurance (IA)

7.5.1. Information Assurance (IA) Overview

7.5.2. Mandatory Policies

7.5.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

7.5.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

7.5.2.3. DoD Directive 8500.01E, "Information Assurance (IA)"

7.5.2.4. DoD Instruction 8500.2, "Information Assurance (IA) Implementation"

7.5.2.5. DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System"

7.5.2.6. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"

7.5.2.7. DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management"

7.5.2.8. DoD Instruction 8581.01, "Information Assurance (IA) Policy for Space

7.5.1. Information Assurance (IA) Overview

Most programs delivering capability to the warfighter or business domains will use information technology (IT) to enable or deliver that capability. For those programs, developing a comprehensive and effective approach to IA is a fundamental requirement and will be key in successfully achieving program objectives. The Department of Defense defines IA as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Program Managers (PMs) and functional proponents for programs should be familiar with statutory and regulatory requirements governing information assurance, and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the program's architecture, developing an Acquisition IA Strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program. The information in the following sections explains these tasks, the policy from which they are derived, their relationship to the acquisition framework, and the details one should consider in working towards effective IA defenses-in-depth in a net-centric environment.

Note: DAG Section 7.5 will be re-written to reflect the re-issuance of DoDI 8500.01 Cyber security and DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) instructions are signed and published. Until then, the current information provided in Section 7.5 remains valid.

7.5.2. Mandatory Policies

7.5.2.1. DoD Directive 5000.01, "The Defense Acquisition System"

Paragraph E1.1.9. "Information Assurance," states:

Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and IT programs that depend on external information sources or provide information to other DoD systems. DoD policy for information assurance of IT, including NSS, appears in DoD Directive 8500.01E.

7.5.2.2. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

Table 8, "Title 40/CCA Compliance," in enclosure 5 requires the following of acquisition PMs:

Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

7.5.2.3. DoD Directive 8500.01E , "Information Assurance (IA)"

This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve DoD information assurance through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare. According to DoD Directive 8500.01E, all acquisitions of DoD Information Systems (to include Automated Information System applications, Outsourced IT-based Processes, and platforms or weapon systems) with connections to the Global Information Grid, must be certified and accredited.

This Directive will be re-written and combined with the revised DoDI 8500.2 and published in Q4FY13 as DoDI 8500.01. The ramifications of the revised policy will move the DoD to the Risk Management Framework as implemented by the National Institute of Standards and Technology (NIST) 800 series Special Publications.

7.5.2.4. DoD Instruction 8500.2, "Information Assurance (IA) Implementation"

This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.01 E. This Instruction is under revision. The ramifications of the revised policy will institute a shift from the current DoD IA control catalog to the NIST SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations".

7.5.2.5. DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System"

This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate information assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy and its applicability and prescribes an Acquisition IA Strategy submission and review process.

7.5.2.6. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)"

This instruction establishes the DoD information assurance (IA) certification and

accreditation (C&A) process for authorizing the operation of DoD information systems consistent with the Federal Information Security Management Act and DoD Directive 8500.01E. The instruction superseded DoD Instruction 5200.40 (DITSCAP) and DoD 8510.1-M (DITSCAP Manual). The DIACAP process supports net-centricity through an effective and dynamic IA C&A process. It also provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DoD information systems, to include core enterprise services and web services-enabled software systems and applications. This Instruction is under revision with the new version due Q4FY13. The ramifications of the revised policy will institute a shift from the current DIACAP process to DoDs adoption, implementation, execution, and maintainance of the NIST RMF.

7.5.2.7. DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management"

This directive establishes policy and assigns responsibilities for DoD IA training, certification, and workforce management. Along with the accompanying manual, it provides guidance and procedures for the identification and categorization of positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in the manual.

7.5.2.8. DoD Instruction 8581.01, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense"

This instruction implements requirements of National Security Directive 42 by establishing IA policy and assigning responsibilities for all space systems used by the Department of Defense in accordance with Committee on National Security Systems Policy No. 12. The instruction supplements IA policy and requirements contained in DoDD 8500.01E and DoDI 8500.2.

7.5.2.9. Other Processes

Other Certification and Accreditation processes (such as Intelligence Community Directive (ICD) 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation") are applicable for systems processing Sensitive Compartmented Information.

7.5.2.10. DoD Strategy for Operating in Cyberspace (July 14, 2011)

This strategy recognizes that cyberspace is a key sector of the global economy. The security and effective operation of U.S. critical infrastructure including energy, banking and finance, transportation, communication, and the Defense Industrial Base rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation. This strategy notes that foreign cyberspace

operations against U.S. public and private sector systems are increasing in number and sophistication.

Accordingly, Program Managers must ensure procedures and processes are in place for the protection of DoD program information residing on or transiting corporate unclassified networks and information systems. The objective is to protect DoD information, not just DoD systems, and it relates to all programs, not just those IT focused. Several policy documents provide additional guidance in this area for inclusion in developing the IA Strategy and RFP IA clauses.

7.5.2.11. Critical Program Information

DoDD 5200.39 Critical Program Information establishes policy to provide comprehensive protection of CPI through the integrated and synchronized application of CI, Intelligence, Security, systems engineering, and other defensive countermeasures to mitigate risk. Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighters capability and DoDs technological superiority.

7.5.3. Information Assurance (IA) Integration into the Acquisition Life Cycle

7.5.3.1. Before Milestone A

7.5.3.2. Before Milestone B

7.5.3.3. Before Milestone C

7.5.3.4. After Milestone C or before the Full Rate Production Decision Review (or equivalent for MAIS Programs)

7.5.3.1. Before Milestone A

Examine program and system characteristics to determine whether compliance with DoD Directive 8500.01E is recommended or required, and whether an Acquisition IA Strategy is required. (Click here for guidelines on making this determination.)

Establish an IA organization. Appoint a trained IA professional in writing as the IA Manager. This and other IA support may be organic to the program office, matrixed from other supporting organizations (e.g., Program Executive Office), or acquired through a support contractor.

Begin to identify system IA requirements. Click here for Baseline IA Controls or IA Requirements Beyond Baseline Controls.

Develop an Acquisition IA Strategy, if required. Click here for IA Compliance Decision Tree or here for an Acquisition IA Strategy Template. Acquisition IA strategies

developed in preparation for Milestone A will be more general, and contain a lesser level of detail than acquisition IA strategies submitted to support subsequent Milestone decisions. Click here to see the Acquisition IA Strategy Instructions.

7.5.3.2. Before Milestone B

If program is initiated post-Milestone A, complete all actions for Milestone A.

Update and submit the Acquisition IA Strategy. Click here for an Acquisition IA Strategy Template.

Secure resources for IA. Include IA in program budget to cover the cost of developing, procuring, testing, certifying and accrediting, and maintaining the posture of system IA solutions. Ensure appropriate types of funds are allocated (e.g., Operations & Maintenance for maintaining IA posture in out years).

Initiate the DoD Information Assurance Certification and Accreditation Process (DIACAP) , or other applicable Certification & Accreditation process (such as Intelligence Community (ICD) 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" for systems processing Sensitive Compartmented Information).

7.5.3.3. Before Milestone C

Incorporate Information Assurance (IA) solutions through:

- Employment of Information Systems Security Engineering (ISSE) efforts to develop or modify the IA component of the system architecture to ensure it is in compliance with the IA component of the GIG architecture and makes maximum use of enterprise IA capabilities and services.
- Procurement of IA/IA-enabled products. DoD Instruction 5000.02, paragraph 6 of Enclosure 5, states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made." The Enterprise Software Initiative (ESI) includes commercial IA tools and should be used as the preferred source for the procurement of IA tools. The ESI Home Page lists covered products and procedures. DFARS (SUBPART 208.74) lists additional requirements for compliance with the DoD ESI. In addition to ESI, the NSTISSP-11 (NIAP) should be used for IA and IA-enabled products.
- Implementation of security policies, plans, and procedures.
- Conducting IA Training.

Test and evaluate IA solutions. See Chapter 9, Test and Evaluation (T&E), for information on testing.

- Developmental Test.

- Security Test & Evaluation, Certification and Accreditation activities.
- Operational Test.

Accredit the system under the DIACAP or other applicable Certification and Accreditation process. For systems using the DIACAP, an Authorization to Operate should be issued by the Designated Accrediting Authority.

7.5.3.4. After Milestone C or before the Full Rate Production Decision Review (or equivalent for MAIS Programs)

Maintain the system's security posture throughout its life cycle. This includes periodic re-accreditation.

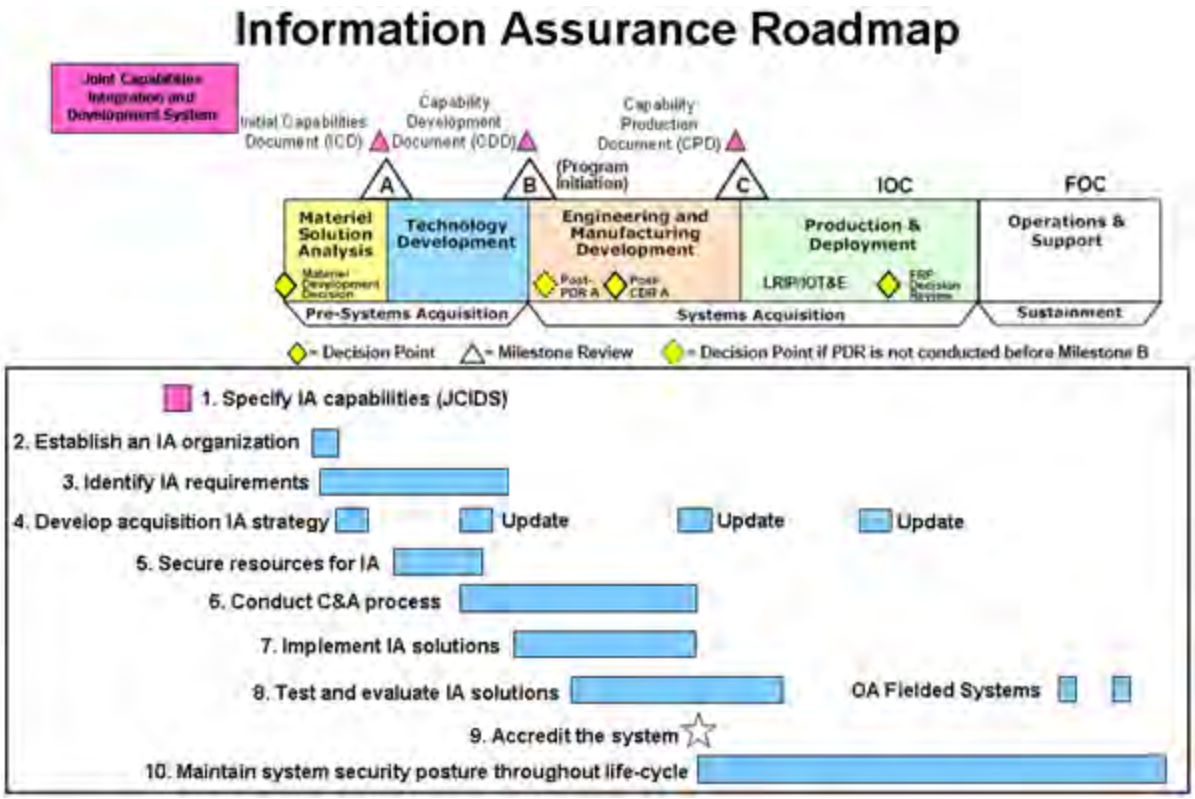
Assess IA during IOT&E on the mature system.

7.5.4. Estimated Information Assurance (IA) Activity Durations and Preparation Lead Times

7.5.4. Estimated Information Assurance (IA) Activity Durations and Preparation Lead Times

Figure 7.5.4.F1 shows the relationship between the acquisition framework and typical timeframes for accomplishing key IA activities.

Figure 7.5.4.F1. Typical Timeframes for Accomplishing Key IA Activities



[7.5.5. Integrating Information Assurance (IA) into the Acquisition Process](#)

7.5.5. Integrating Information Assurance (IA) into the Acquisition Process

Table 7.5.5.T1, IA Compliance by Acquisition Program Type is designed to help PMs determine the degree to which the 8500 series applies to a system acquisition and whether an Acquisition IA Strategy is required.

Table 7.5.5.T1. IA Compliance by Acquisition Program Type

Acquisition Programs for:	Acquisition IA Strategy	Compliance with 8500 Series
No IT	Not Required	Not Required
Non-MC/ME AIS	Not Required *	Required
Non-MC/ME MAIS	Not Required *	Required
MC/ME AIS	Required	Required
MC/ME MAIS	Required	Required
Outsourced IT-based Processes that are not MC/ME	Not Required *	Required
Outsourced IT-based Processes that are MC/ME	Required	Required
Platform IT products/weapons systems that are, or have:		

MC/ME	Network Interconnections to the GIG		
No	No	Not Required *	*Recommended **
No	Yes	Not Required *	Required
Yes	No	Required	*Recommended **
Yes	Yes	Required	Required

Legend: AIS = Automated Information System
GIG = Global Information Grid
IT = Information Technology
MAIS = Major Automated Information System
MC/ME = Mission Critical / Mission Essential
PM = Program / Project Manager

*** Although not required by DoD, the Component may require an Acquisition IA Strategy.**
**** PMs would be prudent to comply with all DoDI 8500.2 IA controls appropriate to the system.**

Because requirements for IA vary greatly across acquisition programs, PMs should examine acquisition programs carefully to identify applicable IA requirements. The following guidelines derived from DoD Directive 8500.01E apply:

1. Programs that do not involve the use of IT in any form have no IA requirements. PMs should carefully examine programs, however, since many programs have IT (such as automatic test equipment) embedded in the product or its supporting equipment.
2. Programs that include IT always have IA requirements, but these IA requirements may be satisfied through the normal system design and test regimen, and may not be required to comply with DoD Directive 8500.01E. Acquisitions that include Platform IT with no network interconnection to the GIG fit into this category. However, such programs require an Acquisition IA Strategy if they are designated Mission Critical or Mission Essential.
3. Acquisitions of Platforms with network interconnections to the GIG must comply with the IA requirements of DoD Directive 8500.01E and DoD Instruction 8500.2.
4. Acquisitions of AIS applications or outsourced IT processes also must comply with DoD Directive 8500.01E and DoDI 8500.2.
5. Programs that include IT, and that are designated Mission Critical or Mission Essential, require an Acquisition IA Strategy without regard to the applicability of DoD Directive 8500.01E. The DoD Component Chief Information Officer (CIO) is responsible for approving the Acquisition IA Strategy. Subsequent to DoD Component CIO approval, in accordance with DoD Instruction 8580.1, the DoD CIO must review the Acquisition IA Strategy.

7.5.6. Program Manager (PM) Responsibilities

7.5.6.1. Platform Information Technology (IT) Systems

PMs for acquisitions of platforms with internal IT (including platforms such as weapons systems, sensors, medical technologies, or utility distribution systems) remain ultimately responsible for the platform's overall IA protection. If the Platform IT has an interconnection to the GIG, in accordance with DoD Instruction 8500.2, the PM must identify all assurance measures needed to ensure both the protection of the interconnecting GIG enclave, and the protection of the platform from connection risks (such as unauthorized access), that may be introduced from the enclave. However, connecting enclaves have the primary responsibility for extending needed IA services (such as Identification and Authentication) to ensure an assured interconnection for both the enclave and the interconnecting platform. These IA requirements should be addressed as early in the acquisition process as possible.

PMs for acquisitions of platforms with IT that does not interconnect with the GIG retain the responsibility to incorporate all IA protective measures necessary to support the platform's combat or support mission functions. The definition of the GIG recognizes "non-GIG IT that is stand-alone, self-contained or embedded IT that is not or will not be connected to the enterprise network." Non-GIG IT may include "closed loop" networks that are dedicated to activities like weapons guidance and control, exercise, configuration control or remote administration of a specific platform or collection of platforms. The primary test between whether a network is part of the GIG or is non-GIG IT is whether it provides enterprise or common network services to any legitimate GIG entity. In any case, PMs for systems that are not connected to GIG networks should consider the IA program provisions in DoD Directive 8500.01E and DoD Instruction 8500.2, and should employ those IA controls appropriate to their system.

7.5.6.2. Automated Information Systems (AIS)

PMs for acquisitions of AIS applications are responsible for coordinating with enclaves that will host (run) the applications early in the acquisition process to address operational security risks which the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement. The baseline IA Controls serve as a common

framework to facilitate this process. The Designated Accrediting Authority for the enclave receiving an AIS application is responsible for incorporating the IA considerations for the AIS application into the enclave's IA plan. The burden for ensuring that an AIS application has adequate assurance is a shared responsibility of both the AIS application PM and the Designated Accrediting Authority for the hosting enclave; however, the responsibility for initiation of this negotiation process lies clearly with the PM. PMs should, to the extent possible, draw upon the common IA capabilities that can be provided by the hosting enclave.

7.5.6.3. Outsourced Information Technology (IT)-based Processes

PMs for acquisitions of Outsourced IT-based Processes must comply with the IA requirements in the 8500 policy series. They are responsible for delivering outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services that present specific and unique challenges for the protection of the GIG. The PM for an Outsourced IT-based process should carefully define and assess the functions to be performed and identify the technical and procedural security requirements that must be satisfied to protect DoD information in the service provider's operating environment and interconnected DoD information systems.

A unique type of Outsourced IT-based Process is "Managed Enterprise Services." These are defined as "Private sector information systems, outsourced information technologies, or outsourced information services managed, maintained and administered as a performance-based service (whether delivered from vendor facilities or within DoD facilities) that delivers a DoD-wide service included within the Enterprise Information Environment Mission Area (EIEMA), as an outsourced IT-based process." Managed Enterprise Services envision two broad categories of implementation scenarios:

- In one scenario, the service is hosted at vendor facilities, and accordingly, DoD does not have significant control of the operations of the Managed Enterprise Service.
- In the second scenario, the Managed Enterprise Service is hosted in a DoD facility, but operations are provided by one or more vendors. Managed services that are DoD Component-wide or that belong to the warfighter or business mission areas are outside the scope of Managed Enterprise Services. If your acquisition includes Managed Enterprise Services, see DoD CIO Memorandum "Certification and Accreditation Requirements for DoD-wide Managed Enterprise Services Procurements," dated June 22, 2006.

7.5.6.4. Privacy Impact Assessment (PIA)

A PIA is an analysis of whether personally identifiable information (PII) when collected in electronic form is stored, shared, and managed in a manner that protects the privacy of individuals. Section 208 of Public Law 107-347 requires that a PIA be conducted prior

to developing or purchasing any DoD information system that will collect, maintain, use, or disseminate PII about members of the public. The DoD Instruction 5400.16 provides procedures for completing and approving PIAs and expanded the requirement to include federal personnel, DoD contractors and, in some cases, foreign nationals.

7.5.7. Information Assurance (IA) Controls

7.5.7.1. Mission Assurance Category (MAC) and Confidentiality Level

DoD Instruction 8500.2, Enclosure 3, establishes fundamental IA requirements for DoD information systems in the form of two sets of graded baseline IA Controls. PMs are responsible for employing the sets of baseline controls appropriate to their programs. The baseline sets of IA controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels as specified in the formal requirements documentation or by the User Representative on behalf of the information owner. IA Controls addressing availability and integrity requirements are keyed to the system's MAC based on the importance of the information to the mission-particularly the warfighters' combat mission. IA Controls addressing confidentiality requirements are based on the sensitivity or classification of the information. There are three MAC levels and three confidentiality levels with each level representing increasingly stringent IA requirements. The three MAC levels are identified in Table 7.5.7.1.T1.

Table 7.5.7.1.T1. Mission Assurance Category (MAC) Levels for IA Controls

MISSION ASSURANCE CATEGORY			
	Definition	**Integrity**	**Availability**
1	These systems handle information that is determined to be **vital to the operational readiness of mission effectiveness of deployed and contingency forces** in terms of both content and timeliness.	**HIGH**	**HIGH**
2	These systems **handle information that is important to the support of deployed and contingency forces.**	**HIGH**	**MEDIUM**

3	These systems handle information that is necessary for the conduct of day-to-day business, but **does not materially affect support to deployed or contingency forces in the short-term.**	**BASIC**	**BASIC**

The other major component in forming the baseline set of IA controls for every information system is determined by selecting the appropriate confidentiality level based on the sensitivity of the information associated with the information system. DoD has defined three levels of confidentiality, identified in Table 7.5.7.1.T2.

Table 7.5.7.1.T2. Confidentiality Levels for IA Controls

Confidentiality Level	Definition
Classified	Systems processing classified information
Sensitive	Systems processing sensitive information as defined in DoD Directive 8500.01E , to include any unclassified information not cleared for public release
Public	Systems processing publicly releasable information as defined in DoD Directive 8500.01E (i.e., information that has undergone a security review and been cleared for public release)

7.5.7.2. Baseline Information Assurance (IA) Controls

The specific set of baseline IA controls that the PM should address is formed by combining the appropriate lists of Mission Assurance Category (MAC) and Confidentiality Level controls specified in the DoD Instruction 8500.2. Table 7.5.7.2.T1 illustrates the possible combinations.

Table 7.5.7.2.T1. Possible Combinations of Mission Assurance Category and Confidentiality Level

Combination	Mission Assurance Category	Confidentiality Level	DoDI 8500.2 Enclosure 4 Attachments
1	**MAC 1**	**Classified**	**1 and 4**
2	**MAC 1**	**Sensitive**	**1 and 5**
3	**MAC 1**	**Public**	**1 and 6**
4	**MAC 2**	**Classified**	**2 and 4**
5	**MAC 2**	**Sensitive**	**2 and 5**
6	**MAC 2**	**Public**	**2 and 6**
7	**MAC 3**	**Classified**	**3 and 4**
8	**MAC 3**	**Sensitive**	**3 and 5**

9	MAC 3	Public	3 and 6

There are a total of 157 individual IA Controls from which the baseline sets are formed. Each IA Control describes an objective IA condition achieved through the application of specific safeguards, or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the objective condition for every IA Control are assignable, and thus accountable. The IA Controls specifically address availability, integrity, and confidentiality requirements, but also take into consideration the requirements for non-repudiation and authentication.

It is important to exercise due diligence in establishing the MAC level of an information system. The baseline set of IA controls for availability and integrity are purposefully graded to become increasingly stringent for the higher MAC levels. The required resource costs to achieve compliance with the baseline IA controls at the higher MAC levels can be very significant as befits information and information systems on which a warfighter's mission readiness or operational success depends. The IA controls also become increasingly stringent or robust at the higher Confidentiality levels.

7.5.7.3. Information Assurance (IA) Requirements Beyond Baseline IA Controls

There are several additional sources of IA requirements beyond the Baseline IA Controls.

A system being acquired may have specific IA requirements levied upon it through its controlling capabilities document (i.e., Capstone Requirements Document, Initial Capabilities Document, Capability Development Document, or Capability Production Document). These IA requirements may be specified as performance parameters with both objective and threshold values.

All IA requirements, regardless of source, are compiled in the system's DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (similar to the system Requirements Traceability Matrix used in the DoD Information Technology Security Certification and Accreditation Process, superseded by the DIACAP). The DIACAP Implementation Plan documents all IA controls and requirements assigned, whether implemented or "inherited," and for each displays the implementation status, resources required, and the estimated completion date.

7.5.7.4. Security Pre-Configuration of Global Information Grid (GIG) Information Technology (IT) Components

To prevent exposing the GIG to avoidable vulnerabilities, all IT components (both hardware and software), for which security guidelines and enhanced configuration management processes have been developed, should be pre-configured before their connection to the GIG (i.e. integrated/connected to a DoD AIS, enclave/network, or platform IT).

The Department regularly publishes security configuration guidelines enabling IT components to deliver the highest level of inherent security. These guidelines can be obtained from the following sites: Security Technical Implementation Guides from the Defense Information Systems Agency, and Security Configuration Guides from the National Security Agency.

The pre-configuration of GIG IT components to the appropriate security configuration guideline by the vendor should be made a preference in selecting components for procurement. To implement this, solicitations should specify the relevant guideline, and evaluation factors for award should include pre-configuration as a factor. Requiring activities should coordinate with their supporting contracting office to determine the appropriate weight for this factor. Note that this is preference, not a mandatory requirement.

Regardless of whether GIG IT components are procured and delivered in a pre-configured state, system managers and IA managers are responsible for ensuring that IT components (both hardware and software), for which security guidelines have been developed, are appropriately configured prior to their installation/connection to the GIG.

7.5.8. Information Assurance (IA) Testing

See Section 9.7.6, Information Assurance Testing.

7.5.9. Acquisition Information Assurance (IA) Strategy

The primary purpose of the Acquisition IA Strategy is to ensure compliance with the statutory requirements of Title 40/Clinger-Cohen Act and related legislation, as implemented by DoD Instruction 5000.02. As stated in Table 8, Enclosure 5, of that instruction, the Acquisition IA Strategy provides documentation that "Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards." The PM develops the Acquisition IA Strategy to help the program office organize and coordinate its approach to identifying and satisfying IA requirements consistent with DoD policies, standards, and architectures.

The Acquisition IA Strategy serves a purpose separate from the documentation

generated from the DIACAP or other Certification and Accreditation (C&A) processes. Developed earlier in the acquisition life cycle and written at a higher level, the Acquisition IA Strategy documents the program's overall IA requirements and approach, including the determination of the appropriate certification and accreditation process. The Acquisition IA Strategy must be available for review at all Acquisition Milestone Decisions, including early milestones when C&A documentation would not yet be available.

The Acquisition IA Strategy lays the groundwork for a successful C&A process by facilitating consensus among the PM, Component CIO, and DoD CIO on pivotal issues such as Mission Assurance Category, Confidentiality Level, and applicable Baseline IA Controls; selection of the appropriate C&A process; identification of the Designated Accrediting Authority and Certification Authority; and documenting a rough timeline for the C&A process.

7.5.9.1. Development

Click here for **Acquisition IA Strategy Instructions**.

Click here for a sample **Acquisition IA Strategy Template** that can be tailored as appropriate.

7.5.9.2. Review Requirements

Acquisition IA Strategies must be submitted for approval and review in accordance with Table 7.5.9.2.T1, which is based on submission requirements detailed in DoD Instruction 5000.02, Enclosures 4 and 5. Sufficient time should be allowed for Acquisition IA Strategy preparation or update, DoD Component CIO review and approval, and DoD CIO review prior to applicable milestone decisions, program review decisions, or contract awards.

Table 7.5.9.2.T1. IA Strategy Approval and Review Requirements

Acquisition Category *	Events requiring prior Review	Acquisition IA Strategy Approval	Acquisition IA Strategy Review
ACAT IAM, IAC, and ID; and (if MAIS) ACAT IC	Milestone A, B, C, full rate production decision and acquisition contract award	Component CIO	DoD CIO
All other acquisitions	Milestone A, B, C, full rate production decision and acquisition contract award	Component CIO or Designee	Delegated to Component CIO

*Acquisition Category (ACAT) descriptions are provided in DoD Instruction 5000.02, Table 1

Click here to view the **Acquisition IA Strategy Development, Review and Approval Process** MS PowerPoint briefing that contains information on Acquisition IA Strategy key success factors, key stakeholders, critical content criteria, and the review and approval process.

7.5.9.3. Additional Information

Questions or recommendations concerning the Acquisition IA Strategy or its preparation or the Acquisition IA strategy template should be directed to the Defense-wide Information Assurance Program Office (DoD CIO-DIAP) at diap.acquisition@osd.mil.

7.5.10. Information Assurance (IA) Certification and Accreditation (C&A)

7.5.11. Software Security Considerations

7.5.10. Information Assurance (IA) Certification and Accreditation (C&A)

In accordance with DoD Directive 8500.01E, all acquisitions of AISs (to include MAISs), outsourced IT-based processes, and platforms or weapon systems with connections to the GIG must be certified and accredited. The primary methodology for certifying and accrediting DoD information systems is the DoD Information Assurance Certification and Accreditation Process (DIACAP) of DoD Instruction 8510.01.

7.5.11. Software Security Considerations

For the acquisition of software-intensive IT, especially IT used in National Security Systems, PMs should consider the significant operational threat posed by the intentional or inadvertent insertion of malicious code. The risks associated with these supply chain risk management (SCRM) issues are being managed within the context of program protection planning. See Chapter 13, Program Protection Planning, regarding requirements for SCRM key practices and intelligence support from Defense Intelligence Agency SCRM Treat Assessment Center (TAC).

7.5.12. Implementing Information Assurance (IA) in the Acquisition of Information Technology (IT) Services

7.5.12.1. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Acquisition Strategies or Acquisition Plans

7.5.12.2. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Requests for Proposals (RFPs)

7.5.12.3. Acquisition of Information Technology (IT) Services Information

Assurance (IA) Considerations for Source Selection Procedures

7.5.12.4. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Ordering Guides

7.5.12.5. Acquisition of Information Technology (IT) Services Information Assurance (IA) Review and Notification Process

7.5.12. Implementing Information Assurance (IA) in the Acquisition of Information Technology (IT) Services

DoD Instruction 5000.02, Enclosure 9, provides specific policy requirements for "Acquisitions of Services." Enclosure 9 defines IT Services as "The performance of any work related to IT and the operation of IT, including National Security Systems. This includes outsourced IT-based business processes, outsourced IT, and outsourced information functions."

Every year the Department acquires a vast array of IT services from the commercial sector, valued in the billions of dollars. These services support, impact, or utilize DoD information systems and networks both on and off the GIG. Because of this broad scope it is essential that IA be carefully considered as a factor in the planning, procurement, and execution of these services.

All acquisitions of IT services, regardless of acquisition of services category, are subject to Title 40/Clinger-Cohen Act, and to the maximum extent practicable, the Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement.

Additionally, in accordance with DoD Directive 8500.01E, IA requirements shall be identified and included in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems. This section describes the actions to be taken to ensure that IA requirements are met, and IA is appropriately addressed in acquisitions of IT services.

IA considerations are described for the following "Acquisitions of IT Services" areas:

- Acquisition Strategies or Acquisition Plans
- Requests for Proposals (RFPs)
- Source Selection Procedures
- Ordering Guides
- Review and Notification Process

Throughout this section, the services of an "IA professional" are recommended for the development and review of IA elements within acquisition strategies, plans, and procurement documentation. In selecting the appropriate IA professional support, ensure that the individual's IA knowledge and experience are appropriate to the task. Table 7.5.12.T1 suggests appropriate IA workforce categories and levels from the DoD

Manual 8570.01-M, "Information Assurance Workforce Improvement Program Manual," for commonly required tasks. See the manual for details of knowledge, experience, and professional certifications required for each category and level.

Table 7.5.12.T1. Suggested IA workforce categories and levels

Task	Suggested DoD 8570.01M Category and Level
Identify IA technical requirements	IA Technical Level II or III depending on scope and complexity
Identify IA policy and procedural requirements	IA Management Level II
Draft IA section of Acquisition Strategy/Plan	IA Management Level II
Draft IA elements of RFP (including SOW/SOO, Section H clause tailoring, CDRL	IA Management Level II
Draft IA section of ordering guide	IA Management Level II
Develop IA Selection Criteria; participate in SSEB (review offerors' proposals)	IA Technical Level III
Review Acquisition documents, RFP, ordering guide	IA Management Level III

7.5.12.1. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Acquisition Strategies or Acquisition Plans

The treatment of IA in an acquisition strategy, and/or acquisition plan, for an acquisition of IT services is different than the considerations normally addressed in a classic system acquisition strategy. In the case of a system acquisition, the focus is to ensure IA is implemented in the design, development, test, and production of the system. In the case of an acquisition of IT services, the IA considerations are dependent on the specific nature of the services being acquired.

The scope of potential IT services, and the associated IA considerations, is extremely diverse. Examples of IT services include, but are not limited to:

- On-site hardware maintenance
- Lease of telecommunications lines (fiber or circuits)
- Software development
- Test and evaluation services
- Certification and accreditation support
- Help desk support
- Computing infrastructure operational support

- Network operations and Computer Security support

Note that in some large indefinite delivery/indefinite quantity (IDIQ) IT services contracts, the actual tasks to be performed are not established until an order is placed, and there may be thousands of individual orders placed by hundreds of different ordering activities. In order to properly inform the acquisition planning process, the acquisition strategy needs to identify the IA requirements that are relevant to the IT services being acquired, and describe how the acquisition is being conducted to ensure those requirements will be met. As noted above, the scope of these considerations will vary with the nature of the IT services, but the following list provides a good baseline:

- What broad IA policies and guidance are applicable?
- What IA protections are relevant to the services being acquired?
- Are there any IT components or systems being delivered coincidental to the IT services?
- Is there an IA professional supporting the acquisition team? Has an IA professional contributed to the development of the solicitation?
- Does the solicitation clearly and unambiguously communicate IA requirements to prospective offerors?
- Does the performance work statement, specification, or statement of objectives meet IA requirements as specified in DFARS Subpart 239.71, "Security and Privacy for Computer Systems," paragraph 239.7102-1(a)?
- Is the satisfaction of IA requirements a factor for award? Will an IA professional provide subject matter expert support to the source selection process?
- If an IDIQ contract is considered, what IA requirements are allocated to the basic contract as global requirements, and what IA requirements are allocated to the order level (and the responsibility of the ordering activity to invoke)? Does the ordering guide clearly communicate to requiring activities and the ordering offices their responsibilities with regards to IA?
- Has the solicitation been reviewed by the appropriate level of IA oversight (Designated Accrediting Authority/Program Executive Officer/Systems Command/Major Command/Component Senior Information Assurance Officer)?
- Will the services contractor have access to or control of Government data?
- Will the contractor need to connect to DoD systems or networks?
- Will the contractor need to certify and accredit his information system?
- Will the contractor's personnel be performing roles that require IA training, IA professional certifications, or background investigations in order to comply with DoD IA policy requirements?

7.5.12.2. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Requests for Proposals (RFPs)

As with the acquisition strategy, the IA language in the RFP is driven by the characteristics of the IT services requirement. However, regardless of the specifics of the acquisition, the goal of the RFP is to clearly and unambiguously communicate to potential offerors what our IA requirements are, and what we expect from them in terms

of compliance and performance.

Identification of IA Policy Requirements . In most cases the IT services contractor will have to comply with fundamental DoD IA policy, such as DoD Directive 8500.01E and DoD Instruction 8500.2, and CJCS Instruction 6510.01. It is best to identify in the RFP that compliance with these documents is required. For requirements beyond the fundamentals, the nature of the service becomes the driver. If contractor personnel will have IA roles or privileged system access, the requirements of DoD Directive 8570.01 will apply. If the service involves certification and accreditation support, the DoD Information Assurance Certification and Accreditation Process (DIACAP) of DoD Instruction 8510.01 should be cited. Because it would be impractical to identify all the possible permutations of IT services and IA policy in this guidebook, requiring activities should utilize an IA professional to identify all IA requirements relevant to the IT service.

Click here for the Sample RFP IA Clause contract language that can be tailored as appropriate, and included in Section H (Special Contract Requirements) of the solicitation.

Performance Work Statement (PWS) or Statement of Objective (SOO). It is in this section that specific IA requirements, functions and tasks should be communicated to the offerors. This may include identification of IA roles to be performed, specific IA controls to be satisfied, specific IA performance criteria (e.g., availability requirements). This section must clearly communicate what needs to be done with regards to IA.

Contract Data Requirements List (CDRL). In this section, identify any IA-related data products that the potential contractor must produce. This may include reports, IA artifacts, or other IA documentation.

Section M: Evaluation Factors for Award. This section contains the evaluation factors and significant subfactors by which offers will be evaluated and the relative importance that the Government places on these evaluation factors and sub-factors. See section 7.5.12.3 for additional guidance.

IA Performance. In situations where IA performance is critical, the RFP may specifically address the impact of non-compliance or lack of IA performance on the part of the contractor. These impacts may include actions such as: documentation of poor performance, rejection of work products/deliverables, denial of network or physical access to non-conforming personnel, reduction of award fees, assessment of liquidated damages, termination of the contract for the convenience of the government, and termination of the contract for default. If IA is a critical element of the service, engage with the Procurement Contracting Officer as early as possible to define these impacts, and to include the appropriate language in the solicitation and resulting contract. The IA professional, PM, and program lead for test and evaluation will identify IA test and evaluation requirements, metrics, success criteria, and how and when best to conduct the IA testing.

7.5.12.3. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Source Selection Procedures

Section M of the Uniform Contract format contains the Evaluation Factors for Award. This section contains the evaluation factors and significant sub-factors by which offers will be evaluated and the relative importance that the Government places on these evaluation factors and sub-factors. IA is just one of numerous factors that may be assessed for the purposes of making a contract award decision. It may be a major contributing factor in a best value determination, or it may be a minimum qualification for an award based primarily on cost or price.

The extent to which IA considerations impact the award factors is a direct function of the clear communication and understanding of the potential loss or damage that an IA failure could subject to a system, organization or mission capability. For this reason, an IA professional should be tasked to assess the IA requirement and risks, and to advise the contracting officer accordingly. As appropriate, an IA professional should develop IA related evaluation factors, and participate in the negotiation of relative weightings of these factors. Correspondingly, an IA professional should also be part of the source selection evaluation board to ensure that the IA aspects of offerors' proposals are assessed for technical and functional appropriateness, adequacy, and compliance with requirements.

7.5.12.4. Acquisition of Information Technology (IT) Services Information Assurance (IA) Considerations for Ordering Guides

In many large IT services contracts, the initial contract award merely establishes the scope of work, pricing, and other global factors, but no specific work is done until separate task orders are established. For these indefinite delivery-indefinite quantity (IDIQ) contracts, the IA considerations can vary widely from order to order. Additionally, orders may be originated from activities separate from the activity that awarded the basic IDIQ contract, even from other agencies. To ensure that IA is appropriately considered in these individual and potentially unique orders, the "ordering guide" for the contract should inform the ordering activities of their responsibilities with regards to IA. Specifically, ordering/requiring activities are responsible to ensure that any order placed for IT services will result in a commitment from the service provider to deliver services that comply with DoD IA policies. To do this, the ordering activity must be aware of what general IA requirements are invoked in the basic contract, and then ensure that individual orders provide specific details, and any supplemental IA requirements that may be needed to achieve policy requirements. For example, the basic contract may invoke DoD Instruction 8500.2 and require "implementation of appropriate baseline IA controls", but the individual order would have to specify the Mission Assurance Category (MAC) and Confidentiality Level relevant to that order.

Finally, since IT services acquisitions must comply with the Title 40/Clinger-Cohen Act which requires a level of assurance that IA compliance is being achieved, it may be appropriate to direct that a hierarchy of IA review and approvals be established based

on factors such as dollar value of the individual orders. This will ensure that qualifying orders are reviewed at an oversight level commensurate with their value.

Click here for the Sample IA Section of an Ordering Guide. The specific form, structure and content should be driven by the needs of the acquisition, and the example is provided merely to offer a point of departure, and may not be appropriate for a specific acquisition.

7.5.12.5. Acquisition of Information Technology (IT) Services Information Assurance (IA) Review and Notification Process

Paragraph 5 of Enclosure 9 of DoD Directive 5000.02 includes specific requirements for higher-level review and approval of proposed acquisitions of services. The following IA reviews are required to be conducted in support of the Decision Authority approval process:

- For acquisitions of IT Services estimated at greater than $250M (basic plus all options)
    - DoD Component IA Review of Acquisition Strategy/Acquisition Plan/Request for Proposal (RFP)
- For acquisitions of IT Services estimated at greater than $500M (basic plus all options)
    - DoD Component IA Review of Acquisition Strategy/Acquisition Plan/RFP, and
    - DoD CIO IA ** Review of Acquisition Strategy/Acquisition Plan/RFP, and
    - Notification of cognizant Mission Area Portfolio Manager by ther DoD CIO Acquisition prior to RFP release.

For acquisitions of IT services below the $250M threshold, follow Component guidance. For acquisition of IT services related to telecommunications or transport infrastructure, recommend review for IA technical sufficiency by Defense IA/Security Accreditation Working Group (DSAWG) representative.

** Contact the Defense-wide Information Assurance Program (DIAP) Acquisition Team at diap.acquisition@osd.mil to arrange for early coordination reviews and formal reviews.

7.5.13. Information Assurance (IA) Definitions

7.5.13. Information Assurance (IA) Definitions

For IA-related definitions, refer to Enclosure 2 of DoD Directive 8500.01E and Enclosure 2 of DoD Instruction 8500.2. All other definitions are defined in CNSSI 4009.

7.6. Electromagnetic Spectrum

7.6.1. EM Spectrum Considerations

7.6.1. EM Spectrum Considerations

In accordance with DoDI 5000.02, Enclosure 12, paragraph 11, the Program Manager (PM) must consider the use of the EM SPECTRUM when delivering capability to the warfighter's or business domains. The fundamental questions are:

- Will the system/equipment require access to the EM SPECTRUM to operate as it is intended (e.g., to communicate with other systems; to collect and/or transmit data, to broadcast signals, etc.)?
- Will sufficient EM SPECTRUM access be available to operate the system/equipment during its life cycle in the intended operational environment?
- Will the system/equipment, including commercial-off-the-shelf systems delivered by the program, radiate EM energy that could be detrimental to other systems or equipment?
- Will the intended operational EM environment produce harmful effects to the intended system, even if the proposed system does not radiate EM energy (such as ordnance)?

Ensuring the compatible operation of DoD systems in peace and in times of conflict is becoming increasingly complex and difficult. DoD's demand for spectrum access is increasing as more systems become net-centric and information is pushed to the "tactical edge". In addition, the EM environment in which the DoD operates around the globe is becoming more congested as consumer applications that require spectrum are introduced and take hold. System developers can no longer assume their systems will be operating in an interference-free frequency band or that a single band will work around the world. Given these circumstances, DoD Instruction 4650.01 states the following as one of spectrum management's core principles: "Pursue spectrum-efficient technologies to support the increasing warfighter demand for spectrum access and encourage development of spectrum-dependent systems that can operate in diverse EM environments."

National and DoD policies and procedures for the management and use of the EM Spectrum direct PMs developing spectrum-dependent systems/equipment to consider EM SPECTRUM requirements and Electromagnetic Environmental Effects (E3) control early in the development process. Given the complex environment (both physical and political) in which DoD forces operate, and the potential for worldwide use of capabilities procured for DoD, early and thorough consideration is vitally important. These policies and procedures are intended to ensure the following:

- Permission is obtained from designated authorities of sovereign ("host") nations

(including the United States) to use the equipment within their respective borders and near the geographic borders of other countries (within coordination zones);
- Sufficient spectrum will be available in the operational environment during the system/equipment's life cycle; and

- Equipment can operate compatibly with other spectrum-dependent equipment already in the intended operational environment (electromagnetic compatibility (EMC)).

Because this requires coordination at the national and international levels, getting spectrum advice early helps a PM identify and mitigate spectrum-related risks and successfully deliver capabilities that can be employed in their intended operational environment.

E3 control is concerned with proper design and engineering to minimize the impact of the EM environment on equipment, systems, and platforms. E3 control applies to the EM SPECTRUM interactions of both spectrum-dependent and non- spectrum-dependent objects within the operational environment. Examples of non- spectrum-dependent objects that could be affected by the EM environment include all other electrical/electronic systems, ordnance, personnel, and fuels. The increased dependency on, and competition for, portions of the EM Spectrum have increased the likelihood of adverse interactions among sensors, networks, communications, weapons systems, fuels, personnel, and ordnance.

DoD has established procedures, described below, to identify and mitigate spectrum-related risks and to control the E3 impacts on the equipment, systems, and platforms used by our military forces. Spectrum requirements shall be addressed early in acquisition programs (DoD Instruction 4650.01). In accordance with DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," proper design and engineering techniques to control E3 shall be considered throughout the acquisition process to ensure the successful delivery of operational capabilities to the warfighter.

7.6.2. Mandatory Policies

7.6.2.1. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

7.6.2.2. Title 47, Code of Federal Regulations (CFR), Chapter III, Part 300.1

7.6.2.3. Office of Management and Budget (OMB) Circular A-11, Section 31.12

7.6.2.4. DoD Instruction 4650.01, "Policy and Procedures for the Management and Use of the Electromagnetic Spectrum"

7.6.2.5. DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program"

7.6.2.1. DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

DoD Instruction 5000.02, dated December 8, 2008, references other spectrum-related policies and restates some of the acquisition-related requirements. However, it was published prior to implementation of DoD Instruction 4650.01 and it needs to be revised. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

The current Instruction states:

- For all EM spectrum-dependent systems, PMs must comply with U.S. and host nation spectrum regulations. They shall submit written determinations to the DoD Component Chief Information Officer (CIO) or equivalent that the EM SPECTRUM necessary to support the operation of the system during its expected life cycle is, or will be, available. These determinations shall be the basis for recommendations provided to the Milestone Decision Authority (MDA) at the milestones defined in Table 3 in Enclosure 4 of DoD Instruction 5000.02.

- Tables 2-1 and 2-2 in Enclosure 4 state the statutory requirement for all developers of systems/equipment that use the EM SPECTRUM in the U.S. and its possessions to submit a DD Form 1494 "Application for Equipment Frequency Allocation" and get Certification of Spectrum Support from the National Telecommunications and Information Administration (NTIA).

See Section 7.6.3 for requirements at each acquisition milestone.

7.6.2.2. Title 47, Code of Federal Regulations (CFR), Chapter III, Part 300.1

This regulation requires compliance with the National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management", and applies to all Federal Agencies that use the electromagnetic spectrum within the United States and its possessions.

7.6.2.3. Office of Management and Budget (OMB) Circular A-11, Section 31.12

This publication contains the requirement to obtain certification by the National Telecommunications and Information Administration (NTIA) that the radio frequency required can be made available before estimates are submitted for the development or procurement of major radio spectrum-dependent communications-electronics systems (including all systems employing satellite techniques) within the United States and U.S. possessions. Additionally, it requires that spectrum efficiency and effectiveness be factored into economic analyses of alternatives to the extent practical.

7.6.2.4. DoD Instruction 4650.01, "Policy and Procedures for the Management and Use of the Electromagnetic Spectrum"

This instruction establishes policy and procedures for management and use of the EM spectrum and the supportability of DoD spectrum-dependent systems in the EM spectrum and states:

- The EM SPECTRUM is a critical resource, and access to the spectrum is vital to the support of military operations. Proper management and use of the spectrum available to the DoD shall be an integral part of military planning, research, development, testing, and operations involving spectrum-dependent systems.
- DoD Components shall comply with U.S. and host nation spectrum regulations and obtain applicable authorizations before operating spectrum-dependent systems.
- DoD Components shall obtain U.S. Government certification of spectrum support, as required by the National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management," prior to authorization to operate for experimental testing, developmental testing, or operations of spectrum-dependent systems in the U.S. and its possessions. In addition, many host nations require their own certification before providing authorization to operate.
- For all spectrum-dependent systems, DoD Components shall determine if there will be sufficient spectrum to support operation of the system during its life cycle. In order to affect design and procurement decisions, DoD Components shall:
    - Identify spectrum-related risks as early as possible via Spectrum Supportability Risk Assessments (SSRAs).
    - Review these assessments at acquisition milestones.
    - Manage the risks throughout the system's life cycle.
- To facilitate planning, DoD Components shall ensure current and complete technical performance (parametric) data on spectrum-dependent systems is captured in DoD spectrum management databases.
- In accordance with NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management," DoD Components shall consider sharing the spectrum with other Federal agencies and with commercial spectrum users. Sharing of spectrum shall be accomplished:
    - Without degradation to the DoD mission.
    - In a manner that provides current and future DoD users with sufficient regulatory protection.
    - With minimal risk that such sharing will result in loss of access to the spectrum necessary to perform the DoD mission.

In addition, DoD Instruction 4650.01 states that spectrum policy and spectrum management functions shall be guided by the following core principles:

- Ensure the U.S. warfighter has sufficient EM spectrum access to support military capabilities.
- Support a U.S. EM spectrum policy that balances national and economic security, with national security as the first priority.
- Use the EM spectrum as efficiently and effectively as practical to provide the

greatest overall benefit to warfighting capability.
- Pursue spectrum-efficient technologies to support the increasing warfighter demand for EM spectrum access.
- Encourage development of spectrum-dependent systems that can operate in diverse EM environments.
- Actively support U.S. policies and interests in international EM spectrum bodies and in international negotiations for spectrum allocation and access.

7.6.2.5. DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program"

This directive establishes policy and responsibilities for the management and implementation of the DoD E3 Program. This program facilitates mutual EM compatibility and effective E3 control among land, air, sea, and space-based electronic and electrical systems, subsystems, and equipment, and the existing natural and man-made environments.

It states DoD policy that all electrical and electronic systems, subsystems, and equipment, including ordnance containing electrically initiated devices, shall be mutually compatible in their intended EM environment without causing or suffering unacceptable mission degradation due to E3.

7.6.3. Spectrum Supportability and E3 in the Acquisition Life Cycle

7.6.3.1. Before Milestone A

7.6.3.2. Before Milestone B (or before the first Milestone that authorizes contract award)

7.6.3.3. Before Milestone C

7.6.3.4. After Milestone C

7.6.3.5. Spectrum Supportability and E3 Control Requirements in the Joint Capabilities Integration and Development System

7.6.3.6. Spectrum and E3 Control Requirements in the Information Support Plan (ISP)

7.6.3.7. Spectrum Supportability and E3 Control Requirements in the Test and Evaluation Master Plan (TEMP)

7.6.3.8. Spectrum and E3 Control Requirements in Performance Specifications

7.6.3.9. Spectrum and E3 Control Requirements in the Statement of Work (SOW)

7.6.3.10. Spectrum and E3 Control Requirements in the Contract Data Requirements List (CDRL)

7.6.3. Spectrum Supportability and E3 in the Acquisition Life Cycle

PMs shall take the following actions to mitigate spectrum-related risks for spectrum-dependent equipment, and minimize the E3 on all military forces, equipment, systems, and platforms (both non- and spectrum-dependent). Consideration of these critical elements throughout the acquisition process will help to ensure successful delivery of capability to the warfighter.

The PM shall include the funding to cover Spectrum Supportability Risk Assessments (SSRAs), required certification processes, and control of E3 as part of the overall program budget. Section 7.6.4.1 addresses SSRAs; Section 7.6.4.4 addresses E3.

7.6.3.1. Before Milestone A

- Develop initial spectrum supportability and E3 control requirements for the materiel solutions being considered.
- Perform initial regulatory SSRA to identify and refine spectrum issues. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 1 (Conceptual) Certification of Spectrum Support through the National Telecommunications and Information Administration (NTIA). Contact your sponsoring military department frequency management office (MILDEP FMO) for details on the process. The process can take several months, so start as early as practical. See Section 7.6.4.2 for details.

7.6.3.2. Before Milestone B (or before the first Milestone that authorizes contract award)

- Update the spectrum supportability and E3 control requirements and ensure they are addressed in the Capability Development Document.
- Perform initial technical and initial operational SSRAs to identify spectrum issues. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 2 (Experimental) Certification of Spectrum Support through the NTIA. Contact your sponsoring MILDEP FMO for details on the process. The process can take several months so start as early as practical. See Section 7.6.4.2 for details.
- For systems that will be operated outside the U.S. and its possessions, initial discussions with host nations should be conducted to determine if there may be significant obstacles to obtaining authorization to operate. MILDEP frequency managers in conjunction with the Joint Staff will assist the PM in initiating

discussions with regional combatant command frequency management offices. Discussion should concentrate on host nations where the systems will be permanently deployed.
- Obtain applicable U.S. and/or host nation authorizations before testing spectrum-dependent systems or components.
- Provide initial technical performance data to Defense Information Systems Agency (DISA) via supporting MILDEP FMOs.
- Discuss spectrum and E3 control requirements and any associated issues in the initial ISP.
- Define, in the TEMP, those spectrum-related and E3 control requirements that must be tested during Developmental Test and Evaluation and Operational Test and Evaluation. TEMPs shall include, within the scope of critical operational issues and sub-issues, the requirement to demonstrate the effective E3 control of systems, subsystems, and equipment.
- Address SSRA, certification of spectrum support, and E3 control requirements in the Government's Statement of Work, Performance Specifications, and contract data requirements to be provided to the contractor.

7.6.3.3. Before Milestone C

- Update the spectrum and E3 control requirements and ensure they are addressed in the Capability Production Document.
- Perform a detailed regulatory and a detailed technical SSRA to ensure all issues have been identified and are being mitigated. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 3 (Developmental) Certification of Spectrum Support through the NTIA. Contact your sponsoring MILDEP FMO for details on the process. The process can take several months so start as early as practical. See Section 7.6.4.2 for details.
- For systems that will be operated overseas, more detailed discussions with host nations may be required to resolve any significant obstacles to obtaining authorization to operate. MILDEP frequency managers in conjunction with the Joint Staff will assist the PM in initiating discussions with regional combatant command frequency management offices. Discussion should concentrate on host nations where the systems will be permanently deployed.
- Obtain applicable U.S. and/or host nation authorizations before testing spectrum-dependent systems or components.
- Provide updated technical performance data to DISA via supporting MILDEP FMOs.
- Refine the discussion of spectrum and E3 control requirements and any associated issues in the ISP for record.
- Refine discussion of spectrum-related and E3 control requirements to be tested in the revised TEMP.
- Address SSRA, certification of spectrum support, and E3 control requirements in the Government's Statement of Work, Performance Specifications, and contract

data requirements to be provided to the contractor.

7.6.3.4. After Milestone C

- Update regulatory, technical, and operational SSRAs as needed prior to requesting authorization to operate for other than testing. See Section 7.6.4.1 for details.
- For systems that will be operated in the U.S. and its possessions, complete a Stage 4 (Operational) Certification of Spectrum Support through the NTIA prior to requesting authorization to operate for other than testing. The process can take several months so start as early as possible. See Section 7.6.4.2 for details.
- Obtain applicable U.S. and/or host nation authorizations before testing or operating spectrum-dependent systems or components.
- Changes to operational parameters (e.g., tuning range, bandwidth, emission characteristics, antenna gain and/or height, or output power, etc.) or proposed operational locations will likely require additional spectrum certification actions or require additional E3 analysis or tests.

- Continue to provide updated technical performance data to DISA via supporting military department frequency management offices.

7.6.3.5. Spectrum Supportability and E3 Control Requirements in the Joint Capabilities Integration and Development System

The JCIDS Manual and CJCS Instruction 6212.01 reference other spectrum-related policies and restate some of the requirements. However, CJCSI 6212.01 was published prior to implementation of DoD Instruction 4650.01 and needs revision. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

CJCSM 3170.01 requires the Capability Development Document and Capability Production Document to address spectrum supportability and E3 control. It also requires spectrum requirements be included in the Net Ready Key Performance Parameter (NR KPP).

CJCSI 6212.01 includes spectrum and E3 requirements in the NR KPP under the heading of Supportability Requirements.

Per CJCSI 6212.01, the Joint Staff will use the following assessment criteria when reviewing documents for interoperability:

- If applicable, does the document identify a requirement for spectrum supportability?
- If applicable, does the document address E3?

- If applicable, does the document address host nation approval?
- If applicable, has a DD Form 1494 been submitted to the military department Frequency Management Office?
- Does the document include a spectrum supportability compliance statement or outline a plan to obtain spectrum supportability?
- Does the document address spectrum supportability as a separate requirement in a paragraph?

- Does the document reference the Spectrum Supportability Risk Assessment (SSRA)?

Sample Language. The sample statements shown below should be included, as applicable, as THRESHOLD requirements. The first is used to denote compliance with applicable DoD, national, and international spectrum policies and regulations. The second is used to require compatible operation and includes an additional statement for ordnance safety.

Spectrum. *The XXX System will comply with the applicable DoD, National, and International spectrum management policies and regulations. Required performance data will be submitted to the supporting MILDEP Frequency Management Office. (Threshold)*

Electromagnetic Environmental Effects (E3). *The XXX System shall be mutually compatible and operate compatibly in the EM Environment. It shall not be operationally degraded or fail due to exposure to electromagnetic environmental effects, including high intensity radio frequency (HIRF) transmissions or high-altitude electromagnetic pulse (HEMP). All ordnance items shall be integrated into the system in such a manner as to preclude all safety problems and performance degradation when exposed to its operational EM Environment (HERO). (Threshold)*

7.6.3.6. Spectrum Supportability and E3 Control Requirements in the Information Support Plan (ISP)

DoD Instruction 4630.8 references other spectrum-related policies and restates some of the requirements. However, it was published prior to implementation of DoD Instruction 4650.01 and it needs revision. In cases of conflicting policy, DoD Instruction 4650.01 takes precedence for spectrum-related requirements.

According to DoD Instruction 4630.8, the ISP must "discuss RF spectrum needs" in Chapter 2 (see details in Section 7.3.6.7.2). Spectrum-related and E3 control issues shall be described in the ISP Chapter 3 (see details in Section 7.3.6.7.3).

7.6.3.7. Spectrum Supportability and E3 Control Requirements in the Test and Evaluation Master Plan (TEMP)

Within the TEMP, the critical operational issues for suitability or survivability are usually

appropriate to address spectrum supportability and E3 control requirements. The overall goals of the test program with respect to spectrum supportability and E3 control requirements are to ensure that appropriate evaluations are conducted during developmental test and evaluation, and that appropriate assessments are performed during operational test and evaluation. See Section 9.5.5 for details.

Sample Language. The following are four examples of critical operational issues statements in the TEMP:

- Will the platform/system (or subsystem/equipment) detect the threat in a combat environment at adequate range to allow a successful mission? (**Note:** In this example, the "combat environment" includes the operational EM environment.)
- Will the system be safe to operate in a combat environment? (**Note:** In this example, EM radiation hazards issues such as hazards of EM radiation to personnel, ordnance, and volatile materials and fuels can be addressed, as applicable.)
- Can the platform/system (or subsystem/equipment) accomplish its critical missions? (**Note:** This example determines if the item can function properly without degradation to or from other items in the EM environment.)
- Is the platform/system (or subsystem/equipment) ready for Joint and, if applicable, Combined operations? (**Note:** In this example, the item must be evaluated in the projected Joint and, if applicable, combined operational EM environments.)

7.6.3.8. Spectrum Supportability and E3 Control Requirements in Performance Specifications

Military Standards (MIL-STD) 461 and 464 and Military (MIL-HDBK) 237 provide crucial guidance that, if followed, should preclude E3 problems with the critical systems provided to the warfighter. (**Note:** MIL-HDBK 237D does not reflect new requirements in DoD Instruction 4650.01, published in January 09, and needs to be revised. DoD Instruction 4650.01 takes precedence.)

Performance specifications should invoke spectrum-related and E3 control requirements. MIL-STD-461, which defines E3 control (emission and susceptibility) requirements for equipment and subsystems, and MIL-STD-464, which defines E3 control requirements for airborne, sea, space, and land platforms/systems, including associated ordnance, can be used as references. Ordnance includes weapons, rockets, explosives, electrically initiated devices, electro-explosive devices, squibs, flares, igniters, explosive bolts, electric primed cartridges, destructive devices, and jet-assisted take-off bottles.

Sample Language. The following examples address E3 control in subsystem/equipment performance specifications:

Electromagnetic Interference (EMI) Control. *The equipment shall comply with the*

applicable requirements of MIL-STD-461.

Electromagnetic Interference (EMI) Test. *The equipment shall be tested in accordance with the applicable test procedures of MIL-STD-461.*

As an alternative, the program manger can tailor E3 control requirements from MIL-STD-461 or MIL-STD-464. Both MIL-STD-461 and MIL-STD-464 are interface standards. See Section 9.5.2 for testing standards and guidance from Director, Operational Test & Evaluation and from Development Test and Evaluation. See the DoD ASSIST homepage for additional information on Military specs and standards.

7.6.3.9. Spectrum Supportability and E3 Control Requirements in the Statement of Work (SOW)

The following is an example SOW statement to address spectrum and E3 control requirements:

The contractor shall design, develop, integrate, and qualify the system such that it meets its Operational Performance Requirements and the applicable spectrum supportability and E3 control requirements in the system specification. The contractor shall perform analyses, studies, and testing to ensure the system is designed to comply with the applicable DoD, National, and International spectrum management and E3 control policies and regulations. The contractor shall perform inspections, analyses, and tests, as necessary, to verify that the system complies with the applicable DoD, National, and International spectrum management and E3 control policies and regulations. The contractor shall prepare and update spectrum-dependent system technical performance data throughout the development of the system and shall perform sufficient analysis and testing to characterize the equipment, where necessary. The contractor shall establish and support spectrum and E3 control requirements Working-level Integrated Product Team (WIPT) to accomplish these tasks.

7.6.3.10. Spectrum Supportability and E3 Control Requirements in the Contract Data Requirements List (CDRL)

The following are examples of data item requirements typically called out for spectrum supportability and E3 control requirements in the CDRL:

- DI-EMCS-80199C EMI [Electromagnetic Interference] Control Procedures
- DI-EMCS-80201C EMI Test Procedures
- DI-EMCS-80200C EMI Test Report
- DI-EMCS-81540A E3 Integration and Analysis Report
- DI-EMCS-81541A E3 Verification Procedures

- DI-EMCS-81542B E3 Verification Report
- DI-MISC-81174 Frequency Allocation Data

Additional information can be found at:

- Spectrum & E3 Compliance
- E3 and Spectrum Acquisition Requirements & Verification

7.6.4. Spectrum Supportability Risk Assessments (SSRAs), Certification of Spectrum Support, Authorizations to Operate, and Electromagnetic Environmental Effects (E3) Control Summaries

7.6.4.1. Spectrum Supportability Risk Assessments (SSRAs)

Spectrum-dependent system developers shall identify and mitigate regulatory, technical, and operational spectrum supportability risks using suggested tasks in Table 7.6.4.1.T1. DoD Components' spectrum-dependent system developers shall increase the detail of these risk assessments as the S-D systems design matures.

Spectrum-dependent system developers shall assess the risk for harmful interference with other spectrum-dependent systems and/or harmful radiation-related effects. At a minimum, electromagnetic interference (EMI) and electromagnetic compatibility (EMC) assessments shall be made.

Spectrum-dependent system developers shall manage spectrum supportability risks with other developmental risks through systems engineering processes.

Spectrum-dependent system developers are encouraged to initiate the SSRA in order to help identify regulatory, technical, and operational risks while completing the appropriate stage of certification of spectrum support.

Complex "family of systems" or "system-of-systems" may require more than one SSRA.

Table 7.6.4.1.T1. SSRA Suggested Tasks (from DoDI 4650.01)

Regulatory	
Initial Regulatory Spectrum Supportability Risk Assessment (SSRA) Tasks	• Determine countries for likely operational deployment within each Combatant Commander area of responsibility. • Determine the internationally recognized radio service of all spectrum-dependent sub-systems. • Identify portions of the system's tuning range supported by each host nation's (HN's) table of frequency allocation. • Determine the relative regulatory status, for example, co-primary or secondary, assigned to the radio service by the HN's table of frequency allocations. • Obtain international comments on U.S. military systems of the same radio service and with similar technical characteristics submitted for HN spectrum certification (available via the DoD Host-Nation Spectrum Worldwide Database Online). • Identify other U.S. military, U.S. civil, and non-U.S. co-band and adjacent-band and harmonically-related systems likely to be co-site or in close proximity by querying DoD system databases or the appropriate National Telecommunications and Information Administration (NTIA) database. • Identify risks and develop recommendations for mitigation of regulatory issues.

Detailed Regulatory SSRA Tasks	• Address Military Communications-Electronics Board (MCEB), NTIA and other guidance resulting from the certification of spectrum support process. • Consult with the DoD Component spectrum management office regarding changes to U.S. Federal or civil telecommunication regulations impacting the system's frequency bands. • Determine if the system meets appropriate military, U.S. national, and international spectrum standards for radiated bandwidth and transmitter characteristics. • Quantify the impacts of any changes to U.S. Government or international spectrum regulations or technical sharing criteria. • Identify risks and develop recommendations for mitigation of regulatory issues.
Updated Regulatory SSRA Tasks	• Address MCEB, NTIA and other guidance resulting from the certification of spectrum support process. • Consult with the DoD Component spectrum management office regarding changes to U.S. Federal or civil telecommunication regulations impacting the system's frequency bands. • Identify risks and develop recommendations for mitigation of regulatory issues.
Technical	

Initial Technical SSRA Tasks	• Determine candidate technologies and their technical parameters:
	  o Application: fixed, transportable, mobile
	  o Host platform (dismounted soldier, airborne, tactical operations center, etc.)
	  o Frequency range of operation
	  o Required data throughput
	  o Receiver selectivity
	  o Receiver criteria required for desired operation
	  o Required radiated bandwidth
	  o Transmitter power output
	  o Antenna performance characteristics
	  o Anticipated HNs for deployment
	• Perform an initial electromagnetic compatibility (EMC) analysis to identify electromagnetic interactions that require further study. The analysis should use, as a minimum, technical parameters for the candidate system and the technical parameters of spectrum-dependent systems expected to be in the candidate's operational environment.
	• Evaluate the initial system parameters with respect to U.S. and appropriate international spectrum standards; develop plans to address non-compliant systems.
	• Identify risks and develop recommendations for mitigation of technical issues.

Detailed Technical SSRA Tasks	• Evaluate systems performance and effect on other spectrum-dependent system that operates co-frequency or adjacent frequency expected to be found in the intended operational environment. • Determine the acceptable received interference level between the system being analyzed and other spectrum-dependent systems to ensure neither is significantly degraded and that coexistence is feasible. • Use measured performance of the system's receiver, transmitter, antenna, and appropriate propagation models whenever feasible. • Use propagation models developed specifically for mobile communications systems to determine potential link degradation and blockage due to atmospheric conditions or terrain and building obstructions within intended deployments areas. • Consider overall system performance to include link availability with and without interference, while taking into account the effects of the environment (e.g., considering path loss, rain attenuation, humidity, climate, temperature, and water and oxygen absorption). • For non-communications systems (radar, passive sensors, etc.), determine the appropriate operational degradation as a function of the level of received environmental and co-site interference. • Quantify intra-platform EMC among co-sited emitters and receivers for complex "system-of-systems" platforms in terms of the possibility and influence of: o Inter-modulation o Transmitter Harmonic Interference o Transmitter Spurious Output Interference o Transmitter Noise Interference o Receiver Desensitization Interference • Compare the measured system parameters with U.S. national and appropriate

	international spectrum standards. • Generate technical recommendations regarding mitigating potential interference by implementing channelization plans, advanced narrow-beam antennas, (active, spot and contoured-beam, etc.), as well as use of passive radio frequency components (filters, diplexers, couplers, etc.). • Identify risks and develop recommendations for mitigation of technical issues.
Updated Technical SSRA Tasks	• Quantify impact of changes to the operational "signals-in-space" radio frequency parameters to co-site EMC and E3. • Identify risks and develop recommendations for mitigation of technical issues.
Operational	
Initial Operational SSRA Tasks	• Determine the expected complement of spectrum-dependent systems anticipated to be in the systems operating environment. The system should operate without experiencing or causing interference as part of the DoD response to conventional and non-conventional (disaster relief) missions. • Perform a more extensive EMC analysis quantifying the potential interference between the candidate system and the spectrum-dependent systems used by other DoD units in the operational environment. Express the results in operational terms, e.g., the frequency-distance separation requirements between a transmitter and a receiver that must be maintained to achieve compatibility. • Identify risks and develop recommendations for mitigation of technical issues.

Updated Operational SSRA Tasks	• Refine the expected complement of spectrum-dependent systems anticipated to be in the systems operating environments. • Refine the EMC analysis quantifying the mutual interference between the candidate system and the spectrum-dependent systems used by other DoD units in the operational environment. • Identify risks and develop recommendations for mitigation of technical issues.

7.6.4.2. U.S. Government (USG) and Host Nation (HN) Certification of Spectrum Support

7.6.4.2.1. U.S. Government (USG) Certification of Spectrum Support

Certification of spectrum support shall be obtained as required National Telecommunications and Information Administration (NTIA) "Manual of Regulations and Procedures for Federal Radio Frequency Management" prior to authorization to operate for experimental testing (Stage 2), developmental testing (Stage 3), or operations (Stage 4) of spectrum-dependent systems. (See Chapter 10 of NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management" for descriptions of the Stages of Certification.)

PMs shall request certification of spectrum support via the appropriate Service Frequency Management Office using procedures in Chapter 10 of NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management."

Additionally, as required by OMB Circular A-11, Section 31.12 (see section 7.6.2.3), this certification must be completed prior to submission of cost estimates for development or procurement of major spectrum-dependent systems and for all space and satellite systems.

Additional coordination is required for satellite systems per NTIA "Manual of Regulations and Procedures for Federal Radio Frequency Management". Information required for requesting either an exemption from the International Telecommunication Union registration or advanced publication, coordination, and notification of a particular space system must be submitted to the NTIA.

7.6.4.2.2. Host Nation (HN) Certification of Spectrum Support

DoD Components shall request HN certification of spectrum support for spectrum-dependent systems using procedures established in Combatant Commander

agreements with HNs and by the Military Communications-Electronics Board. Requirements for certification vary by HN. PMs should contact their appropriate Service Frequency Management Office for details on process and procedures.

7.6.4.3. Authorization to Operate (Frequency Assignment)

Frequency assignments are issued by designated authorities of sovereign nations, such as telecommunications agencies within foreign countries, and the National Telecommunications and Information Administration (NTIA) for the U.S. and its Possessions. Under certain conditions, other designated authorities, such as DoD Area Frequency Coordinators or Unified and Specified Commanders may grant frequency assignments. Equipment that has not been previously granted some level of certification of spectrum support will not normally receive a frequency assignment. Procedures for obtaining frequency assignments, once the equipment, sub-system, or equipment has become operational, are delineated in regulations issued by the Regional and Functional Commands and/or Military Services.

In most cases, the operational frequency assignments are requested and received as a program is being fielded. However, if the PM has implemented guidance received in response to requests for certification of spectrum support and designed the system as described in the performance data provided, system operators have not historically encountered problems in obtaining operational frequency assignments.

Spectrum congestion, competing systems, and interoperability, all can contribute to encountering some operational limitations, such as geographical restrictions or limitations to transmitted power, antenna height and gain, bandwidth or total number of frequencies made available, etc. Certification to operate in a particular frequency band does not guarantee that the requested frequency(ies) will be available to satisfy the system's operational spectrum requirements over its life cycle.

7.6.4.4. Electromagnetic Environmental Effects (E3) Control (DoD Directive 3222.3)

7.6.4.4.1. Objective for E3 Control

The objective of establishing E3 control requirements in the acquisition process is to ensure that DoD equipment, subsystems, and systems are designed to be self-compatible and operate compatibly in the operational EM environment. To be effective, the PM should establish E3 control requirements early in the acquisition process to ensure compatibility with co-located equipment, subsystems, and equipment, and with the applicable external EM environment.

7.6.4.4.2. Impacts When E3 Control Is Not Considered

It is critical that all electrical and electronic equipment be designed to be fully compatible in the intended operational EM environment. The DoD has experience spectrum-

dependent with items developed without adequately addressing E3 which resulted in poor performance, disrupted communications, reduced radar range, and loss of control of guided weapons. Failure to consider E3 can result in mission failure, damage to high-value assets, and loss of human life. Compounding the problem, there is increased competition for the use of the spectrum by DoD, non-DoD Government, and civilian sector users; and many portions of the EM spectrum are already congested with spectrum-dependent systems. Additionally, new spectrum-dependent platforms/systems and subsystems/equipment are technologically complex, highly sensitive, and often operate at higher power levels. All of these factors underscore the importance of addressing E3 control requirements early in the acquisition process.

7.6.4.5. Additional Resources

Defense Spectrum Organization (DSO) enables information dominance through effective spectrum operations; including EM battlespace planning, deconfliction, and joint spectrum interference resolution. DSO develops and implements spectrum management capabilities to enhance efficiency and effectiveness, and pursues emerging spectrum technologies. DSO advocates for current and future military spectrum requirements in national and international forums to protect DoD global operations.

A valuable source of spectrum and E3 compliance information, including current events, videos and links to related sites is found on the Acquisition Community Connection site at: https://acc.dau.mil/sc.

7.6.5. Definitions

Key terms pertaining to spectrum supportability and electromagnetic compatibility (EMC) processes are defined below.

Electromagnetic Compatibility (EMC). *Defined in Joint Publication 1-02 as: The ability of systems, equipment, and devices that use the EM spectrum to operate in their intended operational environments without causing or suffering unacceptable or unintentional degradation because of EM radiation or response. It involves the application of sound EM spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.*

Electromagnetic Environment (EME). *Defined in Joint Publication 1-02 as: The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static.*

Electromagnetic Environmental Effects (E3). *Defined in Joint Publication 1-02 as: The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility and electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static.*

Electromagnetic (EM) Spectrum. *Defined in Joint Publication 1-02 as: The range of frequencies of EM radiation from zero to infinity. It is divided into 26 alphabetically designated bands. The terms "electromagnetic spectrum" and "spectrum" shall be synonymous.*

Host Nations (HNs). *Defined in Joint Publication 1-02 as* : *A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory.*

Net-Centric. Defined in DoDI 8320.02 as: *Relating to, or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes and people) in which data is shared timely and seamlessly among users, applications and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and network-centric warfare (NCW).*

Spectrum Management. *Defined in Joint Publication 1-02 as* : *Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.*

Spectrum-Dependent Systems. *Defined in DoDI 4650.01 as* : *All electronic systems, subsystems, devices, and/or equipment that depend on the use of the spectrum to properly accomplish their function(s) without regard to how they were acquired (full acquisition, rapid acquisition, Joint Concept Technology Demonstration, etc.) or procured (commercial off-the-shelf, government off-the-shelf, non-developmental items, etc.).*

Spectrum Supportability Risk Assessment (SSRA). *Defined in DoDI 4650.01 as* : *Risk assessment performed by DoD Components for all spectrum-dependent systems to identify risks as early as possible and affect design and procurement decisions. These risks are reviewed at acquisition milestones and are managed throughout the system's life cycle.*

7.7. Accessibility of Electronic and Information Technology

7.7. Accessibility of Electronic and Information Technology

In accordance with Section 508 of Public Law 105-220, "The Workforce Investment Act of 1998," now codified as Title 29 USC Sec. 794d, When developing, procuring, maintaining, or using electronic and information technology, each Federal department or agency, shall ensure, unless an undue burden would be imposed, that the electronic and information technology (E&IT) allows, regardless of the type of medium of the technology--

(i) individuals with disabilities who are Federal employees to have access to and use of information and data that is comparable to the access to and use of the information and data by Federal employees who are not individuals with disabilities; and

(ii) individuals with disabilities who are members of the public seeking information or services from a Federal department or agency to have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities (http://www.justice.gov/crt/508/508law.php).

Section 508 does NOT however, in accordance with DoDM 8400.01-M, Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations, apply to the following:

(1) Any E&IT operated by agencies, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or systems critical to the direct fulfillment of military or intelligence missions. Systems that are critical to the direct fulfillment of military or intelligence missions do not include systems used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(2) E&IT acquired by a contractor incidental to a contract. For example, if a firm is contracted to develop a website for the Department of Defense, the website created must be fully compliant with Section 508; however, the firm's own website is not required to be Section 508-compliant.

(3) E&IT located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment.

The law further directs the United States Access Board to develop standards to support Section 508 . For Requiring Officials who will be acquiring E&IT, the General Services Administration provides a website for assistance in developing Section 508 language in DoD contracts . Included at this site is the Voluntary Product Accessibility Template or VPAT, which helps PMs identify products and vendors that comply with this Federal

law. Additional guidance on the DoD Section 508 program is provided in DoD Section 508 Manual (DoDM 8400.01-M) dated June 3, 2011 .

7.8. The Clinger-Cohen Act (CCA) -- Subtitle III of Title 40 United States Code (U.S.C.)

7.8.1. Overview

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (hereinafter referred to as "Title 40/CCA") applies to all Information Technology (IT) investments, including National Security Systems (NSS). (**Note:** Throughout the remainder of this subchapter 7.8, the term IT is presumed to mean IT, including NSS.) Title 40/CCA requires Federal agencies to focus more on the results achieved through its IT investments, while streamlining the Federal IT procurement process. Specifically, this Act introduces much more rigor and structure into how agencies approach the selection and management of IT projects.

Title 40/CCA generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing the acquisition of IT. It elevated oversight responsibility to the Director of the Office of Management and Budget (OMB) and established and gave oversight responsibilities to the departmental Chief Information Officer (CIO). Also, under this Act, the head of each agency is required to implement a process for maximizing the value and assessing and managing the risks of the agency's IT acquisitions.

In DoD, the DoD CIO has the primary responsibility of providing management and oversight of all Department IT to ensure the Department's IT systems are interoperable, secure, properly justified, and contribute to mission goals.

The basic requirements of the Title 40/CCA , relating to DoD's acquisition process, have been institutionalized in DoD Instruction 5000.02, "Operation of the Defense Acquisition System;" in particular, Enclosure 5, IT Considerations . The requirements delineated in the Title 40/CCA Compliance Table at Enclosure 5 of DoD Instruction 5000.02 must also be considered and applied to all IT investments, regardless of acquisition category, and tailored commensurate to size, complexity, scope, and risk levels. Table 7.8.1.T1 depicts a summary of Title 40/CCA obligations and authorities.

Table 7.8.1.T1. Summary of Clinger-Cohen Act Compliance Confirmations*

	Statutory Authority		Regulatory Authority
	40 U.S.C. Subtitle III (aka Clinger-Cohen Act (CCA))	2001 NDAA 811 (P.L. 106-398)	DoDI 5000.02
MDAP	Comply	n/a	Confirm* Compliance by Component CIO
MAIS	Comply	Confirm Compliance	Confirm Compliance by Component CIO
All Other	Comply	n/a	Confirm Compliance by Component CIO
* "Certifications" of CCA compliance are no longer required by any statute or regulation.			

This section assists program managers, program sponsors/domain owners, members of the joint staff, and DoD Component CIO community to understand and comply with Title 40/CCA requirements. Their responsibilities are defined throughout this section and at the IT Community of Practice knowledge center, which also contains a vast array of information pertinent to specific aspects of Title 40/CCA compliance.

7.8.2. Definitions of "information technology" and "National Security System" from Title 40/Clinger-Cohen Act

Information technology.- The term information technology-

(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use-

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer,

software, firmware and similar procedures, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

(1) National security system.- In this section, the term national security system means a telecommunications or information system operated by the Federal Government, the function, operation, or use of which-

(A) involves intelligence activities;

(B) involves cryptologic activities related to national security;

(C) involves command and control of military forces;

(D) involves equipment that is an integral part of a weapon or weapons system; or

(E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

(2) Limitation.- Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

7.8.3. Mandatory Policies

A comprehensive compilation of Federal laws, OMB and Budget circulars, DoD directives and instructions, and OSD policy memorandums, relevant to all aspects of Title 40/CCA compliance, is available in the CCA Policy Folder of the Acquisition Community Connection.

The Title 40/CCA Compliance Table, Table 7.8.4.T1, in Section 7.8.4 below, details actions required to comply with Title 40/CCA regulatory requirements, mandatory DoD policy, and the applicable program documentation that can be used to fulfill the requirement. This table emulates the DoD Instruction 5000.02 Title 40/CCA Compliance Table, Table 8, with the addition of columns relating the requirement to applicable Milestones and regulatory guidance.

The requirements in this table must be satisfied before Milestone approval of any Acquisition Category (ACAT) I (i.e., Major Defense Acquisition Program (MDAP)) and ACAT IA (i.e., MAIS Program) and prior to the award of any contract for the acquisition of a Mission-Critical or Mission-Essential IT system, at any level.

TAKE NOTE: The requirements delineated in this table must also be considered and applied to all IT investments, regardless of acquisition category, and tailored

commensurate to size, complexity, scope, and risk levels.

7.8.4. Title 40/Clinger-Cohen Act (CCA) Compliance Table

7.8.4. Title 40/Clinger-Cohen Act (CCA) Compliance Table

Table 7.8.4.T1 is a Title 40/CCA compliance table that includes hyperlinks relative to each compliance area. A brief discussion of each compliance area and hyperlinks to additional pertinent information follow the table. For comprehensive coverage of the Title 40/CCA, including policy documents, best practices, examples, and lessons learned, refer to the CCA Community of Practice website.

Table 7.8.4.T1. Title 40/CCA Compliance Table, Annotated

Actions Required to Comply With Title 40 U.S.C. Subtitle III	Applicable Program Documentation [1]	Applicable Milestone	Regulatory Requirement
1. Make a determination that the acquisition supports core, priority functions of the Department. [2]	ICD Approval	Milestone A	CJCSI 3170.01
2. Establish outcome-based performance measures linked to strategic goals. [2]	ICD, CDD, CPD and APB approval	Milestone A, B & C	CJCSI 3170.01 DoDI 5000.02
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [2]	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD	Milestone A, B & C	CJCSI 3170.01 DoDI 5000.02
4. Determine that no Private Sector or Government source can better support the function. [3]	Technology Development Strategy Acquisition Strategy page XX, para XX AoA page XX	Milestone A Milestone B	CJCSI 3170.01 DoDI 5000.02

5. Conduct an analysis of alternatives. [3]	AoA	For MAIS: Milestone A & B, & FRPDR (or their equivalent) For non-MAIS: Milestone B or the first Milestone that authorizes contract award	DoDI 5000.02
6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a Life-cycle Cost Estimate (LCCE). [3]	Program LCCE Program Economic Analysis for MAIS	Milestone A & B	CJCSI 3170.01 DoDI 5000.02
7. Develop clearly established measures and accountability for program progress	Acquisition Strategy page XX APB	Milestone B	DoDI 5000.02
8. Ensure that the acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards	APB (Net-Ready KPP) ISP (Information Exchange Requirements)	Milestone A, B & C	CJCSI 6212.01 DoDI 5000.02
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	Acquisition Information Assurance Strategy	Milestone A, B, C, FRPDR or equivalent*****	DoDI 5000.02 DoDD 8580.01

10. Ensure, to the maximum extent practicable, (1) modular contracting has been used, and (2) the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments	Acquisition Strategy page XX	Milestone B or the first Milestone that authorizes contract award	DoDI 5000.02
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO [4/5]	DoD IT Portfolio Repository	Milestone B, Update as required	DoDI 5000.02

Title 40/CCA Compliance Table Notes:

1. The system documents/information cited are examples of the most likely but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited. Include page(s) and paragraph(s), where appropriate.

2. These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command Control Systems that are not themselves IT systems.

3. These actions are also required in order to comply with Section 811 of Public Law 106-398 (Reference (ag)).

4. For NSS, these requirements apply to the extent practicable (Title 40 U.S.C. 11103, Reference (v)).

5. Definitions:

Mission-Critical Information System: A system that meets the definitions of "information system" and "national security system" in the Title 40/CCA (Reference (n)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (**Note:** The designation of mission critical shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)).) A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."

Mission-Essential Information System: A system that meets the definition of "information system" in Reference (n), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (**Note:** The designation of mission essential shall be made by a Component Head, a Combatant Commander, or their designee. A financial management IT system shall be considered a mission-essential IT system as defined by the USD(C).) A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."

5. Only unclassified data may be entered into DoD Information Technology Portfolio Repository. If the information about the system being registered is classified up to SECRET collateral level, the system should be registered with the DoD CIO by entering it into the DoD Secret Internet Protocol Router Network IT Registry.

[7.8.5. Other Title 40/Clinger-Cohen Act (CCA)-Related Legislative Requirements]

7.8.5. Other Title 40/Clinger-Cohen Act (CCA)-Related Legislative Requirements

One other topic not addressed in the Title 40/CCA Compliance Table is the Post

Implementation Review (PIR), previously referred to as the Post Deployment Performance Review. See Section 7.9 of this guide for an in-depth discussion of PIR.

7.8.6. Title 40, Subtitle III /Clinger-Cohen Act (CCA) Compliance Requirements

This section provides an overview of the actions stipulated in the Title 40/CCA Compliance Table, which must be addressed and ultimately lead to confirmation of compliance of a MAIS or MDAP by the DoD CIO. The DoD Component Requirements Authority, in conjunction with the Acquisition Community, is accountable for requirements 1 through 5 of the table; the program manager (PM) is accountable for requirements 6 through 11.

The PM should prepare a table similar to Table 7.8.4.T1, above, to indicate which documents support the Title 40/CCA requirements. DoD Component CIOs should use those supporting documents to assess and confirm Title 40/CCA compliance. For in-depth coverage of each Title 40/CCA requirement, refer to the CCA Community of Practice as well as the links provided in subsections 7.8.6.1 through 7.8.6.11 and

section 7.9.

7.8.6.1. Determining that the Acquisition Supports the Core, Priority Functions of the Department

Overview: This element of the Title 40/CCA asks if the function supported by a proposed acquisition is something the Federal government actually needs to perform; i.e., for the DoD, is the function one that we (DoD and/or its Components) must perform to accomplish the military missions or business processes of the Department?

For Warfare Mission Area and Enterprise Information Environment functions, this question is answered in the Joint Capabilities Integration and Development System (JCIDS) process. Before a functional requirement or new capability enters the acquisition process, the JCIDS process (See the JCIDS Manual) requires the Sponsor/Domain Owner (hereafter referred to as the Sponsor)to conduct a series of analyses. The result of these analyses is reported in an Initial Capabilities Document.

Ideally, these analyses will show that the acquisition supports core/priority functions that should be performed by the Federal Government. Moreover, the analysis should validate and document the rationale supporting the relationship between the Department's mission (i.e., core/priority functions) and the function supported by the acquisition.

Who is Responsible? The Sponsor with cognizance over the function leads the analysis work as part of the JCIDS processes.

Implementation Guidance: Ensure that the JCIDS analytical work addresses the Title 40/CCA question by establishing the linkage between the mission, the function supported, the capability gap and potential solutions. The following questions should be helpful in determining whether a program supports DoD core functions:

- Does the program support DoD core/primary functions as documented in national strategies and DoD mission and strategy documents like the Quadrennial Defense Review, Strategic Planning Guidance, Joint Operating Concepts, Joint Functional Concepts, Architectures (as available), the Business Enterprise Architecture, the Universal Joint Task List, mission area statements, or Service mission statements?

7.8.6.2. Establish Outcome-based Performance Measures

Overview: Title 40/Clinger-Cohen Act mandates performance and results-based management in planning and acquiring IT A key element of performance and results-

based management is the establishment of outcome-based performance measures, also known as measures of effectiveness (MOE), for needed capability. MOEs for capabilities needed by the Warfighting and Enterprise Information Environment Mission Areas are developed during a Capabilities-based Assessment (CBA) and recorded in a validated Initial Concept Document. The Business Mission Area identifies outcome-based performance measures during the business case development process and records the approved measures in the business plan.

This section defines measurement terminology, relates it to DoD policy and provides guidance for formulating effective outcome-based performance measures for IT investments. For clarification, the various uses and DoD definitions of MOEs are provided in the CCA Community of Practice (CoP). Regardless of the term used, the Title 40/CCA states that the respective Service Secretaries shall:

- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the agency's customers through the effective use of IT.
- Ensure that performance measurements are prescribed for IT programs used by or to be acquired for the executive agency, and that the performance measurements measure how well the IT supports programs of the executive agency.
- Conduct post-implementation reviews of fielded capabilities to determine if they were achieved, verify estimated benefits, and document effective management practices for broader use.

In summary, we are obligated to state the desired outcome, develop and deploy the solution, and then measure the extent to which we have achieved the desired outcome. For further discussion, see the Title 40/CCA language in OMB Circular A-11, Part 7, Page 16 of Section 300, Part ID. Additionally, discussions on the statutory basis and regulatory basis for MOEs and their verification are available in the IT-CoP.

Who is Responsible?

- The program Sponsor with cognizance over the function oversees the development of the MOEs during the CBA phase of the JCIDS process. The Sponsor ensures that the MOEs are outcome-based standards for the validated capabilities.
    - The PM must be aware of the MOEs and how they relate to overall program effectiveness and document these MOEs in the Exhibit 300 that is part of DoD's budget submission to OMB.
- The DoD CIO assesses the outcome-based measures in deciding whether to confirm Title 40/CCA compliance for ACAT IA programs and recommend Section 801 (2366(a)) (or subsequent defense authorization provision) compliance to the Milestone Decision Authority (MDA) for ACAT ID programs.

Implementation Guidance: This section is written to help the Sponsor prepare the MOEs

and to help the PM understand his/her role in the MOE refinement process. The key to understanding and writing MOEs for IT investments is to recognize their characteristics and source. Therefore, MOEs should be:

- Written in terms of desired outcomes.
- Quantifiable (note that both subjective and objective goals can be quantified).
- Serve as a measure of the degree to which the desired outcome is achieved.
- Independent of any solution and should not specify system performance or criteria.

To satisfy the requirement that an MOE be independent of any solution and not specify system performance or criteria, the MOE should be established before the Materiel Solution Analysis phase because the MOEs guide the analysis and selection of alternative solutions leading up to Milestone A. Although the MOE may be refined as a result of the analysis undertaken during this phase, the source of the initial mission/capability MOE is the functional community. The MOE is the common link between the Initial Capabilities Document (ICD), the Analysis of Alternatives (AoA) and the benefits realization assessment conducted during a PIR as described in Section 7.9 of this guide.

As stated in Table 8 of DoD Instruction 5000.02, for a weapon system with embedded IT and for command control systems that are not themselves IT systems, it shall be presumed that the acquisition has outcome-based performance measures linked to strategic goals and that they are likely to be found in a JCIDS document (ICD, Capability Development Document (CDD) or Capability Production Document (CPD)). Note however that the presumption exists because the JCIDS requires the development of MOEs. For Title 40/CCA confirmation, approved MOEs are required to be presented to the DoD Component CIO.

For further MOE writing guidance, see the Information Technology Community of Practice Measures of Effectiveness Area.

7.8.6.3. Redesigning the Processes that the Acquisition Supports

Overview: This element of the Title 40/CCA asks if the business process or mission function supported by the proposed acquisition has been designed for optimum effectiveness and efficiency. Title 40/CCA requires the DoD Component to analyze its mission, and based on the analysis, revise its mission-related processes and administrative processes as appropriate before making significant investments in IT. There are a number of ways to accomplish this requirement, but this is known as business process reengineering (BPR) and is used to redesign the way work is done to improve performance in meeting the organization's mission while reducing costs.

To satisfy this requirement, BPR is conducted before entering the acquisition process. However, when the results of the JCIDS analysis, including the AoA, results in a Commercial-Off-The-Shelf (COTS) enterprise solution, additional BPR is conducted

after program initiation, to reengineer an organization's retained processes to match available COTS processes. As stated in Table 8 of DoD Instruction 5000.02, for a weapon system with embedded IT and for command and control systems that are not themselves IT systems, it shall be presumed that the processes that the system supports have been sufficiently redesigned if one of the following conditions exist: "(1) the acquisition has a JCIDS document (ICD, CDD, CPD) that has been validated by the Joint Requirements Oversight Council (JROC) or JROC designee, or (2) the MDA determines that the AoA is sufficient to support the initial Milestone decision."

Who is Responsible?

- The Sponsor with cognizance over the function with input from the corresponding DoD Component functional sponsor is responsible for BPR.
- The PM should be aware of the results of the BPR process and should use the goals of the reengineered process to shape the acquisition.
- The Director of the Office of the Secretary of Defense (OSD), Cost Assessment and Program Evaluation (CAPE) (OD/CAPE) assesses an ACAT IAM program's AoA to determine the extent to which BPR has been conducted.
- The DoD CIO assesses an ACAT IAM program's AoA to determine whether sufficient BPR has been conducted.

Business Process Reengineering: Benchmarking

Benchmarking is necessary for outcome selection and BPR. The Sponsor should quantitatively benchmark agency outcome performance against comparable outcomes in the public or private sectors in terms of cost, speed, productivity, and quality of outputs and outcomes.

Benchmarking should occur in conjunction with a BPR implementation well before program initiation. Benchmarking can be broken into four primary phases:

- *Planning Phase:* Identify the product or process to be benchmarked and select the organizations to be used for comparison. Identify the type of benchmark measurements and data to be gathered (both qualitative and quantitative data types). One method to gather data is through a questionnaire to the benchmarking organization that specifically addresses the area being benchmarked.
- *Data Collection and Analysis Phase:* Initiate the planned data collection, and analyze all aspects of the identified best practice or IT innovation to determine variations between the current and proposed products or processes. Compare the information for similarities and differences to identify improvement areas. Use root cause analysis to break the possible performance issues down until the primary cause of the gap is determined. This is where the current performance gap between the two benchmarking partners is determined.
- *Integration Phase:* Communicate the findings; establish goals and targets; and define a plan of action for change. This plan of action is often the key to

successful BPR implementation. Qualitative data from a benchmarking analysis is especially valuable for this phase. It aids in working change management issues to bring about positive change.
- *Implementation Phase:* Initiate the plan of action and monitor the results. Continue to monitor the product or process that was benchmarked for improvement. Benchmark the process periodically to ensure the improvement is continuous.

7.8.6.4. Determining That No Private Sector or Other Government Source Can Better Support the Function

Overview: This element of the Title 40/CCA asks if any private sector or other government source can better support the function. This is commonly referred to as the "outsourcing determination." The Sponsor determines that the acquisition MUST be undertaken by DoD because there is no alternative source that can support the function more effectively or at less cost. Note that for weapon systems and for command and control systems, the need to make a determination that no private sector or Government source can better support the function only applies to the maximum extent practicable. As an example, consider that both the DoD and the Department of Homeland Security have common interests. This requirement should be presumed to be satisfied if the acquisition has a MDA-approved acquisition strategy.

Who is Responsible?

- The Sponsor with cognizance over the function leads the analysis work as part of the AoA process.
- The PM updates and documents the supporting analysis in the AoA and a summary of the outsourcing decision in the Acquisition Strategy.

7.8.6.5. Analysis of Alternatives (AoA)

Overview: The Director of the Office of the Secretary of Defense (OSD), Cost Assessment and Program Evaluation (OD/CAPE), provides basic policies and guidance associated with the AoA process. Detailed AoA guidance can be found in Chapter 3.3. Analysis of Alternatives. For ACAT ID and IAM programs, OD/CAPE prepares and approves the AoA study guidance, approves the Component-prepared AoA study plan, and reviews the final analysis products (briefing and report). After the review of the final products, OD/CAPE provides an independent assessment to the MDA (see DoD Instruction 5000.02, Enclosure 7, paragraph 5). See Section 3.3 of this guidebook for a general description of the AoA and the AoA Study Plan.

7.8.6.6. Economic Analysis (EA) and Life-Cycle Cost (LCC) Estimates

Overview: An EA consists of an LCC and a benefits analysis and is a systematic

approach to selecting the most efficient and cost effective strategy for satisfying an agency's need. See Sections 3.6 and 3.7 of this guidebook for detailed EA and LCC estimate guidance.

7.8.6.7. Acquisition Performance Measures

Overview: Acquisition performance measures are clearly established measures and accountability for program progress. The essential acquisition measures are those found in the acquisition program baseline (APB): cost, schedule and performance. See section 2.1 of this guide for detailed APB guidance.

7.8.6.8. The acquisition is consistent with the Global Information Grid (GIG) policies and architecture

Overview: The GIG is the organizing and transforming construct for managing IT for the Department. See Section 7.2.1.2 for detailed guidance on GIG policies and architecture.

7.8.6.9. The program has an Information Assurance (IA) strategy that is consistent with DoD policies, standards and architectures

Overview: IA concerns information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities. See Section 7.5 of this guidebook for detailed guidance on IA.

7.8.6.10. Modular Contracting

Overview: Under modular contracting, a system is acquired in successive acquisitions of interoperable increments. The Title 40 is concerned with modular contracting to ensure that each increment complies with common or commercially acceptable standards applicable to IT so that the increments are compatible with the other increments of IT comprising the system.

Who is Responsible?

- The PM is responsible for ensuring that modular contracting principles are adhered to.
- The contracting strategy is addressed in the Acquisition Strategy, which is approved by the MDA.

Implementation Guidance: See Section 4.5.4 of this guidebook for a discussion of Open Systems Approach as a systems engineering technique that will support modularity, and Section 39.103 of the Federal Acquisition Regulations for a detailed discussion of Modular Contracting.

7.8.6.11. DoD Information Technology (IT) Portfolio Repository (DITPR)

Overview: The DITPR (requires login) supports the Title 40 /CCA inventory requirements and the capital planning and investment processes of selection, control, and evaluation. The DITPR contains a comprehensive unclassified inventory of the Department's mission-critical and mission-essential NSS and their interfaces. It is web-enabled, requires a Common Access Card (CAC) to obtain access, and requires a user account approved by a DoD Component or DoD IT Portfolio Management (PfM) Mission Area or Domain Sponsor. There is a separate inventory on the Secret Internet Protocol Router Network (SIPRNET) called the DoD SIPRNET IT Registry, which requires a separate user account to obtain access. DoD Components provide their IT systems inventory data to either DITPR or the DoD SIPRNET IT Registry there is no overlap between the two repositories. Data is entered into DITPR by one of two means. For the Army, Air Force, Department of the Navy (Navy, US Marine Corps), and the TRICARE Management Activity, data is entered into the DoD Component's IT inventory system and uploaded to DITPR by batch update monthly. All other Components work directly online in DITPR. The applicable policy and procedure document is the DoD IT Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance, August 10, 2009.

Who is Responsible? The PM is responsible for ensuring the system is registered and should follow applicable DoD CIO procedures and guidance.

DITPR Update Procedure: The DITPR guidance outlines a standard, documented procedure for updating its contents on a monthly basis. The rules, procedures, and protocols for the addition, deletion, and updating of system information are available to users once they are registered. Service and Agency CIOs confirm the completeness of the inventory and the accuracy of the data on the inventory on an annual basis.

Use of the DITPR for Decision Making: The DITPR and the DoD SIPRNET IT Registry are the Department's authoritative inventories of IT systems. They provide senior DoD decision makers a coherent and contextual view of the capabilities and associated system enablers for making resource decisions and a common central repository for IT system information to support the certification processes of the various Investment Review Boards (IRBs) and the Defense Business Systems Management Committee (DBSMC). DITPR provides consistent automated processes across the DoD Components to meet compliance reporting requirements (e.g., Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (NDAA), Federal Information Security Act of 2002 (FISMA), E-Authentication, Privacy Act, Privacy Impact Assessments, Social Security Number Reduction, Records Management, and Interoperability). DITPR also enables the Mission Areas and the Components to accomplish IT PfM.

7.8.7. Procedure for Risk-Based Oversight (RBO) Process

7.8.7.1. Background

Since the enactment of the Information Technology Management Reform Act of 1996, currently referred to as the Title 40/CCA , the DoD CIO has overseen the Title 40/CCA implementation of ACAT I and IA weapons and automated information systems, in accordance with the provisions of DoDI 5000.02. Under the risk-based oversight policy, the objective is to make DoD CIO oversight of Title 40/CCA compliance the exception.

Further, the risk-based Title 40/CCA compliance oversight enables the DoD CIO to identify and implement a cost-effective means for ensuring Title 40/CCA compliance, by providing a decision making framework to help leverage Title 40/CCA oversight responsibility to the DoD Component CIO. In a risk-based oversight model, the DoD Component CIOs oversee programs within their portfolios, commensurate with their demonstrated level of capability across Title 40/CCA compliance areas.

7.8.7.2. Procedures for Title 40/CCA Risk-Based Oversight

These procedures are applicable to all MAIS programs and MDAPs, even those delegated to the DoD Components. Nothing in these procedures detracts from responsibilities described in DoDI 5000.02. The risk-based oversight process addresses the manner and level of DoD CIO and DoD Component CIO involvement in oversight of MAIS and MDAP programs. The process is initiated when the DoD Component CIO conducts a self-assessment of Title 40/CCA compliance oversight capability.

7.8.7.3. DoD Component Chief Information Officer (CIO) Self-Assessment Document

This document asks a series of questions related to the implementation of oversight for Title 40/CCA within DoD Components. The primary audience for this assessment is the DoD Component CIO. These questions were derived from a range of resources, including policy and guidance documents, feedback from a 2004-2005 Title 40/CCA Assessment sponsored by the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer ()DoD CIO)/Deputy CIO (DCIO), and USD(AT&L), and input from DoD personnel across multiple organizations and functions. For further information, see the Risk-Based Oversight for Title 40/Clinger-Cohen Act (CCA) Compliance folder in the Information Technology (IT) Community of Practice .

This document "Sample Self-Assessment file: 7.8.7.5. Self-Assessment of CCA

Compliance.doc" asks a series of questions related to the implementation of oversight for Title 40/ CCA within DoD Components. The primary audience for this assessment is the DoD Component CIO. These questions were derived from a range of resources, including policy and guidance documents, feedback from a 2004-2005 Title 40/CCA Assessment sponsored by the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO/DCIO and USD(AT&L), and input from DoD personnel across multiple organizations and functions .

7.9. Post-Implementation Review (PIR)

7.9.1. Background

The Government Performance and Results Act (GPRA) Modernization Act of 2010 requires that Federal Agencies compare actual program results with established performance objectives. In addition, Section 11313 of Subtitle III of title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (hereinafter referred to as "Title 40/CCA") requires that Federal Agencies ensure that outcome-based performance measurements are prescribed for the Information Technology (including National Security Systems (IT/NSS)) to be acquired and that these performance measurements measure how well the IT/NSS supports the programs of the Agency.

DoD Instruction 5000.02, Tables 2-1 and 2-2 , identify this information requirement as a Post-Implementation Review (PIR) and require a PIR for all acquisition program increments at the Full-Rate Production Review/Full-Deployment Decision Review (FRPDR/FDDR). To clarify this requirement, it is a plan for conducting a PIR that is due

at the FRPDR or FDDR. The actual PIR is conducted, and a report is generated after Initial Operational Capability (IOC) and generally before Full Operational Capability. (Refer to section 7.9.5 of this guidebook for specific PIR Implementation Steps.)

The Office of Management and Budget (OMB) in OMB Circular A-130 Chapter 8 paragraph b.1(c and d) prescribes PIR procedures within the capital planning and investment control construct for measuring how well acquired IT supports Federal Agency programs.

OMB Guidance for IT Investment Reporting, Table C1 of Section C to Exhibit 300B. Performance Measurement Report requires operational data that measures the effectiveness of the investment in delivering the desired service or support level and measures the investment against its defined process standards or technical service level agreements (SLAs) (e.g., Reliability and Availability). The 300B is an annual report that is submitted twice annually, BES in September and PB in March. Since the 300B is a new report, procedures for coordination with PIR information requirement are TBD. Updates will be posted in the PIR section of the IT-CoP. (Readers who are members of ACC can receive notification of PIR process changes between DAG versions by going to IT-CoP and clicking on Other Actions and then clicking on Subscribe. To become a member of ACC, click on Become a Member in the left margin.)

7.9.2. Overview

This section provides guidance on how to plan and conduct a PIR for a capability that has been fielded and is operational in its intended environment. A PIR verifies the measures of effectiveness (MOEs) of the Initial Capabilities Document (ICD) or the benefits of a business plan and answers the question, "Did the Service/Agency get what it needed, per the ICD/Business Plan, and if not, what should be done?

Who is Responsible? The Sponsor is responsible for articulating outcome-based performance measures in the form of MOEs or benefits and ensuring they are reported in the ICD or Business Plan. The Sponsor is responsible for planning the PIR, gathering data, analyzing the data, and assessing the results. The Program Manager (PM) is responsible for maintaining an integrated program schedule that includes the PIR on behalf of the Sponsor. The PM is also responsible for supporting the Sponsor with respect to execution and reporting of the PIR.

What is a PIR? The PIR is a process that aggregates information needed to successfully evaluate the degree to which a capability has been achieved. Table 7.9.2.T1 represents potential sources of such data. Note that the information sources in this table represent a broad segment of acquisition, administrative, and operational activities.

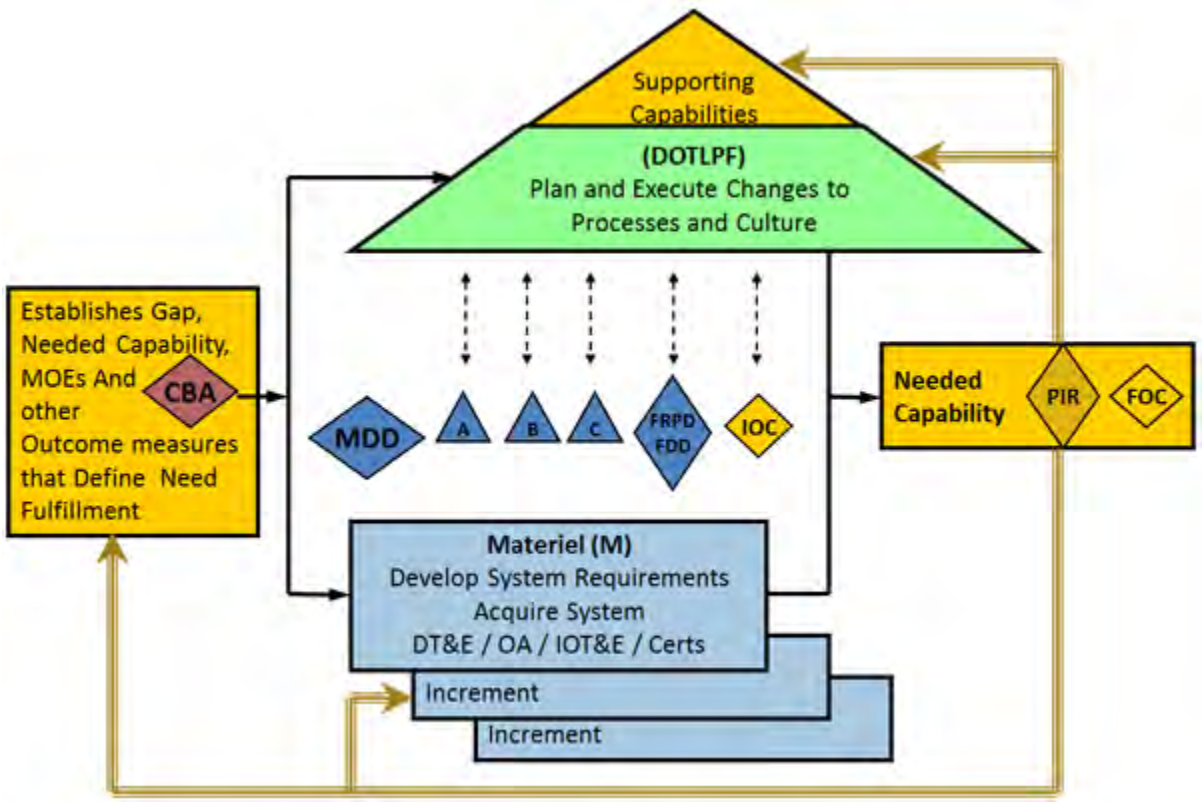
Table 7.9.2.T1. Potential PIR Information Sources

FOT&E Results	Annual Chief Financial Officer Report
Platform Readiness Assessments	Mission Readiness Reviews
COCOM Exercises	Return on Investment Assessment
User Satisfaction Surveys	War Games
Information Assurance Assessments	Lessons Learned

7.9.3. Post Implementation Review (PIR) Within the Acquisition Framework

A useful way to view a PIR is that it is a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) assessment. As shown in Figure 7.9.3.F1, the capability-based assessment (CBA) (or business case for business systems) defines the need, provides MOEs, and analyzes the changes that may be needed to one or more Joint Capability Areas (JCA) (For definitions and a discussion of JCAs see the IT-CoP page on JCAs). The "materiel (M)" contribution to the need enters the defense acquisition framework, which coordinates with the remaining DOTLPF process and arrives at the FRPDR/FDDR. The final PIR plan is presented at this time. Following IOC the fielded system is integrated with the changes to process and culture implemented during DOTLPF, and becomes a recognizable and measurable capability. The PIR takes place at this time and informs the DOTLPF, acquisition, and future CBA processes.

Figure 7.9.3.F1. Identification, Development and Verification of Capability



7.9.4. Post Implementation Review (PIR) Implications for Evolutionary Acquisition

PIRs provide important user feedback and consequently are a fundamental element of evolutionary acquisition. Ideally, we want to understand how well a recently completed increment meets the needs of users before finalizing the requirements for a subsequent increment. In practice however, the opportunity for such feedback depends on the level of concurrency in the increment development schedule.

Additionally, changes in the environment may drive new requirements. The PIR gives both the Sponsor, PM, and other stakeholders such as DOT&E and CAPE, empirical feedback to better understand DOTMLPF issues with the completed increment. This feedback enables the acquisition principals to adjust or correct the Capability Development Document/Capability Production Document and/or the DOTMLPF Change Recommendation (DCR) for subsequent increments.

7.9.5. Post Implementation Review (PIR) Implementation Steps

7.9.5.1. Plan the PIR and submit plans and report

The final PIR Plan is due at the FRP/FD Decision Review.

When planning the PIR, consider the following:

- Timing of the PIR. The PIR should take place post-IOC after a relatively stable operating environment has been established and the data identified in the PIR plan has been collected. Time frame for the PIR varies with the solution deployment strategy, but the PIR is to be executed and a report submitted prior to Full Operational Capability. If an FOC is not planned, the PIR is to be executed within one year of IOC.
- Identification of Scope.
- Identification of Stakeholders. Remember to consider those who will be tasked to provide resources.
- Team Composition. The PIR team should include, at minimum, the following:
    - Functional experts with working knowledge of the business area and its processes;
    - People with relevant technical knowledge;
    - CIO representatives, functional sponsors, and Domain Owners;
    - Oversight representatives.
- Identification of information sources. The ICD or Business Plan that articulated the outcome-based performance measures, or MOEs, is a good place to start. Additional data can be gleaned from operations conducted in wartime and during exercises. The lead time for most major exercises is typically one year and requires familiarity with the exercise design and funding process. Sources to consider are found in Table 7.9.2.T1.
- Analysis approach. The analysis approach is key to defining the structure and metadata of the information to be collected. For example, the definition of return on investment (ROI) in the Economic Analysis will drive the analysis approach of achieved ROI and the data to be collected.
- Reporting. The report describes the execution of the PIR, addresses the capability gaps that the IT/NSS investment was intended to fill, addresses the degree to which the gaps were filled, and recommends actions to mitigate unfilled capability gaps.
- Resource requirements. Identify the sources of resources such as manpower, travel, analysis tools, communications and other needs unique to the program. Demonstrate agreement by the resource providers; including them in the chop page or citing existing agreements.
- Schedule.
- Routing of the draft and final PIR Plan should include the identified stakeholders. An information copy of the final PIR Plan and Report is sent to the Senior Military Advisor DOT&E and the Program's CAPE Action Officer.

7.9.5.2. Conduct the Post Implementation Review (PIR)

The PIR should be carried out according to the PIR planning that was reviewed and approved at the FRPDR/FDDR. Care should be given to quality of the raw data. Based

on the PIR plan, the PIR should, at a minimum, address:

- Customer Satisfaction: Are the users satisfied that the IT investment meets their needs?
- Mission/Program Impact: Did the implemented capability achieve its intended impact?
- Confirmation that the validated need has not changed; or if it has, include as part of the course of action provided in the PIR report.
- A measure of the MOE found in the ICD.
- Benefits such as the ROI found in the business plan. Compare actual project costs, benefits, risks, and return information against earlier projections. Determine the causes of any differences between planned and actual results.

7.9.5.3. Conduct the Analysis

The analysis portion of the PIR should answer the question, "Did we get what we needed?" This provides a contrast to the test and evaluation measurements of key performance parameters that answer the question, "Did we get what we asked for?" This would imply that the PIR should assess, if possible, the extent to which the DoD's investment decision-making processes were able to capture the warfighter's/users initial intent. The PIR should also address whether the warfighter/user needs changed during the time the system was being acquired. The outputs of the analysis become the PIR findings. The findings should clearly identify the extent to which the warfighters got what they needed.

7.9.5.4. Prepare a Report and Provide Recommendations

Based on the PIR findings, the PIR team prepares a report and makes recommendations that can be fed back into the capabilities and business needs processes. The primary recipient of the PIR report is the Sponsor who articulated the original objectives and outcome-based performance measures on which the program or investment was based.

A copy of the PIR report is also forwarded to DOT&E and CAPE. DOT&E will use the results to confirm the effectiveness and suitability assessment made during IOT&E and possibly to improve the test planning and execution for follow-on increments or similar systems (see Section 9.7.9). CAPE will compare the benefits of selected programs to those presented in the Economic Analysis.

The results of the PIR can also aid in refining requirements for subsequent increments. Recommendations may be made to correct errors, improve user satisfaction, or improve system performance to better match warfighter/business needs. The PIR team should also determine whether different or more appropriate outcome-based performance measures should be developed to enhance the assessment of future spirals or similar IT investment projects.

For further guidance on PIRs, see the Information Technology Community of Practice Post Implementation Review Area. This contains the following additional guidance:

- PIR Measurement Framework
- Common Problems with PIR Implementations
- Example plan and report

7.9.6. Post Implementation Review (PIR) Further Reading

Both government and the commercial sector address the practice of conducting a PIR for materiel, including software IT investments. The Government Accountability Office and several not-for-profit organizations have written on the subject of measuring performance and demonstrating results. The Clinger-Cohen Act Community of Practice PIR Area lists a number of key public and private sector resources that can be used in planning and conducting a PIR.

7.10. Commercial, Off-the-Shelf (COTS) Software Solutions

7.10.1. The Impetus for COTS Software Solutions

One of the Department's goals is to migrate to COTS solutions to fill Information Technology capability gaps.

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act (CCA) (referred to as "Title 40/Clinger-Cohen Act") and DoD Instruction 5000.02, Enclosure 2, paragraphs 4.c.(6) and 5.d.(1)(b)3, all require the use

of COTS IT solutions to the maximum practical extent.

7.10.2. Definition

Commercial, Off-the-Shelf (COTS) is defined as "commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency."

[From the Twelfth Edition of GLOSSARY: Defense Acquisition Acronyms and Terms.]

7.10.3. Mandatory Policies

The following bullets quote or paraphrase sections in the DoD 5000 series that specifically address COTS:

DoD Directive 5000.01, "The Defense Acquisition System" Paragraph E1.1.18, states "The DoD Components shall work with users to define capability needs that facilitate the following, listed in descending order of preference:

> *"E1.1.18.1. The procurement or modification of commercially available products, services, and technologies, from domestic or international sources, or the development of dual-use technologies; ."*

Hence, commercially available products, services, and technologies are a first priority for acquisition solutions.

DoD Instruction 5000.02, "Operation of the Defense Acquisition System"

- DoD Instruction 5000.02, Enclosure 2, paragraph 4.c.(6), states that "existing commercial off-the-shelf (COTS) functionality and solutions drawn from a diversified range of large and small businesses shall be considered," when conducting the Analysis of Alternatives.
- Enclosure 5, "IT Considerations," Table 8, "Title 40, Subtitle III /CCA Compliance Table," requires that, to be considered Title 40/CCA compliant, the Department must redesign the processes being supported by the system being acquired, to reduce costs, improve effectiveness and maximize the use of COTS technology.
- Enclosure 5, "IT Considerations," Section 8, states that: "When the use of commercial IT is considered viable, maximum leverage of and coordination with the DoD Enterprise Software Initiative shall be made."

7.10.4. COTS Software--Reuse Custom Components

Modifying the core code of a COTS product should be avoided. It is possible to add

code to the existing product, to make the product operate in a way it was not intended to do "out-of-the-box." This, however, significantly increases program and total life-cycle costs, and turns a commercial product into a DoD-unique product. The business processes inherent in the COTS product should be adopted, not adapted, by the organization implementing the product. Adopting a COTS product is done through business process reengineering (BPR). This means the organization changes its processes to accommodate the software, not vice versa. In many cases there will be a few instances where BPR is not possible. For example, due to policy or law, it may be necessary to build or acquire needed reports, interfaces, conversions, and extensions. In these cases, adding to the product must be done under strong configuration control. In cases where a particular COTS product does not provide the entire set of required functionality, a "bolt-on" could be used. A bolt-on is not part of the COTS software product, but is typically part of a suite of software that has been certified to work with the product to provide the necessary additional functionality. These suites of software are integrated to provide the full set of needed functionality. Using a bolt-on, however, also increases program and total life-cycle costs.

See section 7.10.6.3 for a more detailed discussion of reports, interfaces, conversions, and extensions.

7.10.5. COTS Integration into the Acquisition Life Cycle

The actions below are unique to acquiring COTS Information Technology solutions. These activities should occur within a tailored, responsive, and innovative program structure authorized by DoD Instruction 5000.02. The stakeholder primarily responsible for each action is shown at the end of each bullet.

7.10.5.1. Before Milestone A

- Define strategy and plan for conducting BPR during COTS software implementation phase of the program.
  (Sponsor/Domain Owner)
- Consider COTS and BPR when developing the Analysis of Alternatives. (See section 3.3 and Table 7.8.4.T1 of this guidebook).
  (Sponsor/Domain Owner)
- Consider commercially available products, services, and technologies when defining initial user needs in the Initial Capabilities Document.
  (Sponsor/Domain Owner)
- When developing the Technology Development Strategy and/or the Acquisition Strategy, consider commercial best practice approaches and address the rationale for acquiring COTS.
  (Program Manager (PM))

7.10.5.2. Before Milestone B

- To the maximum extent possible, redesign business processes to conform to the

best practice business rules inherent in the COTS product. Define a process for managing and/or approving the development of reports, interfaces, conversions, and extensions.

7.10.5.3. Before Milestone C or Full Rate Production Decision/Full Deployment Decision Review

- Ensure scope and requirements are strictly managed and additional reports, interfaces, conversions, and extensions objects are not developed without prior authorization.
  (Program Manager (PM))
- Ensure adequate planning for life-cycle support of the program. See section 3.4, Engineering for life-cycle support, of "Commercial Item Acquisition: Considerations and Lessons Learned".

7.10.5.4. After Milestone C or Full-Rate Production Decision/Full-Deployment Decision Review

Conduct ongoing engineering and integration for sustainment activities throughout the life cycle of the program.

7.10.6. Best Practices, Tools, and Methods

Various methodologies, toolsets, and information repositories have been developed to assist the Program Manager (PM) in the implementation of COTS software-based programs. The remainder of this section provides the PM descriptions of best practices, available tools and methods, and critical success factors for use in the acquisition of commercially-based solutions. Additionally, Chapter 4 of this Guidebook, Systems Engineering, presents a complete discussion of applicable systems engineering practices, to include a discussion of the Open Systems Approach.

7.10.6.1. DoD Enterprise Software Initiative

The DoD Enterprise Software Initiative (DoD ESI) is a joint, Chief Information Officer (CIO)-sponsored project designed to: "Lead in the establishment and management of

enterprise COTS information technology (IT) agreements, assets, and policies for the purpose of lowering total cost of ownership across the DoD, Coast Guard and Intelligence communities." DoD ESI is a key advisor to the DoD Strategic Sourcing Directors Board. With active working members from OSD, Department of the Army, Department of the Navy, Department of the Air Force, Defense Logistics Agency, Defense Information Systems Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, Director of National Intelligence, and Defense Finance and Accounting Service, the DoD ESI team collaborates to create Enterprise Software Agreements (ESA) for use by DoD, the Intelligence Community, and U.S. Coast Guard IT buyers. ESA negotiations and management activities are performed by IT acquisition professionals within participating DoD Components, who are designated ESI "Software Product Managers (SPM)." SPM are supported by experienced IT contracting experts.

The DoD ESI can use the Defense Working Capital Fund to provide "up-front money" for initial wholesale software buys and multi-year financing for DoD customers. This funding process assures maximum leverage of the combined buying power of the Department of Defense, producing large software discounts.

On-line resources include the DoD ESI websitelisting general products, services and procedures; the Defense Federal Acquisition Regulation Supplement Subpart 208.74; DoD Instruction 5000.2, Enclosure 5, Paragraph 6 and DoD Component requirements for compliance with DoD Enterprise Software Initiative policies.

7.10.6.2. SmartBUY

SmartBUY is a federal government strategic sourcing initiative intended to support effective enterprise level software management and achieve government-wide cost avoidance through aggregate buying of commercial software. Besides providing reduced prices and more favorable terms/conditions, the SmartBUY program assists agencies to achieve greater standardization, improved configuration management, and more robust Information Technology security.

The General Services Administration (GSA) manages the SmartBUY Program, and leads the interagency team in negotiating government-wide enterprise licenses for software. The GSA SmartBUY Program focuses on commercial-off-the-shelf software that is generally acquired using license agreements with terms and prices that vary based on volume. The GSA SmartBUY Program was formally announced on June 2, 2003 in an Office of Management and Budget Memorandum to the federal agencies. The DoD ESI Team has worked closely with the SmartBUY project since its inception, and negotiates and manages many of the SmartBUY agreements as a partner to GSA.

The DoD ESI team implements SmartBUY within the DoD through the joint DoD Deputy CIO and DPAP Policy Memorandum of December 22, 2005: Department of Defense (DoD) Support to the SmartBUY Initiative. This policy mandates use of SmartBUY agreements when user requirements match a product on SmartBUY, and also provides the framework for migrating existing Enterprise Software Initiative Enterprise

Agreements to SmartBUY Enterprise Agreements. The OMB Memo establishes requirements to be followed by federal departments and agencies. Specifically, federal agencies are to: develop a migration strategy and take contractual actions as needed to move to the government-wide license agreements as quickly as practicable; and integrate agency common desktop and server software licenses under the leadership of the SmartBUY team. This includes, to the maximum extent feasible, refraining from renewing or entering into new license agreements without prior consultation with, and consideration of the views of, the SmartBUY team.

The Federal Acquisition Regulation (FAR) Committee has developed draft regulations to implement SmartBUY.

7.10.6.3. Commercial, Off-the-shelf (COTS) Testing

On September 14, 2010, the Director, Operational Test and Evaluation, signed an updated memorandum entitled "Guidelines for Conducting Operational Test and Evaluation of Information and Business Systems." The guidelines help streamline and simplify COTS software testing procedures. They assist in tailoring pre-deployment test events to the operational risk of a specific system increment acquired under OSD oversight. For increments that are of insignificant to moderate risk, these guidelines streamline the operational test and evaluation process by potentially reducing the degree of testing. Simple questions characterize the risk and environment upon which to base test decisions, for example, "If the increment is primarily COTS, or government off-the-shelf items, what is the past performance and reliability?"

7.10.6.4. Emerging Information Technology (IT) Market Research and Commercial, Off-the-shelf (COTS) IT Lessons Learned

Section 881 of the FY 2008 National Defense Authorization Act (NDAA) requires the Department to have a Clearing-House for Rapid Identification and Dissemination of Commercial Information Technologies. To meet this need, a partnership between the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L), the Director of Defense Research and Engineering (DDR&E), the Defense Technical Information Center (DTIC) and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (DoD CIO) was formed to develop a capability that 1) allows better visibility into the Department's technology needs, 2) attracts non-traditional defense emerging technology suppliers, and 3) allows for review and discussion of COTS IT products in wide use throughout the Department. This effort, termed "DoD Techipedia" comprised of both an internal, DoD CAC-only Wiki-based collaboration area, and an external Wiki (internal.dodtechipedia.mil or a separate redirected .mil site) where DoD Capability buyers and their representatives can collaborate with Industry on a range of technology areas. Regarding wide-use COTS IT products, the objective is to raise the awareness of Government and commercial sector practices relative to the use of COTS software.

7.11. Space Mission Architectures

7.11. Space Mission Architectures

Implementation of space capabilities through space system acquisitions will be guided by an associated space mission architecture(s). Space mission architectures will be used to inform requirements validation, resourcing and the budget build process, policy, and key milestone acquisition decisions. Integration into the requirements, resourcing/budget, and policy processes will be accomplished through the governing documents for those processes. Space acquisition decisions and the resulting development programs will be evaluated at several points during the acquisition process against their associated space mission architecture(s) as a means to demonstrate added mission value to the warfighter and nation. Acceptable interoperability with other elements of the architecture, resilience, compliance with any governing policies of the architecture, and identification and mitigation of impacts resulting from unintended consequences of integration into the architecture shall also be demonstrated as well as impacts to other space and non-space related DoD mission architectures.

The purpose of developing and maintaining a space mission architecture is to have an authoritative baseline by which the Department can judge investment, cost-benefit, resilience, or operational decisions, and thereby make the best informed resourcing and acquisition decisions possible. There are two basic architectures that are widely recognized as adding value to the decision processes associated with requirements, resourcing, policy, and acquisition. The first is an As-Is architecture which represents the physical instantiation or schematic of a space mission area as it appears at the current time. Because architectures constantly evolve as new elements are added or older elements are upgraded, the As-Is architecture represents a snap-shot in time to support the immediate decision being made. The other widely used architecture is a To-Be architecture which represents how the architecture is expected to look and perform in the near term. The To-Be architecture is usually based upon funded initiatives within the most recent program review; but for acquisition decisions, should support analysis of the acquisition decision(s) under consideration. It also evolves with the completion of each budget cycle as out year plans are refined. The To-Be architecture informs the general direction in which DoD desires to proceed with a collection of mission area capabilities. Additional architecture excursions may be explored to support the annual program review or complex acquisition analyses.

A space mission architecture will be used by the MDA as the baseline or *gold standard* of performance attributes of a mission capability to aid in key decisions regarding new or improved capabilities. The architecture serves as one of many sources of information

that will be available to inform deliberations at milestone reviews, and uniquely provides the overarching strategic viewpoint to ensure introduction of new capability will support the global joint warfighter with performance against approved requirements, and result in a high degree of interoperability with other elements of the architecture. The MDA will need to understand important items such as the progress that the anticipated space system provides in moving from the As-Is toward its contribution to the To-Be (in light of other parallel efforts reflected within the architecture), the performance and capability benefits to end users, remaining gaps and shortfalls, secondary impacts to other users, alignment with the goals of the National Security Space Strategy, and the implications to health and welfare of the supporting industrial base. Likewise, the MDA will use the space mission architecture to ensure that inserting new capabilities is not disruptive; generate unnecessary costs of sustainment, or any other unintentional consequence that would necessitate an unanticipated expenditure of resources.

A formal assessment of a system and its relationship, value, functions, contributions, performance, and impacts to an associated baseline space mission architecture will be integral to the deliberations of key acquisition decisions and milestone (MS) reviews, specifically including the Materiel Development Decision and, MS A, MS B, and MS C. For all other DAB meetings, the latest approved space mission architecture assessment should be available as part of a read-ahead package to the MDA and DAB participants. The assessment of space system performance, et al, against the associated mission architecture will vary in degree of depth depending on the level of development information available during the acquisition process. The most stringent assessment can be expected to occur at MS B as part of the decision to commit significant resources to the Engineering and Manufacturing Development phase. For space system capability development, the architecture assessment for the MDA will be prepared and delivered jointly by (1) the Office responsible for the associated mission architecture(s), (2) the applicable Principal Staff Assistant(s) (PSAs), (3) the Joint Staff, and (4) Office of the Director of Cost Assessment and Program Evaluation (ODCAPE), and will include all contributing domains to the mission area (space, air, ground, maritime, cyber, etc.) This joint assessment will be led by the PSA and is meant to be an independent, unbiased analysis; however, its development should include input from the Program Management Office to ensure the proposed space system attributes are accurately represented. Dedicated participation by offices responsible for other mission area architectures that are related to, or impacted by, the proposed space system should also actively participate and achieve a common level of understanding of the architecture assessment. For key milestone reviews, or other events as directed, that will include an Independent Program Assessment (IPA) of the acquisition program by a separate team of experts, the IPA team will be thoroughly briefed on the space mission architecture assessment jointly by the responsible office, applicable PSA, Executive Agent (EA) for Space, Joint Staff, and ODCAPE, and then perform their own review and judgment for the MDA.

The offices responsible for development, maintenance, and content of the As-Is and To-Be architectures will be the EA of the Department of Defense for the mission areas to which they have been assigned. The EA for Space is responsible for maintaining

architectures associated with space systems and space missions. For those mission areas without an EA, such as communications, PNT, etc., the Principle Staff Assistant will serve as the responsible party for the architecture. The content of a space mission architecture should include, but not be limited to, a comprehensive schematic (detailed picture) of the architecture physical elements, space components, ground components, data flow between components, interface specifications both internal and external to the boundary of the architecture, performance specifications, logistics support, and communication protocols, etc. Validation of each DoD mission area architecture from a requirements perspective will be the responsibility of the Joint Staff, and will ultimately be validated by the Joint Requirements Oversight Council as comprehensive and necessary in meeting the needs of the warfighter. Validation of architectures will also be accomplished from an acquisition, requirements, resourcing and policy perspective. The Office of the Under Secretary of Defense (Acquisition, Technology & Logistics) (USD(AT&L)) will validate that architecture updates are consistent with MDA decisions, ODCAPE will validate that architectures are affordable and consistent with assigned funding by the Department, and USD(Policy) will validate that architectures are in compliance with current policy, respectively. When there is a mission architecture that does not receive validation from one of more of these sources, it is incumbent upon the office responsible for the mission architecture to assemble a joint session between requirements, acquisition, resourcing, and policy to develop a refined architecture that achieves unanimous validation. Conflicts between validation activities should be taken to the Defense Space Council for resolution. The timeline for subsequent revalidation of architectures will be determined jointly by the responsible offices, the Joint Staff, and ODCAPE as having changed sufficiently to warrant fresh review and validation; or at the discretion of the DEPSECDEF. Offices responsible for architecture development and maintenance should anticipate and resource for at least an annual update to their respective mission area architectures.

There may also be opportunities where space-related mission area architectures containing space systems will be called upon to support assessments of related non-space mission architectures that are the focus of acquisition of other DoD capabilities, or provide validation of the relationship and traceability of an acquisition program requirements baseline to overarching mission area architecture requirements.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 8 - Intelligence Analysis Support to Acquisition

8.0. Introduction

8.0. Introduction

Intelligence analysis integration is increasingly critical to DoD acquisition programs. Threat intelligence analysis and/or signatures and other Intelligence Mission Data (IMD) are required to inform and enable program capabilities and minimize costs to the government across the entire acquisition process.

Early and incremental involvement and collaboration with the DoD Intelligence Community (DoD IC) will help reduce program risks to schedule, cost, and performance. Early collaboration also increases the likelihood that the delivered system will be fully capable and more survivable against the relevant adversary threats.

Reduced risk to schedule is derived from the early identification of work to be performed by the DoD IC, proper tasking of the DoD IC at the appropriate acquisition milestone through production requirements, identification of capability gaps, costing, and negotiated delivery dates for products.

Reduced risk to cost is derived from the earliest identification of the costs and resource strategies to realize the intelligence support needed to close capability gaps throughout the acquisition life-cycle. Collaboration with the DoD IC assists both the DoD IC and the acquisition communities in determining the costs to be borne by the DoD IC and the

costs to be borne by the program.

Reduced risk to performance is driven by obtaining and inculcating threat analysis information and signature and other IMD from Material Solution Analysis through Full-Rate Production phases.

For Program Protection, Security and Counterintelligence support to acquisition programs see Chapter 13, Program Protection.

8.0.1. Purpose

The purpose of this chapter is to enable the PM to use intelligence information and data to ensure maximum war-fighting capability at the minimum risk to cost and schedule.

8.0.2. Contents

This Chapter is divided into three sections as follows:

Section 8.1 Threat Intelligence Support.

The program may require intelligence analysis of foreign threat capabilities integral to the development of future U.S. military systems and platforms over the life of the program. Identifying projected adversarial threat battlefield capabilities and evolving scientific and technical developments that affect a program or a capability's design or implementation is crucial to successful development, employment, and sustainment processes.

Section 8.2 Signatures and other IMD.

This section explains how PMs can successfully account for signatures and other IMD during system and sensor acquisition for building target models, developing algorithms, optimizing sensor design, and validating sensor functionality. As requirements for smarter, interoperable platforms and systems grow, the need for signatures and other IMD will continue to trend upwards.

Section 8.3 Intelligence Certification.

This section explains how PMs complete the Intelligence Certification and threat validation required by the Joint Staff in support of the Joint Capabilities Integration and Development System (JCIDS) process.

8.0.3. Applicability

This chapter applies to programs that are dependent upon threat intelligence analysis, signatures, and other IMD to enable mission capability in accordance with DoDD

5000.02 , and DoDD 5250.01 .

Threat intelligence analysis is provided as Capstone Threat Assessments (CTA), System Threat Assessment Report (STAR) or System Threat Assessment (STA); these are defined and explained in this chapter.

A signature is a distinctive characteristic or set of characteristics that consistently recurs and identifies a piece of equipment, material, activity, individual, or event such as a radio frequency or acoustic characteristics.

IMD is DOD intelligence used for programming platform mission systems in development, testing, operations and sustainment including, but not limited to, the following functional areas: Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics & Performance (C&P), and Geospatial Intelligence (GEOINT).

Programs dependent on signature and other IMD are those that require data for programming platform mission systems in development, testing, operations and sustainment to conduct combat identification; Intelligence, Surveillance and Reconnaissance; and targeting using, but not limited to the signatures and IMD as described above.

This Chapter does not apply to acquisitions by the DoD Components that involve a Special Access Program (SAP) created under the authority of Executive Order 12958 . The unique nature of SAPs requires compliance with special security procedures of DoDD 5205.07 .

8.0.4. Acquisition Documents Discussed in Chapter 8

The acquisition program documents discussed in Chapter 8 are listed below in Table 8.0.4.T1.

Table 8.0.4.T1. Acquisition Documents Discussed in Chapter 8

Document	Prepare	Preparation Reference
Capstone Threat Assessment (CTA)	During capability shortfall identification process. (Maintained by the DoD Intelligence Community throughout the capability development and acquisition lifecycle.)	JCIDS Manual CJCSI 3312.01B DIAI 5000.002

System Threat Assessment Report (STAR) / System Threat Assessment (STA) MAIS programs and AIS programs on the DOT&E Oversight List regardless of ACT designation are to use the Information Operations Capstone Threat Assessment	Prior to Milestone A, task the supporting intelligence production center.	DoDI 5000.02 E4, Table 3 DIAI 5000.002 Service and Component Intelligence Support to Acquisition policies
Technology Development Strategy	To support Milestone A decision. Provide summary of the threat assessment in relation to the capabilities or operational concepts the system will support.	DoDI 5000.02 Encl 2 PDUSD AT&L Memo, 20 APR 2011 Document Streamlining Program Strategies and Systems Engineering Plan
Life-cycle Signature Support Plan (LSSP)	When an acquisition program is signature (and other IMD)-dependent.	DoDD 5250.01 DIAI 3115.03

8.0.5. Support from Functional Offices

To properly accomplish activities described in this chapter, the PM needs the cooperation and support of related functional offices. Support to the acquisition community from the intelligence community involves a number of staff organizations and support activities that may be unfamiliar to members of the acquisition community. Table 8.0.5.T1 lists the functional offices that may support the PM in various tasks discussed in Chapter 8. This table identifies (and links to) the sections of Chapter 8 that describe various situations involving these offices. The individual assigned responsibility for coordinating intelligence support within a program office, laboratory, test and evaluation center, or other Research, Development, Test and Evaluation (RDT&E) organization should identify the proper contacts in these organizations prior to initiating program planning.

Table 8.0.5.T1. Functional Offices in Chapter 8

Functional Offices	Chapter 8 References

Intelligence Support Organization
 	
• Threat Intelligence
  o DoD Intelligence Community
  o Capability Development Threat Support Offices
  o System/Material Command Threat Support Offices
• Intelligence Mission Data
	8.1
	
	8.2

Intelligence Requirements Certification Office
 	
• Support to the Intelligence Certification Process
  o Joint Staff
  o DoD Intelligence Community
	8.3

8.1. Threat Intelligence Support

Threat Intelligence support to the acquisition process provides an understanding of foreign threat capabilities that is integral to the development of future U.S. military systems and platforms. Identifying projected adversarial threat capabilities, to include scientific and technical developments, which may affect a program or a capability's design or implementation is crucial to a successful development process. Furthermore, the applicable threat information must be continually updated to account for adversarial capabilities throughout the program or capability's projected acquisition to ensure that technological superiority over adversarial capabilities is maintained. See the graphic in Figure 8.1.F1.

Figure 8.1.F1. Depiction of Life-Cycle Intelligence Analysis Requirements

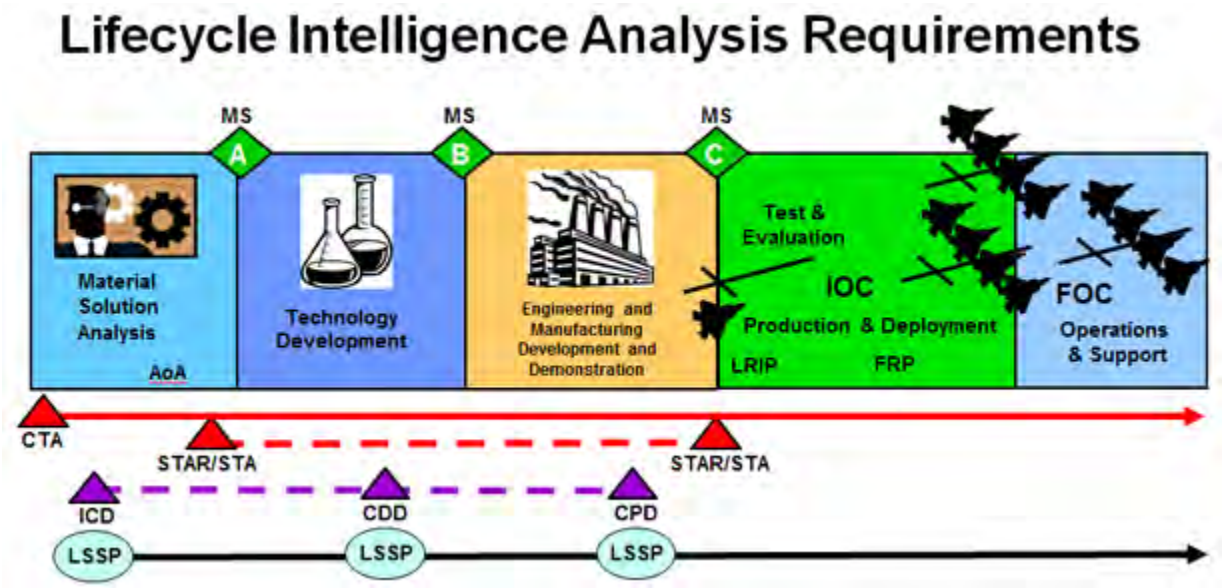


Figure 8.1.F1 illustrates the range of support provided by the threat intelligence community over the life of a particular capability shortfall identification process and resulting system acquisition program. Capstone Threat Assessments (CTA) inform the capability shortfall identification process as well as during early phases of system acquisition prior to the generation of a STAR/STA. The CTAs project foreign capabilities in particular warfare areas looking out 20 years.

At the beginning of the Material Solution Analysis phase, the program office or capability sponsor should contact the appropriate intelligence production center to support integration of validated threat information into the Technology Development Strategy. Threat information may come from DIA-validated Capstone Threat Assessments or other DIA/Service validated STARs/STAs that align with the capability mission, CONOPs, and employment timeline.

Once the capabilities sponsor, program manager or other appropriate enabler identifies concepts or prototypes for the materiel solution, the program office or capability sponsor should task the appropriate intelligence production center for the lead service to produce the System Threat Assessment Report (STAR) for Acquisition Category (ACAT) I/ Major Defense Acquisition Programs (MDAPs) and the System Threat Assessment (STA) for ACAT II programs in accordance with the regulations of that service. The program office needs to work with the producing intelligence center to provide system specific characteristics, employment CONOPS, and employment timeline as they evolve. The program office must also work with the appropriate Service Intelligence Production Center to identify Critical Intelligence Parameters (CIPs) and ensure production requirements are levied against those CIPs.

Analytic Baseline . A systems Analytic Baseline is comprised of DoD-level authoritative

policy planning guidance and an intelligence assessment of present trends, patterns and conditions, combined with validated parametric, characteristics/performance and employment data needed for development, testing, and/or training. When combined with information on appropriate friendly and neutral (Blue/Gray/White*) systems, it represents an extrapolation of the total security environment in which the system is expected to operate. A package comprises a scenario, concept of operations, and integrated data used by the DOD components as a foundation for strategic analyses. Examples of analytical baselines include scenarios and supporting data used for computer assisted war games and theater campaign simulations.

* The three colors reflect three different entities. Blue represents U.S. system data, Gray represents U.S.-produced but foreign-operated system data, and White represents neutrals. When doing long-term analysis, the impact of Blue systems must be taken in light of friendly and neutral systems.

8.1.1. Capstone Threat Assessment (CTA)

CTAs provide the bedrock analytical foundation for threat intelligence support to the defense acquisition process. CTAs, covering major warfare areas, present the DoD Intelligence Community validated position with respect to those warfare areas and will constitute the primary source of threat intelligence for the preparation of Initial Threat Environmental Assessments, STARs/STAs, and threat sections of documents supporting the JCIDS process. In order to effectively support both the capability development and acquisition processes, CTAs are not specific to existing or projected US systems, cover the current threat environment, and, in general, project threats out 20 years from the effective date of the CTA. With the lead intelligence production center, DIA's Defense Warning Office (DIA/DWO) co-chairs the Threat Steering Group (TSG) that produces and reviews the document. CTAs should be updated as determined by the responsible TSG but in any case every 24 months. DIA validates all CTAs.

Table 8.1.1.T1. Listing of Capstone Threat Assessments

WARFARE AREA	PRIMARY PRODUCTION OFFICE OR CENTER
Air Warfare	National Air and Space Intelligence Center (NASIC)
Chemical, Biological and Radiological Defense	Defense Intelligence Agency (DIA)
Information Operations	DIA/Joint Information Operations Threat Working Group
Land Warfare	National Ground Intelligence Center (NGIC)
Missile Defense	Defense Intelligence Agency (DIA)
Naval Warfare	Office of Naval Intelligence (ONI)

Space Warfare	National Air and Space Intelligence Center (NASIC)
The Capstone Threat Assessments can be found at the JWICS or SIPRNET websites of the primary production office or center. For more information contact DIAs Defense Warning Office at: JWICS email - dise541@dodiis.ic.gov SIPRNET Email jeffery.vales@dse.dia.smil.mil Commercial 434-956-2170 DSN 521	

8.1.2. System Threat Assessment Report (STAR)/System Threat Assessment (STA)

The Defense Intelligence Agency (DIA) provides validation for System Threat Assessment Reports (STARs), prepared by the appropriate Service, to support Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). Appropriate Defense Intelligence organization(s), identified by the component headquarter intelligence organizations, prepare the STAR. The assessment should be kept current and validated throughout the acquisition process. DoD Instruction 5000.02 requires that MDAPs have a validated STAR in place at Milestones B and C (and at program initiation for shipbuilding programs). The assessment should be system specific, to the degree that the system definition is available at the time the assessment is being prepared, and should address projected adversary capabilities at system initial operating capability (IOC) and at IOC plus 10 years. DIA will co-chair the TSGs for ACAT ID STARs with the producing command or center. STARs for ACAT IC MDAPs and STAs for ACAT II non-MDAPs are prepared and validated by the lead service in accordance with service regulations. DIA Instruction 5000.002 describes the required STAR elements and format.

Critical Intelligence Parameters (CIPs) are established and examined through the joint and collaborative efforts of the intelligence, capability sponsor, and acquisition management community to aid in developing intelligence production requirements to support an acquisition program. CIPs are those key performance thresholds of foreign threat systems, which, if exceeded could compromise the mission effectiveness of the U.S. system in development. Adversary military doctrine, tactics, strategy, and expected employment of systems should be considered in the CIPs. Program specific CIPs, and their associated production requirements, are a key part of a STAR and will be required for validation. The inclusion of CIPs is also encouraged for STAs. If a CIP is breached, the responsible intelligence production center will notify the program office and DIA/DWO in accordance with DIA Instruction 5000.002. DIA/DWO will notify the

appropriate organizations in the Office of the Secretary of Defense.

At the discretion of the responsible TSG, STARs/STAs can be used to support multiple programs which address like performance attributes, share an employment CONOPs, and have a similar employment timeline. Individual system descriptions and CIPs are still required to support the generation of the STAR.

Major Automated Information System (MAIS) programs use the Joint Information Operations Working Group and DIA-validated Information Operations (IO) Capstone Threat Assessment or service produced System Threat Assessment Report. DIA will validate service produced ACAT IAM STARs when the IO CTA is not used. Non-MAIS programs are encouraged to use the IO Capstone Threat Assessment or service produced System Threat Assessment Report as their threat baseline. MAIS programs still need to provide system descriptions, as well as the CIPs and production requirements that are specific to their program's needs.

8.1.3. Threat Validation

As noted above, for Major Defense Acquisition Programs (MDAPs) subject to Defense Acquisition Board review, the Defense Intelligence Agency (DIA) validates System Threat Assessment Reports (STARs) for Acquisition Category (ACAT) ID/ Major Defense Acquisition Programs (MDAPs). STARs for ACAT IC MDAPs and System Threat Assessments for ACAT II programs are validated by the appropriate service. DIA validation assesses the appropriateness and completeness of the intelligence, consistency with existing intelligence positions, and the use of accepted analytic tradecraft in developing the assessments. Working with its partners in the DOD intelligence community and, as needed, in the larger intelligence community, validation is intended to ensure that all relevant data is considered and appropriately used by author(s) of the assessment.

DIA validates threat information contained in Joint Capabilities Integration and Development System documents as described in the JCIDS Manual . When requested by the appropriate authority, DIA may also validate other threat information not contained in the STAR but needed for program development.

8.1.4. Support to Operational Test and Evaluation

The Test and Evaluation Master Plan should define specific intelligence requirements to support program operational test and evaluation. When requested by the appropriate authority in the offices of the Director, Operational Test and Evaluation (DOT&E) or the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DIA, working with the Department of Defense Intelligence Community (DoD IC), will provide additional intelligence support to the operational testing of programs on the annual DOT&E Oversight List. DIA support will not include the validation of specific testing scenarios or the validation of "Blue" (see paragraph 8.1) surrogate systems or platforms, but can include certification that the threat information in the test plan is

correct and consistent with existing assessments.

Per DoD Instruction 5000.02 certain programs on the DOT&E Oversight List are to be considered as MDAPs for testing and evaluation purposes and will require a System Threat Assessment Report regardless of Acquisition Category designation.

8.2. Signature and other Intelligence Mission Data Support

The first step for managers involved with acquisition efforts and programs is to identify any requirement for intelligence analysis related to enabling mission capability. The data derived from this analysis and needed by acquisition programs is commonly referred to as signatures and other IMD. See definitions at Section 8.0.3. Applicability .

Further, Services have liaisons with expertise in both intelligence and acquisitions. These professionals know how to interface with the DoD IC and are typically part of the acquisition team (or are accessible to the team).

DoD Directive 5250.01 , Management of Signature Support Within the Department of Defense, establishes the Signatures Support Program (SSP) (previously known as the National Signatures Program (NSP)) to manage and execute the DoD Signature Support Mission (SSM). Signatures are essential for building target models, developing algorithms, optimizing sensor design, and validating sensor functionality. The PM should account for signatures during system and sensor acquisition.

The PM documents detailed signature requirements in a Life-cycle Signature Support

Plan (LSSP) (per DoD Directive 5250.01) and defines overall signature support requirements and compliance with signature standards in the Capability Development Document and Capability Production Document (per CJCS Instruction 3312.01 , "Joint Military Intelligence Requirements Certification"). Under CJCS Instruction 3312.01, the SSP uses the LSSP to assess the ability of the signatures community to support a program's signature requirements.

8.2.1. Signature and other Intelligence Mission Data support in the Technology Development Strategy (TDS)

DoD Directive 5250.01 requires that signature support requirements and funding be incorporated into a program's acquisition strategy. Per PDUSD AT&L Memo, 20 APR 2011 Document Streamlining Program Strategies and Systems Engineering Plan, the TDS should provide a table that indicates the program life-cycle signature support requirements. Life-cycle signature support funding requirements will be reflected in the TDS program funding summary. [Technology Development Strategy Memo] If required signatures are not already available in the distributed national signatures pool, the program will need to plan and budget for development of these signatures. Stating in the TDS that a program is signature dependent and will identify requirements in a Life-cycle Signature Support Plan ensures that the Program Office has considered signature development resource needs in the program planning and budgeting process.

8.2.2. Distributed DoD Signatures and other Intelligence Mission Data Pool and Standards

DoD Directive 5250.01 requires that all signatures provided for the DoD be made available through a distributed DoD signature pool and adhere to established standards. Whether developed by a government signature center or by a contractor, if the signatures and other IMD are made available through a distributed pool, they can be shared to prevent duplication of work and cost across the DoD.

An essential element to make this possible is the use of standards to ensure common meta-data tags and processing methods are used. This in turn ensures the signatures will be discoverable in the distributed pool and that the signatures will be usable for multiple customer’s including acquisition programs and operational systems.

The Signatures Support Program provides single access point connectivity to the distributed pool through web-pages on JWICS (http://ssp.dodiis.ic.gov/), SIPRNet (http://dt.dia.smil.mil/ssp), and NIPRNet (site under development). (**NOTE:** These sites cannot be accessed via the Internet or Non-secured Internet Protocol Router Network.) Current signature standards are also available at these web-sites.

8.2.3. Intelligence Mission Data (IMD) Support

DoD Directive 5250.01, Management of Signature Support Within the Department of Defense, requires all signature-dependent technology and acquisition programs and

efforts to submit a Life-cycle Signature Support Plan (LSSP) throughout their respective lifecycle. An LSSP is intended to facilitate collaboration and agreement between the acquisition, requirements and intelligence communities regarding signatures, also known as Intelligence Mission Data (IMD), which is DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment including, but not limited to the following functional areas: Intelligence Signatures, Electronic Warfare Integrated Reprogramming (EWIR), Order of Battle (OOB), Characteristics and Performance (C&P), and Geospatial Intelligence (GEOINT).

Technology initiatives and weapons systems design, development, test, evaluation, operation and sustainment increasingly rely on signatures and other Intelligence Mission Data to meet expected capability. The identification of required data type, conditions, fidelity, precision, etc., often evolves as the technology and systems mature. Additionally, the intelligence community must constantly respond to these requirements in an ever changing environment as threats, targets, and systems evolve over time. For these reasons developing an LSSP must be initiated early in a programs lifecycle to establish an effective and efficient flow of communication and actions to ensure timely support for IMD requirements.

The LSSP defines specific technology and program IMD requirements. The DAU LSSP webpage provides an LSSP template, instructions for LSSP completion, an LSSP Signature Requirements Table template, and an example Contract Data Requirements List form for procuring signature data. The LSSP Template provides an outline and guidance that standardizes communication between the technology or program offices and the intelligence community. The LSSP should contain as much detail as possible to inform intelligence community production and collection decisions. Therefore, increasing detail should be provided in each update and submission of the LSSP. Content considerations for an LSSP by phase and milestone can be found below.

8.2.3.1. Materiel Solution Analysis Phase to Milestone A

In accordance with DAG Chapter 2, a programs strategy document (Technology Development Strategy (TDS)) should identify the (a) systems and subsystems of the program that require intelligence mission data necessary to deliver the intended capabilities; and (b) IMD funding requirements as appropriate. The TDS should refer to the programs LSSP for a listing of the actual IMD requirements and additional detail.

Since final material solutions are yet to be approved prior to Milestone A, specific system configuration and detailed signature requirements are generally not known. However, based on the intended operational mission, the program should identify the IMD type(s) (e.g. Radar, Thermal, Acoustic, EWIR, GEOINT etc.) the domain (e.g. Space, Air, Land, Naval, Missile Defense, etc.), data fidelity (e.g. queuing quality), and possibly sub-categories within a domain (e.g. for Air: Fighter Aircraft) for each subsystem that requires the data. To the level that specific requirements are known, they should be stated.

IMD requirements and related implications to design, performance, and test & evaluation, will be accounted for and considered throughout the Materiel Solution Analysis Phase. Relevant questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed material solution identified during the Analysis of Alternatives (AoA) process, will the solution require the detection and identification of an activity, event, person, material, or equipment? If yes, then for each proposed detection or identification method (radar, EO/IR, acoustic, chemical, etc.), assess the technical feasibility of acquiring IMD within cost and schedule constraints. Consider the quality of available IMD, the ICs capability to deliver IMD and whether the IMD needs to be collected, processed and/or developed.

Actions:

- During development of the preliminary system specification, identify which system functions will likely drive the need for IMD, either directly or through derived requirements.
- During development of mission and functional threads, identify potential IMD requirements for inclusion in the LSSP.
- During development of Test and Evaluation strategies and plans, identify IMD requirements based on the need to verify and validate detection and identification functionality. Characterize associated technical risk in the Test and Evaluation Strategy . Estimate IMD delivery requirements to meet projected test schedules.

8.2.3.2. Technology Development Phase to Milestone B

As a program approaches Milestone B (MS B), the LSSP must include mission or capability specific details and IMD requirements to support program development. For example, as the design matures, additional details should emerge about the design of the sensors and the algorithms. The LSSP should also identify any IMD-based models and intelligence production requirements (PRs) already submitted to a Service Intelligence Production Center (NASIC, NGIC, ONI, MSIC, etc.), other IMD production efforts (e.g. lab, warfare research center, or other agency, organization, etc.), and planned IMD collection events that the program will conduct.

Based on initial IMD requirements defined for Milestone A, refine and add details for the MS B LSSP during development of the Systems Performance Specification and the Allocated Baseline. Relative questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed detection/identification method (radar, Electro Optical/Infra-Red (EO/IR), acoustic, chemical, etc.), does the required IMD (signature, EWIR, GEOINT, OOB, C&P) already exist (at the estimated quality needed) or will it need to be processed, produced, or collected?
- Is the required detection/identification technology sufficiently mature (Technology Readiness Level 6 or higher) to proceed into end-item design or Milestone B?
- Which IMD-dependent performance requirements need to be verified through test and evaluation?
- Does the program have IMD requirements derived from Modeling and Simulation activities?
- Can the estimated IMD processing, production, collection be completed within required cost and schedule?
- Do the detection/identification algorithms or processes need to be designed to accommodate IMD updates?
- Is there potential for the detection/identification hardware and software to perform IMD collection and provide updates to IMD databases? If yes, has a design study been conducted to assess feasibility and cost/benefit analysis?
- Have significant IMD-dependent functions been included in the proposed exit criteria for the Engineering & Manufacturing Development (EMD) Phase?
- Has the programs spectrum requirements taken into account bandwidth needed for IMD updates during system operations and sustainment?
- Should any IMD data sets be considered as GFE for the EMD Contract?

Actions:

- During the functional allocation process, conduct sensitivity analyses on IMD level of quality (e.g. resolution, frequency range, etc.) to assess quality of available data versus required quality to meet performance KPPs/KPAs.
- Define system level functional and performance requirements derived from items such as: Concept of Operations, system-level performance metrics, mission threads/use cases, and usage environment. Document results and requirements in the System Requirements Document (SRD), LSSP, and Systems Engineering Plan (SEP) as appropriate.
- Assess IMD requirements and schedule relative to DOT&E needs. Document results in the LSSP and by reference in the Test and Evaluation Master Plan (TEMP) .

8.2.3.3. Engineering & Manufacturing Phase to Milestone C

This LSSP will be an update to the previous LSSP. The purpose is to add any new IMD requirements resulting from design maturity or changes in the Concept of Operations

(CONOP). It should identify the expected IMD production support and concept necessary for system employment in an operational environment. The LSSP should include information on IMD data existing within the program (modeling and simulation or measured physical parameters) for sensor or algorithm development or for testing purposes, and; information on the existence of any blue IMD collected to support the program. Additionally, the IMD production concept must be defined and coordinated with the intelligence community. At a minimum this should include the identification of organizations for the production of IMD, addressing responsible entities for adversary commercial systems, and US systems (blue). This information is required to ensure that this form of IMD is available through the DoD data sources.

Based on IMD requirements defined in the Milestone B LSSP, refine and add details for the MS C LSSP during development of the System Functional Spec and the Initial Product Baseline. Relevant questions to consider and actions to take during this phase include:

Questions:

- Has the program been identified for Foreign Military Sales (FMS)? If yes, then how will this effect design, development, testing, disclosure and releasability of IMD-dependent components?
- For each proposed detection/identification method (radar, EO/IR, acoustic, chemical, etc.), has IMD (signature, EWIR, GEOINT, OOB, C&P) required for system operations and sustainment been accounted for in the LSSP and Acquisition Plan, at the level of quality needed?
- Which IMD requirements need to be verified in Follow-on test and evaluation (FOT&E)?

Actions:

- Determine IMD-related schedule events (need date from Intelligence Production Center, algorithm or sensor critical test-related dates, etc.) for inclusion in the System Technical Schedule within the SEP.
- Assess IMD-related functions for inclusion in Risk Management assessments in the SEP.
- Assess IMD requirements and schedule relative to FOT&E needs. Document results in the LSSP and by reference in the updated TEMP .

8.2.3.4. Low-Rate Initial Production to Full-rate Production/Full Deployment Decision Review (FRP-DR) to Disposal

In preparation for IOC, an LSSP update is required to ensure congruence with the Final Production Baseline and to fully account for required operational signatures based on the latest threat assessments and CONOPS for the system. This LSSP also needs to fully account for IMD sustainment plans including identification of processes and data sources which are essential for system operations, such as: IMD production processes;

IMD databases; IMD verification and validation for operational use; processes and systems which support development and dissemination of IMD data loads for operational missions.

This LSSP requires COCOM coordination and identification of COCOM processes for updating and fulfilling IMD requirements during operation and sustainment of the system. Relevant questions to consider and actions to take during this phase include:

Questions

- For FMS versions of the system, have IMD-dependent components been verified for release and approved by the Designated Disclosure Authority?
- Have IMD support requirements been included in the Life-cycle Sustainment Plan and the Product Support Package?
- Does the current CONOPS for the system drive new or updated IMD requirements? Have these new/updated IMD requirements been handed off to the COCOM requirements prioritization process?
- If the operational system has an IMD reprogramming process, is the reprogramming system and organization ready for operations?

Actions

- Coordinate the LSSP with the systems COCOM.
- Confirm operations of the IMD reprogramming process.

8.2.4. Life-cycle Signature Support Plan (LSSP) Assessment

Each LSSP is assessed to identify existing signature holdings, requirements, standards, collection events, technologies and associated cost estimates relative to the program. As a result, a custom assessment is provided to the PM to use in planning signature collection, development, and processing to ensure signatures and other IMD are available in time to meet system design and delivery schedules .

8.3. Support to the Intelligence Certification Process

8.3. Support to the Intelligence Certification Process

The Joint Staff provides review, coordination, and certification/endorsement functions in support of the Joint Capabilities Integration and Development System (JCIDS) process. These functions include intelligence supportability for intelligence certification and threat validation. All acquisition programs or capabilities that are expected to operate in a threat environment must be developed in accordance with the most current threat information. Per CJCS Instruction 3312.01 , the applicable threat information must be continually updated to account for threats throughout the program or capability's projected acquisition life cycle. DIA's Defense Warning Office (DIA/DWO) will assist sponsors with incorporating adversarial threat capabilities throughout the JCIDS review

process, and will review and validate the threat input within the JCIDS documents. Threat sections should not include non-adversarial, natural events as threats to capabilities or systems.

Initial Capabilities Document (ICD) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated Capstone Threat Assessments (CTAs) or System Threat Assessment Reports (STARs)/System Threat Assessments (STAs) are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. The ICDs reference the threat documents used to support the analysis.

Capability Development Document (CDD) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. Programs designated as ACAT-ID MDAPs, or programs with the potential to be so designated, must use DIA-validated threat references.

Capability Production Document (CPD) . The initiating DOD Component prepares a concise threat summary and threat rationale, working with DIA/DWO as needed. If validated CTAs or STARs/STAs are available and address the threat areas affecting the U.S. capability, these documents should be used as the primary sources for the threat statements. Programs designated as ACAT ID MDAPs, or programs with the potential to be so designated, must use DIA-validated threat references.

Information Support Plan (ISP). Per DoDI 4630.8 and CJCSI 3312.01B, DIA/DWO reviews program generated ISPs during the Intelligence Certification process. A threat summary or section is not required in the ISP format; however, if used should reference the current and applicable CTA or STAR/STA.

Additional Criteria . The certification also evaluates intelligence-related systems with respect to open system architecture, security, and intelligence interoperability standards. (J-6 Interoperability certification is conducted in a separate, but related process, and is documented in CJCS Instruction 6212.01 .)

Those personnel with a SIPRNET terminal can access the specific procedures and criteria for the Intelligence Certification on the Intelligence Requirements Certification Office homepage (under "Certification Process"). By telephone, additional information may be obtained by calling the Intelligence Requirements Certification Office at 703-571-9543 (Mr. Vernon Wilson) or 703-571-9541 (Mr. Dana Smith).

DEFENSE ACQUISITION GUIDEBOOK
Chapter 9 - Test and Evaluation (T&E)

9.0. Overview

9.0.1. Purpose

This chapter supplements direction and instruction in DoDD 5000.01 and DoDI 5000.02 with processes and procedures for planning and executing an effective and affordable T&E program in the DoD acquisition model. A rigorous and efficient T&E program provides early knowledge of developmental and operational issues. Correcting these issues early enough can mitigate risks of cost overruns and schedule slippages, and can ultimately contribute to delivery of effective and suitable weapons, information technology (IT) and National Security Systems (NSS) to the Warfighters in a timely manner. The principles and practices in this chapter apply to all acquisition programs regardless of size or cost; however, some aspects focus on acquisition programs of sufficient interest, cost, size, complexity, or need for interoperability, requiring oversight by the Office of the Secretary of Defense (OSD): the OSD T&E Oversight List.

9.0.2. Contents

Section 9.1 OSD T&E Organization provides a guide to OSD organizations having roles

in the accomplishment or overseeing the DoD T&E mission.

Section 9.2 Service-level T&E Management identifies the top level management structure for the Services and the Major Range and Test Facilities Base (MRTFB).

Section 9.3 Test and Evaluation describes the different types of T&E and test events.

Section 9.4 Integrated Test and Evaluation defines integrated testing and describes how all areas within T&E utilize Integrated Testing.

Section 9.5 T&E Planning describes actions needed to develop an Evaluation Plan, Test and Evaluation Strategy (TES), Test and Evaluation Master Plan (TEMP), and test plan.

Section 9.6 T&E Reporting describes actions and documentation needed to report T&E results and evaluations.

Section 9.7 Special Topics addresses T&E programs deviating from the DoDI 5000.02 Defense Acquisition System model (e.g., associated with urgent needs programs, defense business systems, National Security Systems (NSS), etc.).

Section 9.8 Best Practices presents examples of best practices to improve planning, execution, and reporting of T&E.

Section 9.9 Prioritizing Use of Government Test Facilities for T&E provides information on the mandate to use Government test facilities for T&E.

Throughout this chapter, interpret the terms developmental and operational as broad statements of the types of testing or evaluation, and not as the testing controlled by a particular organization.

9.1. OSD T&E Organization

The Director of Operational Test and Evaluation (DOT&E) for operational test and evaluation (OT&E) and live fire test and evaluation (LFT&E), and the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) within the office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E))

in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) provide oversight and policy for T&E of certain acquisition programs within OSD. The DASD(DT&E) also serves as the Director, Test Resource Management Center (TRMC) and has responsibility for oversight of DoD T&E resources and infrastructure. By law, DASD(DT&E) closely coordinates with Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), and routinely coordinates with other OSD organizations, such as Cost Assessment and Program Evaluation (CAPE).

DOT&E and DASD(DT&E) share or coordinate on the following responsibilities:

- Prescribe policies and procedures for the T&E within the DoD
- Provide advice and make recommendations to the Secretary of Defense (SecDef),Deputy SecDef (DepSecDef), and USD(AT&L); as well as support Overarching Integrated Product Teams (OIPTs) and Defense Acquisition Boards/Information Technology Acquisition Boards for programs on the OSD T&E Oversight List
- Develop, in consultation with the DoD Components, the OSD T&E Oversight List
- Ensure the adequacy of T&E strategies and plans for programs on the OSD T&E Oversight List
- Ensure DoD Components do not terminate or substantially reduce participation in joint Acquisition Category (ACAT) ID or ACAT IAM programs without Requirements Authority review and USD(AT&L) approval
- Attend systems engineering technical reviews
- Monitor and review DT&E, OT&E, and LFT&E events of oversight programs
- Participate in the operational test readiness review (OTRR) process by providing recommendations concerning a systems readiness for operational testing
- Provide independent performance, schedule, and T&E assessments to the Defense Acquisition Executive Summary (DAES) process
- Provide representatives to the T&E working-level integrated product team (T&E WIPT) for oversight programs to assist program managers (PMs) in developing their strategy as well as preparing a TES / TEMP

9.1.1. OSD T&E Oversight List

The DOT&E and the DASD(DT&E), jointly, and in consultation with the DoD Component T&E executives and other offices as appropriate, publish an annual OSD T&E Oversight List . DOT&E and the DASD(DT&E) designate programs for DT&E, OT&E, and/or LFT&E oversight. They consider all programs for inclusion, regardless of ACAT level, and can add to or delete from the list at any time during the year. OSD considerations for inclusion on formal T&E oversight include:

- ACAT level
- Potential for Joint designation
- Potential for establishment as an acquisition program (such as Technology Projects identified in Enclosure 3 of DoDI 5000.02 or a pre-Major Defense

Acquisition Program (MDAP))
- Stage of development or production
- Potential for DAES reporting
- Congressional and/or DoD interest
- Programmatic risk (cost, schedule, or performance)
- Past programmatic history of the developmental command
- Relationship with other systems as part of a system-of-systems (SoS)
- Technical complexity of system

9.1.2. Director of Operational Test and Evaluation

The DOT&E, a Principal Staff Assistant and advisor to the Secretary of Defense, has specific responsibilities as identified in DoDD 5141.02 , "Director of Operational Test and Evaluation", dated February 2, 2009. Sections 139 and 2399 of title 10 USC prescribe the duties for OT&E and section 2366 of title 10 USC for LFT&E . For additional information on the DOT&E office, visit the DOT&E website . For purposes here, DOT&E:

- Prescribes policies and procedures for the conduct of OT&E and LFT&E for DoD.
- Assesses the adequacy of OT&E and LFT&E performed by the Services and operational test agencies (OTAs) for programs on the OSD T&E Oversight List, for their effectiveness and suitability for advising the USD(AT&L) as well as for reporting to the SecDef and Congress.
- Advises the DoD Executive Agent for Space and the acquiring Military Department on T&E of DoD Space MDAPs and other space programs designated for T&E oversight, in support of DoDD 3100.10 Space Policy, dated July 9, 1999.
- Manages:
    - The efforts to improve interoperability and information assurance (IA) through the operational evaluation of the systems under oversight and major exercises conducted by the Combatant Commands and the Military Departments.
    - The Joint Test and Evaluation (JT&E) Program .
    - The Joint Live Fire Program.
    - The Center for Countermeasures .
    - The activities of the Joint Aircraft Survivability Program .
    - The activities of the Joint Technical Coordinating Group for Munitions Effectiveness and producing the Joint Munitions Effectiveness Manual.
    - The activities of the T&E Threat Resource Activity .
- Provides support to the Director, Joint Improvised Explosive Device Defeat Organization (JIEDDO), consistent with DoDD 2000.19E Joint Improvised Explosive Device Defeat Organization (JIEDDO), dated February 14, 2006.
- Assists the Chairman of the Joint Chiefs of Staff (CJCS) in efforts to ensure the Joint Capabilities Integration and Development System (JCIDS) documents, in terms verifiable through testing or analysis in support of CJCS Instruction 3170.01 Joint Capabilities Integration and Development System, dated March 1,

2009, provides the expected joint operational mission environment, mission level measures of effectiveness (MOEs), and key performance parameters (KPPs).
- Oversees and assesses operational capability demonstrations conducted by the Missile Defense Agency, consistent with DoDD 5134.09 Missile Defense Agency (MDA), dated September 17, 2009.
- Establishes policy on the verification, validation, and accreditation (VV&A) of models and simulations used in support of OT&E and LFT&E.
- Oversees the International T&E (IT&E) program for the SecDef.
- Oversees and prescribes policy, as appropriate, to ensure adequate usage and verification of protection of human subjects and adherence to ethical standards in OT&E and LFT&E; in support of DoDD 3216.02 Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research, dated November 8, 2011.

9.1.3. Deputy Assistant Secretary of Defense for Developmental Test and Evaluation

As an advisor to the USD(AT&L) for DT&E through ASD(R&E), the DASD(DT&E) has responsibilities and duties as prescribed in section 139b of title 10 USC . For additional information on DASD(DT&E), visit the ODASD(DT&E) website. For purposes here, the DASD(DT&E):

- Develops policies and guidance:
  - For the conduct of DT&E in the DoD (including integration and developmental testing of software).
  - In coordination with the DOT&E, for the integration of DT with OT.
  - For the conduct of DT&E conducted jointly by more than one Component or Defense Agency.
  - In coordination with DASD(SE), ensure the full integration of DT&E activities of the DoD into and consistent with the SE and developmental planning processes of the Department.
- Monitors and reviews the DT&E activities of the MDAPs, including approval of the TEMP and TES.
- Reviews and approves the DT&E plan within the TEMP for each DoD MDAP.
- Develops DT&E technical workforce, by providing advocacy, oversight, and guidance to elements of the acquisition workforce responsible for DT&E.
- Periodically reviews the organizations and capabilities of the Components and Defense Agencies with respect to DT&E; identifies needed changes or improvements to such organizations and capabilities; and provides input regarding needed changes or improvements to the strategic plan for DoD T&E resources.

Additionally, the DASD(DT&E) functions as Director, TRMC ; a field activity reporting directly to the USD(AT&L). DoDD 5105.71 , Department of Defense Test Resource Management Center (TRMC), dated March 8, 2004, states TRMC shall plan for and assess the adequacy of the Major Range Test Facility Base (MRTFB) . . . to provide

adequate testing in support of development, acquisition, fielding, and sustainment of defense systems; and, maintain awareness of other T&E facilities and resources, within and outside the Department, and their impacts on DoD requirements. The above directive also provides the specific responsibilities of the TRMC.

TRMC provides reports and recommendations on current and projected MRTFB infrastructure issues to ensure adequate capabilities and resources exist to support testing of DoD acquisition programs in accordance with responsibilities found in DoDD 3200.11 Major Range and Test Facility Base (MRTFB), December 27, 2007.

9.2. Service-Level T&E Management

9.2.1. Program Managers

9.2.2. T&E Board of Directors (BoD(ES))

9.2.3. Component and Joint T&E Organizations

9.2.3.1. Defense Information Systems Agency (DISA) T&E Executive (TEO)

9.2.3.2. Assistant Deputy Under Secretary of the Army for Test & Evaluation (ADUSA(T&E))

9.2.3.3. Director, Air Force Test & Evaluation (AF/TE)

9.2.3.4. Department of the Navy Test & Evaluation Executive (OPNAV N091)

9.2.4. Office of the Secretary of Defense T&E Management

9.2.4.1. Developmental Test & Evaluation

9.2.4.2. Operational Test & Evaluation

9.2.5. Major Range and Test Facility Base

9.2. Service-Level T&E Management

9.2.1. Program Managers

Ultimately, management responsibility for an acquisition programs T&E resides with the PM. However, the planning, executing, and reporting of T&E involves interactions, support, and oversight from other organizations within OSD, the Services, Defense Agencies, and in some cases, other government agencies; as well as the system contractor(s). The PM charters a T&E WIPT early in the acquisition model to support development of test strategies and estimates of resource requirements, strengthening the overall input to the programs integrated product team (IPT). For additional

information, consult Rules of the Road A Guide for Leading a Successful Integrated Product Team , October 1999.

The PM, in concert with the user and the T&E community, coordinates DT&E,

OT&E, LFT&E, family-of-systems (FoS) interoperability testing, IA testing, reliability and maintainability (RAM) growth testing (DTM 11003 , Reliability Analysis, Planning, Tracking, and Reporting, dated December 2, 2011), and modeling and simulation (M&S) activities, into an efficient continuum, closely integrated with requirements definition and systems design and development. The PM has responsibility for the development and final approval of the TEMP that effectively describes the overall strategy for T&E supporting the programs acquisition strategy and Systems Engineering Plan (SEP) , and the resources necessary to execute the test program. MDAP/MAIS programs and programs identified as being on OSD T&E Oversight List require Component level approval and OSD approval by DASD DT&E for programs on DT&E oversight and DOT&E for programs on OT&E and/or LFT&E oversight. For a program requiring LFT&E in accordance with section 2366 of title 10 USC , the PM must ensure timely submission of waivers and alternative plans to meet SecDef obligations to advise Congress of any deviations from full up, system level (FUSL) LFT&E requirements. All MDAP/MAIS programs should identify key leadership positions (KLPs) early in the acquisition process. An early charter for a T&E WIPT proves essential to the success of a test and evaluation program.

9.2.2. T&E Board of Directors (BoD(ES))

Acting as the agent for the Service Vice Chiefs and equivalent OUSD and Defense Agency representatives with T&E management responsibilities is the BOD Executive Secretariat (BOD(ES)), consisting of the Service T&E principals and equivalent OUSD and Defense Agency representatives with T&E infrastructure management responsibilities. The BOD(ES):

- Endorses guidance and policy for T&E infrastructure and investment management to ensure a disciplined test process that supports weapon, IT & NSS system acquisition and operational, safety, suitability, and effectiveness assessments with a cost-effective infrastructure.
- Supports program review and advocacy for T&E capabilities and requisite infrastructure to OSD and Congress.
- Endorses the T&E Executive Agent Test Resources Master Plan.
- Approves and directs studies in support of T&E infrastructure management, standards, policy, configuration and investments.
- Endorses T&E infrastructure standards that promote interoperability and commonality among test centers and ranges.
- Endorses processes for workload measurement, forecasting, utilization, and full cost visibility application to T&E infrastructure investments and other related decisions.
- Endorses principles of T&E Reliance (joint OSD and individual Services efforts to

maximize commonality, interoperability, and effective utilization of products and services in support of the T&E infrastructure).
- Approves joint T&E requirements and recommends solutions from the needs and solutions process for the Central T&E Investment Program (CTEIP) consideration.
- Serves as the T&E representatives on the OSD chartered Defense Test and Training Steering Group (DTTSG).

9.2.3. Component and Joint T&E Organizations

9.2.3.1. Defense Information Systems Agency (DISA) T&E Executive (TEO)

The DISA T&E Executive serves as the Test, Evaluation, and Certification (TE&C) subject matter expert and Special Advisor to the DISA Director, DISA, and Senior Executive Leadership. The DISA T&E Executive duties and responsibilities include:

- Establishing and providing oversight of DISAs overarching TE&C strategies, policies, and procedures as well as missions and functions.
- Coordinating accomplishment of TE&C goals and investment strategies with DISAs Joint Interoperability Test Command (JITC) , program executive officer (PEOs), and PMOs for the development and management of the DISA T&E Resource Management Plan.
- Providing oversight of DISA TE&C missions and functions, to include formulation of overarching T&E strategies, policies, and program direction.
- Providing policy oversight and resource management.
- Publishing and enforcing TE&C policies and guidance related to agency acquisition programs and projects, examines TE&C strategies to ensure consistent application of sound agile TE&C strategies, methodologies, and processes.
- Providing TE&C oversight and support for the agency in the development of program documentation (e.g., TES and TEMP) to ensure governance, construct, infrastructure, and operations satisfy legal and regulatory requirements for adequate TE&C. Functions as the final TE&C review authority and signatory for TEMPs prior to Component Acquisition Executive (CAE) and OSD approval and signature.
- Leading internal and external transitional TE&C concepts and methodologies to ensure agile, mission capabilities-based, and Warfighter-relevant processes for IT Systems and Services for the agency and DoD.
- Representing the agency to the DoD T&E community, ensuring alignment with the OSD and Joint Staff as a member of the T&E BoD(ES) and as a voting member of the Military Communications-Electronics Board (MCEB) Interoperability Policy & Certification Panels (IP/ICP) as well as other OSD TE&C advisory working groups.
- Providing oversight and development of Agency's TE&C career management plan for recruiting, training, and retaining a professional TE&C workforce. Serves

as the track manager for the DAWIA T&E component.

9.2.3.2. Assistant Deputy Under Secretary of the Army for Test & Evaluation (ADUSA(T&E))

Within the Army, the T&E Executive is the Director, T&E Office under the authority, direction, and control of the Deputy Under Secretary of the Army. Key Army T&E Executive duties and responsibilities include:

- Serving as the senior advisor to the Secretary of the Army and the Chief of Staff, Army, on all Army T&E matters.
- Advising the Army Systems Acquisition Review Council (ASARC), the Army Requirements Oversight Council (AROC), and OIPTs on T&E matters.
- Approving test-related documentation for the Secretary of the Army and forwards, as appropriate, to OSD.
- Coordinating T&E matters with the Joint Staff and OSD, to include serving as principal Army interface on matters of T&E with the USD(AT&L) and DOT&E.
- Overseeing all Army T&E missions and functions, to include formulating overarching Army T&E strategy, policy, and program direction, providing policy oversight, and managing resources.
- Providing HQDA oversight on the funding of the Army Threat Simulator Program , Army Targets Program , and Army Instrumentation Program ; and coordinate with the Project Manager for Instrumentation, Targets, and Threat Simulators (PM ITTS).
- Overseeing Army responsibilities in Joint T&E, Foreign Comparative Testing (FCT), and multi-Service and multinational T&E acquisition programs.
- Serving as the Acquisition Workforce Functional Chief for the T&E acquisition workforce Career Field.

9.2.3.3. Director, Air Force Test & Evaluation (AF/TE)

The Air Force T&E Executive serves as the Director, Air Force Test and Evaluation (AF/TE), who serves under the authority and direction of the Secretary of the Air Force (SECAF) and the Chief of Staff of the Air Force (CSAF). In this capacity, the AF/TE:

- Functions as the sole focal point for Air Force T&E policy, guidance, direction, and oversight for the formulation, review, and execution of T&E plans, programs, and budgets.
- Functions as the chief T&E advisor to senior Air Force leadership on T&E processes; DT&E, including contractor testing and LFT&E; OT&E; and the use of M&S in T&E.
- Functions as the final T&E review authority and signatory for TEMPs prior to CAE and OSD approval and signature.
- Collaborates with requirements sponsors and system developers to improve operational requirements, system development, and the fielding of operationally effective, suitable, safe, and survivable systems.

- Reviews and/or prepares T&E information for timely release to OSD, Congress, and decision makers.
- Oversees the Air Force T&E infrastructure by determining the adequacy of T&E resources required to support system acquisition activities. Administers various T&E resource processes and chairs or serves on various committees, boards, and groups supporting T&E activities.
- Acts as the single point of entry for the Air Force Foreign Materiel Program.
- Manages the Air Force Joint Test & Evaluation Program according to DoDI 5010.41 Joint Test and Evaluation (JT&E) Program, dated September 12, 2005.
- Functions as the certifying authority for T&E personnel for T&E Level 3 in the Acquisition Professional Development Program (APDP) when not delegated to the Major Commands (MAJCOMs).

9.2.3.4. Department of the Navy Test & Evaluation Executive (OPNAV N091)

The Director, Test and Evaluation and Technology Requirements (OPNAV N091) serves as the Department of Navy (DON) T&E Executive. The DON T&E Executive reports to the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and the Principle Military Deputy to the Assistant Secretary of the Navy for Research, Development, and Acquisition (PMD ASN (RDA)) on all matters pertaining to test and evaluation.

The DON T&E Executive supports and advises the Vice Chief of Naval Operations (VCNO) regarding the VCNOs role on the T&E BOD and serves as the Navy representative on the T&E BOD Executive Secretariat.

The Director, Test and Evaluation and Technology Requirements (N091):

- Approves all Navy Test and Evaluation Master Plans for CNO.
- Establishes Navy T&E requirements and promulgates policy, regulation, and procedures governing Navy T&E.
- Acts for CNO in resolving T&E requirements.

9.2.4. Office of the Secretary of Defense T&E Management

9.2.4.1. Developmental Test & Evaluation

Statute and policy prescribes the management of DT by the DASD(DT&E), who, for all programs on DT oversight, acts as the final approval authority for DT planning in the TEMP. ODASD(DT&E) staff representatives actively participate in acquisition program T&E WIPTs and provide advice to the T&E WIPT and PM; as well as providing independent assessments to DASD(DT&E) on progress of performance of the test program and overall performance of the system. By statute, the DASD(DT&E) has access to all test data and program information relevant to the execution of testing and fulfillment of the ODASD(DT&E) responsibilities. As a member of the OIPT, the DASD(DT&E) provides advice and recommendations at Defense Acquisition Board

(DAB), reviews and submits an independent Assessment for Operational Test Readiness (AOTR) to the Component Acquisition Executive (CAE) and USD(AT&L) for all programs on DT oversight prior to the CAE decision on material readiness for initial operational test and evaluation (IOT&E).

The PM should initiate early engagement with the ODASD(DT&E) and charter a T&E WIPT to aid in development of test strategies and building a TEMP. Given that DT spans the entire lifecycle of an acquisition program and remains a vital part of all levels in the work structure of the systems engineering process, DASD(DT&E) expects due diligence from the PMs to ensure they base program and design decisions on test results conducted and reported as independent verification steps in the process, and not simply pulled from design and test learning processes. This effort requires close and continuous coordination with the SEP, Information Support Plan (ISP), and developing activity engineering and test activities to ensure test plans and reports reflect independent evaluation of the test data from the engineering staff vested in the development activities.

Ideally, the PM bases all development decisions on test events and not schedules or costs; but in the pragmatic environment of developing systems for the Warfighter, time and cost prove significant drivers in pressuring test activities. Therefore, DT activities must provide realistic T&E schedules to PMs during the establishment of the programs integrated management schedule. This effort ensures the effective management of the overall progress and cost of the program; particularly with complex systems that have a number of dependent sub systems and technologies requiring efficient integration as an end product.

As such, the DASD(DT&E):

- Develops policies and guidance for the planning, execution, and reporting of DT&E in the DoD, according to section 139b of title 10 USC .
- Develops policies and guidance for the integration of DT and OT, in coordination with DOT&E.
- Publishes, in conjunction with DOT&E, a combined list of OSD T&E Oversight programs for DT&E, OT&E, and LFT&E.
- Monitors and reviews the DT&E activities of MDAPs and other programs.
- Periodically conducts AOTRs.
- Provides advocacy, oversight, and guidance to the acquisition workforce responsible for test and evaluation.
- Reviews and approves TES/TEMPs and selected DT&E plans.
- Periodically reviews the Services organizational DT&E capabilities to identify needed changes or improvements.

9.2.4.2. Operational Test & Evaluation

By law, DOT&E prescribes policies and procedures for the conduct of OT&E in the Department of Defense. For programs on DOT&E OT oversight, DOT&E serves as the

final approval authority for OT&E planning to include approval of the TEMP. DOT&E staff representatives actively participates in acquisition program T&E WIPTs and provide advice to the T&E WIPT and PM; as well as providing independent assessments to the DOT&E on progress of performance of the test program and overall performance of the system. By law, DOT&E has access to all data and records DOT&E considers necessary to review in fulfillment of DOT&E OT&E responsibilities. DOT&E serves as a member of both the Joint Requirements Oversight Council and the OIPT, providing advice and recommendations at DAB reviews; and has direct access to both USD(AT&L) and the SecDef, on all matters relating to operational test and evaluation.

The PM should initiate early engagement with DOT&E through the Service and Defense Agency T&E Executive and independent OTA and charter a T&E WIPT to aid in development of T&E strategies and the TEMP. Since OT&E generally acts as the validation process in SE, early engagement of the OTA and DOT&E, as early as the Analysis of Alternatives and requirements development, ensures a comprehensive assessment of measurability and testability of requirements; and the associated implications to cost and schedule to effectively evaluate the system capabilities and limitations. This requires close and continuous coordination with users, sponsors, developers, and all test activities to ensure understanding and articulation of end-game expectations during program planning and documentation.

Per section 2399 of title 10 USC , an MDAP must complete IOT&E before proceeding beyond full-rate production (FRP). Law also requires DOT&E to provide a Beyond Low-Rate Initial Production (BLRIP) report to the SecDef, USD(AT&L), and congressional defense committees on the adequacy of OT&E conducted; as well as the results of T&E to confirm effectiveness and suitability for combat. Additionally, DoDI 5000.02 charges DOT&E with completing the section 2366 of title 10 USC LFT&E report requirement for submission to the congressional defense committees, SecDef, and USD(AT&L) before the system may proceed to FRP. For purposes of compliance with completion of IOT&E, the PM must ensure the system under test reflect production configured or representative systems, preferably Low Rate Initial Production (LRIP) systems. Title 10 requires DOT&E to determine the number of LRIP systems for all operational testing of programs on DOT&Es OT&E oversight and the Service OTA to determine LRIP requirements for non-OSD T&E oversight programs. DOT&E and the OTAs routinely engage the PM in those decisions. For programs not on the OSD T&E Oversight List, the Service or Defense Agency OTA will work with the PMs for OT&E, including planning, applicable oversight, execution and reporting. Service or Defense Agency OTAs may delegate the responsibilities to other responsible DoD test agencies.

DOT&E approves all OT&E plans, to include early operational assessments (EOAs), OAs, Limited User Tests (LUTs), IOT&E, and Follow-on Operational Test & Evaluation (FOT&E). DOT&E requires the OTAs to provide plans to assess adequacy of data collection and analysis planning to support the operational evaluation of a systems operational effectiveness and operational suitability, since integrated test concepts aid in generating test efficiencies and reduced development time. OTAs must schedule test concept briefings 180 days prior to an operational test. PMs must provide OT&E plans

for DOT&E approval 60 days prior to test events.

In addition to OT&E oversight, the SecDef charges DOT&E with approving waivers to full up system level (FUSL) LFT&E and approval of required alternative LFT&E plans prior to Milestone B.

For programs to effectively track through the complex acquisition process and meet their cost, schedule, and performance goals, it remains essential to engage OSD early, continuously, and to quickly resolve working issues presenting obstacles to any of the T&E stakeholders duties. Service T&E Executives must establish clear issue resolution processes to resolve issues in a timely fashion.

As such, the DOT&E:

- Prescribes OT&E and LFT&E policies for the DoD according to sections 139 , 2366 , 2399 , and 2400 of title 10; and DoDD 5141.2 , Director of Operational Test and Evaluation (DOT&E), dated February 2, 2009.
- Exercises oversight responsibility for ACAT I or other programs in which the SecDef has special interest. Monitors and reviews OT and LF activities in the DoD.
- Participates in integrated test teams and test integrated product teams to foster program success.
- Publishes, in conjunction with the DASD(DT&E), a combined list of OSD T&E Oversight programs for DT, OT, and LF.
- Approves, in writing, the adequacy of operational test plans for those programs on OSD OT&E Oversight prior to the commencement of operational testing. Approves the operational test portions of integrated test plans. Approves the quantity of test articles required for operational testing of major defense acquisition programs (MDAP).
- Approves TEMP and T&E strategies for OSD T&E Oversight programs in conjunction with the DASD(DT&E) and DoD Chief Information Officer (CIO).
- Approves LFT&E strategies and waivers prior to commencement of LFT&E activities.
- Submits a report to SecDef and Congress before systems on OSD OT&E Oversight may proceed BLRIP.

9.2.5. Major Range and Test Facility Base

The DoD, through the TRMC, oversees sustainment of twenty-four T&E organizations or activities with a skilled workforce and T&E technical capabilities and processes, and available to all components under a common charge policy. In accordance with DoDD 3200.11 Major Range and Test Facility Base MRTFB, dated December 27, 2007 and DoDI 3200.18 Management and Operation of the Major Range Test Facility Base (MRTFB), dated February 1, 2010, TRMC manages the following activities:

ARMY ACTIVITIES

White Sands Test Center

High Energy Laser Systems Test Facility

U.S. Army Kwajalein Atoll (Ronald Reagan Ballistic Missile Defense Test Site)

Yuma Test Center

Cold Regions Test Center

Tropic Regions Test Center

West Desert Test Center

Aberdeen Test Center

Electronic Proving Ground

NAVY ACTIVITIES

Naval Air Warfare Center-Weapons Division, Point Mugu

Naval Air Warfare Center-Weapons Division, China Lake

Naval Air Warfare Center-Aircraft Division, Patuxent River

Atlantic Undersea Test and Evaluation Center

Pacific Missile Range Facility

Keyport Pacific Northwest Range Complex (Nanoose and Dabob Ranges)

AIR FORCE ACTIVITIES

45th Space Wing

30th Space Wing

Arnold Engineering Development Center

Nevada Test and Training Range

Air Force Flight Test Center

Utah Test and Training Range

46 th Test Wing, to include 46 th Test Group

DEFENSE-WIDE ACTIVITIES

Defense Information Systems Agency, Information Technology Test bed, to include capabilities in the National Capitol Region

Joint Interoperability Test Command, to include capabilities at Indian Head, MD, and Fort Huachuca, AZ

9.3. Test and Evaluation

DoD employs three formal types of T&E (directed by statute) in the acquisition of weapon systems, business systems, NSS, and joint systems administered by OSD: DT&E, OT&E, and LFT&E. The TRMC, also directed by statute, oversees the MRTFB to ensure availability of capabilities to support the three T&E types. Within these broad categories, the military departments and Defense Agencies have their own directives, guidance, organizations, T&E resources, ranges, and facilities specific to their needs. This section provides distinguishing features of each type.

9.3.1. Developmental Test and Evaluation

Programs conduct DT&E throughout the systems life cycle, from program initiation through system sustainment, to reduce design and programmatic risks and provide assessments. DT&E can occur as either contractor testing or government testing or a mix of both. As such, DT&E:

- Assesses achievement of Critical Technical Parameter(s) (CTPs) and Key System Attribute(s) (KSAs) along with assessment of progress toward achievement of KPPs and Critical Operational Issue(s) (COIs).
- Assesses system satisfaction of the thresholds as described in the capabilities requirements documentation.

- Supports progress toward and final characterization of the system readiness for dedicated IOT&E via the AOTR process and document.
- Characterizes system functionality and provides information for cost, performance, and schedule tradeoffs.
- Assesses system specification compliance.
- Reports progress to plan for Reliability Growth and characterizes reliability and maintainability.
- Identifies system capabilities, limitations, and deficiencies.
- Assesses system safety.
- Assesses compatibility with legacy systems.
- Stresses the system within an intended mission environment.
- Supports the joint interoperability certification process and achieves information assurance certification and accreditation.
- Documents achievement of contractual technical performance and verifies incremental improvements and system corrective actions.

In general, DT&E is the disciplined process of generating experimental performance data from systems, subsystems, components and materiel for the purpose of informing optimum solutions and the state of performance progress toward design performance goals.

Evaluation in the context of DT&E refers to evaluating the generated performance data to ensure it appropriately depicts the performance of the item as tested in the conditions of the test.

Testing in the context of DT&E refers to the process of establishing appropriate conditions and generating performance data from systems, subsystems, components and materiel.

9.3.2. Operational Test and Evaluation

Service and Defense Agency OTAs have a responsibility for OT&E. OT&E determines the operational effectiveness and operational suitability of a system under realistic operational conditions, including joint combat operations; determines the satisfaction of thresholds in the approved JCIDS documents and critical operational issues; assesses impacts to combat operations; and provides additional information on the systems operational capabilities.

OTAs have a responsibility for early involvement in a systems acquisition; for example, EOAs during the Technology Development (TD) phase, OAs during engineering and manufacturing development (EMD) phase, and review of Capabilities Documents to assess measurability, testability, and operational relevancy of requirements in the JCIDS documents (that is, Capability Development Document (CDD) and Capability Production Document (CPD)). OTAs also have responsibility for the assessment and evaluation of systems operational effectiveness, operational suitability, and survivability or operational security completed in IOT&E, and when necessary, Follow-on

Operational Test and Evaluation (FOT&E).

General guidelines for the conduct of OT&E include:

- For dedicated OT&E, typical users operate and maintain the system under test conditions simulating combat and peacetime operations.
- OT&E uses threat or threat representative forces, targets, and threat countermeasures, validated by the Defense Intelligence Agency (DIA) or the DoD Component intelligence agency, as appropriate, and approved by DOT&E during the test plan approval process.
- Conducting IA Testing and evaluation for all weapon, information, and C4ISR programs depending on external information sources, or providing information to other DoD systems.
- Persons employed by the contractor for the system under development may only participate in the OT&E of MDAPs to the extent the PM planned for their involvement in the operation, maintenance, and other support of the system when deployed in combat.
- Testing production representative systems, which include any system accurately representing it's final configuration using mature and stable hardware and software; that accurately mirrors the production configuration, but not produced on a final production line (although production tooling may account for some components).

9.3.2.1. Evaluation of Operational Effectiveness

DoD defines operational effectiveness as the overall degree of mission accomplishment of a system when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, training, doctrine, tactics, survivability or operational security, vulnerability, and threat.

The evaluation of operational effectiveness links to mission accomplishment. The early planning for the evaluation should consider any special test requirements, such as the need for large test areas or ranges or supporting forces, requirements for threat systems or simulators, new instrumentation, or other unique support requirements.

For weapon systems, integrate LFT&E of system lethality into the evaluation of weapon system effectiveness. For example, operational testing could identify likely shot lines, hit points, burst points, or miss distances providing a context for LFT&E lethality assessments. Fuse performance, as determined under DT&E, can provide information for both OT&E and LFT&E assessments.

9.3.2.2. Evaluation of Operational Suitability

Operational suitability defines the degree in which a system satisfactorily places in field use, with consideration given to reliability, availability, compatibility, transportability, interoperability, wartime usage rates, maintainability, safety, human factors, manpower

supportability, logistics supportability, documentation, environmental effects, and training requirements.

Early planning for the operational suitability evaluation should include any special needs for the number of operating hours, environmental testing, maintenance demonstrations, testing profiles, usability of DT&E data, or other unique test requirements.

Operational suitability evaluates a mission context to provide meaningful results. For example, maintaining a required operations tempo over an extended period while conducting realistic missions gives insight into the interactions of various suitability factors.

9.3.2.3. Evaluation of Survivability or Operational Security

Survivability or operational security includes the elements of susceptibility, vulnerability, and recoverability. As such, survivability or operational security acts as an important contributor to operational effectiveness and suitability. All systems under OT&E oversight should receive survivability or operational security assessment if exposed to threat weapons in a combat environment or to combat-induced conditions that may degrade capabilities, regardless of designation for LFT&E oversight. For example, unmanned vehicles may not have a requirement to undergo survivability LFT&E under section 2366 of title 10 USC , but should receive an assessment for survivability or operational security. The assessment may identify issues needing addressed through testing.

Integrate DT&E, OT&E, and LFT&E strategies to ensure the consistent assessment of the full spectrum of system survivability or operational security. The COIs should include any issues needing addressed in the OT&E evaluation of survivability or operational security. Systems under LFT&E oversight must address personnel survivability (reference section 2366 of title 10 USC) and integrate it into the overall system evaluation of survivability or operational security conducted under OT&E.

Generally, LFT&E address vulnerability while OT&E addresses susceptibility, but areas of overlap exist. The evaluation of LFT&E results requires realistic hit distributions. The OT&E evaluation of susceptibility might identify realistic hit distributions of likely threats, hit/burst points, and representative shot lines providing a context for LFT&E vulnerability assessments. DT&E and OT&E testing of susceptibility may provide other LFT&E insights, such as information on signatures, employment of countermeasures, and tactics used for evasion of threat weapons. Similarly, LFT&E tests, such as Total Ship Survivability trials, may provide OT&E evaluators with demonstrations of operability and suitability in a combat environment.

Recoverability addresses the consequences of system damage. Typically, LFT&E addresses recoverability; however, both OT&E and LFT&E have an interest in tests relating to recoverability from combat damage or from peacetime accidents, battle

damage assessment and repair, crashworthiness, crew escape, and rescue capabilities.

LFT&E conducts real time casualty assessment (RTCA) during IOT&E to ensure assumptions supporting the RTCA remain consistent with LFT&E results.

Networked and C3I systems evaluation should include effectiveness of IA and Computer Network Defense (CND) measures against cyber threats in accordance with the DOT&E memo Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs , dated November 4, 2010, and Procedures for Operational Test and Evaluation of Information Assurance in Acquisition programs , dated January 21, 2009.

9.3.3. Live Fire Test and Evaluation

9.3.3.1. Life Fire Test & Evaluation Objectives

9.3.3.2. Covered Systems

9.3.3.3. Early Live Fire Test and Evaluation

9.3.3.4. Full-Up, System-Level Testing and Waiver Process

9.3.3.5. Personnel Survivability

9.3.3. Live Fire Test and Evaluation

9.3.3.1. Life Fire Test & Evaluation Objectives

LFT&E objectives provide a timely assessment of the vulnerability/lethality of a system as it progresses through its design and development, prior to full-rate production. In particular, LFT&E should:

- Provide information to decision-makers on potential user casualties, vulnerabilities, and lethality; taking into equal consideration susceptibility to attack and combat performance of the system.
- Ensure testing of the system under realistic combat conditions includes knowledge of user casualties and system vulnerabilities or lethality.
- Allow correction in design or employment of any design deficiency identified by T&E before proceeding BLRIP.
- Assess recoverability from battle damage and battle damage repair capabilities and issues.

Structure and schedule the LFT&E Strategy to incorporate any design changes resulting from testing and analysis before proceeding beyond LRIP.

9.3.3.2. Covered Systems

The DoD term for a covered system includes all categories of systems or programs requiring LFT&E. A "covered system" defines a system that DOT&E, acting for the SecDef, designates for LFT&E oversight. These systems include, but are not limited to, the following categories:

- Any major system within the meaning of that term in section 2302(5) of title 10 USC , including user-occupied systems and designed to provide some degree of protection to its occupants in combat; or
- A conventional munitions program or missile program; or a conventional munitions program planning to acquire more than 1,000,000 rounds (regardless of major system status); or
- A modification to a covered system likely to significantly affect the survivability or lethality of such a system.

9.3.3.3. Early Live Fire Test and Evaluation

DOT&E approves the adequacy of the LFT&E Strategy before the program begins LFT&E. LFT&E issues identified in the strategy should drive the program, and fully integrate it with planned DT&E and OT&E. LFT&E typically includes testing at the component, subassembly, and subsystem level; and may also draw upon design analyses, modeling and simulation, combat data, and related sources such as analyses of safety and mishap data. As a standard practice, this occurs regardless of whether the LFT&E program culminates with FUSL testing, or obtaining a waiver from FUSL testing. Conducting LFT&E early in the program life cycle allows time to correct any design deficiency demonstrated by the T&E. Where appropriate, the program manager may correct the design or recommend adjusting the employment of the covered system before proceeding beyond LRIP.

9.3.3.4. Full-Up, System-Level Testing and Waiver Process

DoD defines "full-up, system-level testing" as testing that fully satisfies the statutory requirement for "realistic survivability" or "realistic lethality testing," as defined in section 2366 of title 10 USC . The criteria for FUSL testing differs somewhat based on the type of testing: survivability or operational security or lethality. The following describes FUSL testing:

Vulnerability testing conducted using munitions likely to be encountered in combat on a complete system loaded or equipped with all the dangerous materials that normally would be on board in combat (including flammables and explosives), and with all critical subsystems operating that could make a difference in determining the test outcome; or

Lethality testing of production-representative munitions or missiles, for which the target is representative of the class of systems that includes the threat; and the target and test conditions are sufficiently realistic to demonstrate the lethality effects the weapon is

designed to produce.

The statute requires a LFT&E program to include FUSL testing unless granted a waiver in accordance with procedures defined by the statute. To request a waiver, submit a waiver package to the appropriate Congressional defense committees prior to Milestone B; or, in the case of a system or program initiated at Milestone B, as soon as practicable after Milestone B; or if initiated at Milestone C, as soon as practicable after Milestone C. Typically, this should occur at the time of TEMP approval.

The waiver package includes certification by the USD(AT&L) or the DoD CAE that FUSL testing would prove unreasonably expensive and impractical. It also includes a DOT&E-approved alternative plan for conducting LFT&E in the absence of FUSL testing. Typically, the alternative plan appears similar or identical to the LFT&E Strategy contained in the TEMP. This alternative plan should include LFT&E of components, subassemblies, or subsystems; and, as appropriate, additional design analyses, M&S, and combat data analyses.

Programs receiving a waiver from FUSL testing conduct their plans as LFT&E programs (with exception of the statutory requirement for FUSL testing). In particular, the TEMP contains an LFT&E Strategy approved by DOT&E; and DOT&E, as delegated by the SecDef, submits an independent assessment report on the completed LFT&E to the Congressional committees as required by statute.

9.3.3.5. Personnel Survivability

LFT&E has a statutory requirement to emphasize personnel survivability for covered systems occupied by U.S. personnel (section 2366 of title 10 USC). In general, LFT&E addresses personnel survivability through dedicated MOEs, such as "expected casualties." Address the ability of personnel to survive even in cases where the platform cannot survive. If designated by DOT&E for survivability LFT&E oversight, the system or program should integrate the T&E to address crew survivability issues into the LFT&E program supporting the DOT&E LFT&E Report to Congress.

9.4. Integrated Test and Evaluation

9.4. Integrated Test and Evaluation

According to OSD Memorandum Definition of Integrated Testing , dated April 25, 2008, OSD defines integrated testing as the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the development (both contractor and government) and operational test and evaluation communities.

Integrated testing’s goal: conduct a seamless test program producing credible qualitative and quantitative data useful to all evaluators, and addressing developmental, sustainment, and operational issues. Integrated testing allows for the collaborative

planning of test events; where a single test point or mission can provide data to satisfy multiple objectives, without compromising the test objectives of participating test organizations. Test points in this context, mean a test condition denoted by time, three-dimensional location and energy state, and system operating configuration; where applying a pre-planned test technique to the system under test and observing and recording the response(s).

Integrated testing includes more than just concurrent or combined DT and OT, where both DT and OT test points remain interleaved on the same mission or schedule. Integrated testing focuses the entire test program (contractor test, Government DT, OT, and LFT) on designing, developing, and producing a comprehensive plan that coordinates all test activities to support evaluation results for decision makers at required decision reviews.

Integrated testing may include all types of test activities such as contractor testing, developmental and operational testing, interoperability and IA testing, and certification testing. All testing types, regardless of the source, should receive consideration; including tests from other Services for multi-Service programs. Software intensive and IT systems should use the reciprocity principle as much as possible, i.e., "Test by one, use by all." Specifically name any required integrated test combinations.

For successful integrated testing, understanding and maintaining the pedigree of the data proves vital. The pedigree of the data refers to accurately documenting the configuration of the test asset and the actual test conditions under which each element of test data was obtained. The pedigree of the data should indicate whether the test configuration represented operationally realistic or representative conditions. The T&E WIPT plays an important role in maintaining the data pedigree within the integrated test process for a program. The T&E WIPT establishes agreements between the test program stakeholders; regarding roles and responsibilities in not only implementing the integrated test process, but also in developing and maintaining data release procedures, and data access procedures or a data repository, where all stakeholders will have access to test data for separate evaluations.

Integrated testing must provide shared data in support of independent analyses for all T&E stakeholders. A requirement exists for a common T&E database, including descriptions of the test environments to ensure commonality and usability by other testers. Integrated testing must allow for and support separate, independent OT&E according to section 2399 of title 10 USC and DoDI 5000.02 , Operation of the Defense Acquisition System, dated December 8, 2008. It does not include the earliest engineering design or testing of early prototype components.

Integrated testing serves as a concept for test design, not a new type of T&E. Programs must intentionally design it into the earliest program strategies, plans, documentation, and test plans, preferably starting before Milestone A. Developing and adopting integrated testing strategies early in the process increases the opportunities and benefit’s. If done correctly, the enhanced operational realism in DT&E provides greater

opportunity for early identification of system design improvements, and may even change the course of system development during EMD. Integrated testing can increase the statistical confidence and power of all T&E activities. Most obviously, integrated testing can also reduce the number of T&E resources needed in OT&E. However, integrated testing does not replace or eliminate the need for dedicated IOT&E, as required by section 2399 of title 10 USC , "Operational Test and Evaluation of Defense Acquisition Programs" and DoDI 5000.02 .

The T&E strategy should embed integrated testing, although most of the effort takes place during the detailed planning and execution phases of a test program. It is critical that all stakeholders understand the required evaluations to assess risks, assess maturity of the system and assess the operational effectiveness, operational suitability and survivability or operational security /lethality. Up front, define the end state for evaluation, ensuring all stakeholders work toward the same goal. Once accomplished, develop an integrated test program that generates the data required to conduct the evaluations.

Early identification of system and mission elements enable the development and execution of an efficient and effective T&E strategy and an integrated DT/OT program. The use of scientific and statistical principles for test and evaluation; for example, design of experiments (DOE), will help develop an integrated DT/OT program by providing confidence about the performance of a system in a mission context.

Although DT and OT require different fidelity to meet their individual objectives (e.g., data parameters, mission control, onboard and test range instrumentation, data collection and analysis), some of areas of commonality include:

- Evaluation in complex joint mission operating environments with systems of different levels of maturity (integrating upgraded systems with legacy systems)
- Replication of the real world environment as closely as practical in a safe and affordable manner
- Need for a distributive live/virtual/constructive (LVC) representation of the joint operational environments (the only affordable way to test and train in a complex system-of-systems environment)
- Use of validated tactics, techniques, and procedures (TTPs)
- Representation of Blue and Red Forces
- Validated scenarios
- Threat and threat countermeasures
- Dedicated instrumented ranges. (differences exist in the instrumentation fidelity required to control participants, collect data, and support real-time and post-event analyses)
- Data collection, management, archiving, and retrieval processes
- Embedded sensors and instrumentation

Integrated DT/OT initiatives encourage all testers contractor, developmental, operational, and live fire to plan an integrated test program, seeking an efficient

continuum. They focus on the early discovery of problems in a mission context and in realistic operational environments even for component testing. The appropriate T&E environment includes the system under test (SUT) and any interrelated systems (that is, it's planned or expected environment in terms of weapons, sensors, command and control, and platforms, as appropriate) needed to accomplish an end-to-end mission in combat. The following includes a few integrated test concerns:

1. Balancing the test event to effectively capture different DT and OT data collection objectives
2. Requiring early investment in detailed planning that many programs lack in early stages
3. Requiring constant planning and updates to effectively maximize test results
4. Much of the early information for a program is preliminary, requiring rework and updates
5. Analyzing proves difficult when unanticipated anomalies appear in test results

9.5. Test and Evaluation Planning

T&E planning should include statistically defensible test results to effectively support decision makers. A common approach, DOE serves as a structured process to assist in developing T&E strategies utilizing statistical analyses. Many constraints exist in testing limited test resources, limited test time, and limited test articles. DOE aids in the understanding of the tradeoffs among these constraints and their implications. Additionally, DOE can provide a statistically optimum allocation of assets under given constraints. It can also provide optimal allocation test points between multiple phases of testing. DOE ensures the synergistic results in the data collected in multiple phases in sequential learning about the system.

A program applying DOE should start early in the acquisition process and assemble a team of subject matter experts who can identify operational and environmental conditions (the driving factors in the successful performance of the system and the consideration of levels of each factor). The team should include representation for all testing (contractor testing, Government DT and OT). The developed TEMP should include the resources needed, the plan for early tests (including component tests), and use of the results of early tests to plan further testing.

9.5.1. DT&E Planning

A well planned and executed DT&E program supports the technology development and acquisition strategies as well as the systems engineering process; providing the information necessary for informed decision-making throughout the development process and at each acquisition milestone. DT&E provides the verification and validation (V&V) of the systems engineering process as well as confidence that the system design solution satisfies the desired capabilities. The strategy for T&E should remain consistent with and complementary to the SEP and acquisition strategy. The T&E WIPT, working closely with the PM and the system design team, facilitates this process. Rigorous component and sub-system DT&E enables early performance and reliability assessments for utilization in system design. DT&E and integrated testing events should advance to rigorous, system-level and system-of-systems (SoS) level T&E; ensuring the system maturity to a point where it can enter production, and ultimately meet operational employment requirements.

DT&E reduces technical risk and increases the probability of a successful program. During early DT&E, the prime contractor focuses contractor testing on technical contract specifications. Government testers observe the critical contractor testing, conduct additional T&E, and, when practical, facilitate early user involvement. The PMs contract with industry must support open communication between government and contractor testers. The OSD document, "Incorporating Test and Evaluation into Department of Defense Acquisition Contracts," dated October 2011, provides additional guidance on contract-related issues for the successful solicitation, award, and execution of T&E related aspects of acquisition contracts. Items such as commercial-off-the-shelf, non-developmental items, and Government-off-the-shelf products, regardless of the manner of procurement, must undergo DT&E to verify readiness to enter IOT&E, for proper evaluation of operational effectiveness, operational suitability, and survivability or operational security for the intended military application. Programs should not enter IOT&E until the DoD Components indicate confidence that the production representative system will successfully demonstrate effective, suitable, and survivable criteria established in the capability production document (CPD). In addition, the government will report DT&E results at each program milestone, providing knowledge to reduce the risk in those acquisition decisions.

9.5.2. OT&E Planning

DoDI 5000.02 Enclosure 6 lists mandatory elements of OT&E planning and execution.

Other considerations include:

- Planning should consider an integrated testing approach. The integrated approach should not compromise either DT&E or OT&E objectives. Planning should provide for an adequate OT period and report generation, including the DOT&E BLRIP report to the SecDef and Congress prior to the FRP decision.
- OT&E should take maximum advantage of training and exercise activities to increase the realism and scope of both the OT&E and training, and to reduce testing costs.
- OTAs should participate in early DT&E and M&S to provide operational insights to the PM, the JCIDS process participants, and acquisition decision-makers. OT&E responsibility resides with the DoD Component OTA; including planning, gaining DOT&E plan approval, execution, and reporting.
- Prototype testing should be emphasized early in the acquisition process and during EOAs to identify technology risks and provide operational user impacts. OTAs should maximize their involvement in early, pre-acquisition activities. T&E provides early operational insights during the developmental process. This early operational insight should reduce the scope of the integrated and dedicated OT&E, thereby contributing to reduced acquisition cycle times and improved performance.
- OT&E planning should consider appropriate use of accredited M&S to support DT&E, OT&E, and LFT&E and be coordinated through the T&E WIPT. Test planners should collaborate early with the PMs M&S proponent on the planned use of M&S to support or supplement their test planning or analyze test results. Where feasible, consider the use or development of M&S that encompasses the needs of each phase of T&E. Test planners must coordinate with the M&S proponent/developer/operator to establish acceptability criteria required to allow VV&A of proposed M&S. It is the responsibility of the PMs M&S proponent to ensure the conduct of V&V in a manner supporting accreditation of M&S for each intended use. Whenever possible, an OA should draw upon test results with the actual system, or subsystem, or key components thereof, or with operationally meaningful surrogates. When a PM cannot conduct actual system testing to support an OA, such assessments may utilize computer modeling and/or hardware in the loop, simulations (preferably with real operators in the loop), or an analysis of information contained in key program documents. However, the PM must ensure they receive a risk assessment when system testing cannot support an OA. The TEMP explains the extent of M&S supporting OT&E, whether to develop M&S, the identification of resources, and a cost/benefit analysis. Naval vessels, the major systems integral to ship construction, and military satellite programs typically have development and construction phases extending over long periods of time and involve small procurement quantities. To facilitate evaluations and assessments of system performance (operational effectiveness, operational suitability and mission capability) the PM should ensure the involvement of the independent OTA in the monitoring of or participating in all relevant activity to make use of any/all relevant results to complete operational assessments (OAs). The OTA should determine the

inclusion/exclusion of test data for use during OAs and determine the requirement for any additional operational testing needed for evaluation of operational effectiveness, operational suitability and mission capability.
- OT&E uses threat or threat representative forces, targets, and threat countermeasures, validated by the DIA or the DoD Component intelligence agency, as appropriate, and approved by DOT&E during the operational test plan approval process. DOT&E oversees threat target, threat simulator, and threat simulation acquisitions and validation to meet OT&E and LFT&E needs.
- PMs and OTAs assess the reliability growth required for the system to achieve its reliability threshold during IOT&E and report the results of that assessment to the MDA at Milestone C.

- OT&E will evaluate Information Assurance on any system collecting, storing, transmitting, or processing unclassified or classified information. This evaluation will include IA vulnerability and penetration testing. Additionally, all networked and command, control, communications & intelligence (C3I) systems on the OSD T&E Oversight List shall receive IA effectiveness evaluations and Computer Network Defense (CND) measures against cyber threats in accordance with the DOT&E memo " Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs ," dated 4 November, 2010, and " Procedures for Operational Test and Evaluation of Information Assurance in Acquisition programs " dated 21 January 2009.
- OT&E will evaluate potentially adverse Electromagnetic Environmental Effects (E3) and spectrum supportability situations. Operational testers should use all available data and review DD Form 1494 , "Application for Equipment Frequency Allocation," dated August 1996, to identify which systems need field assessments.

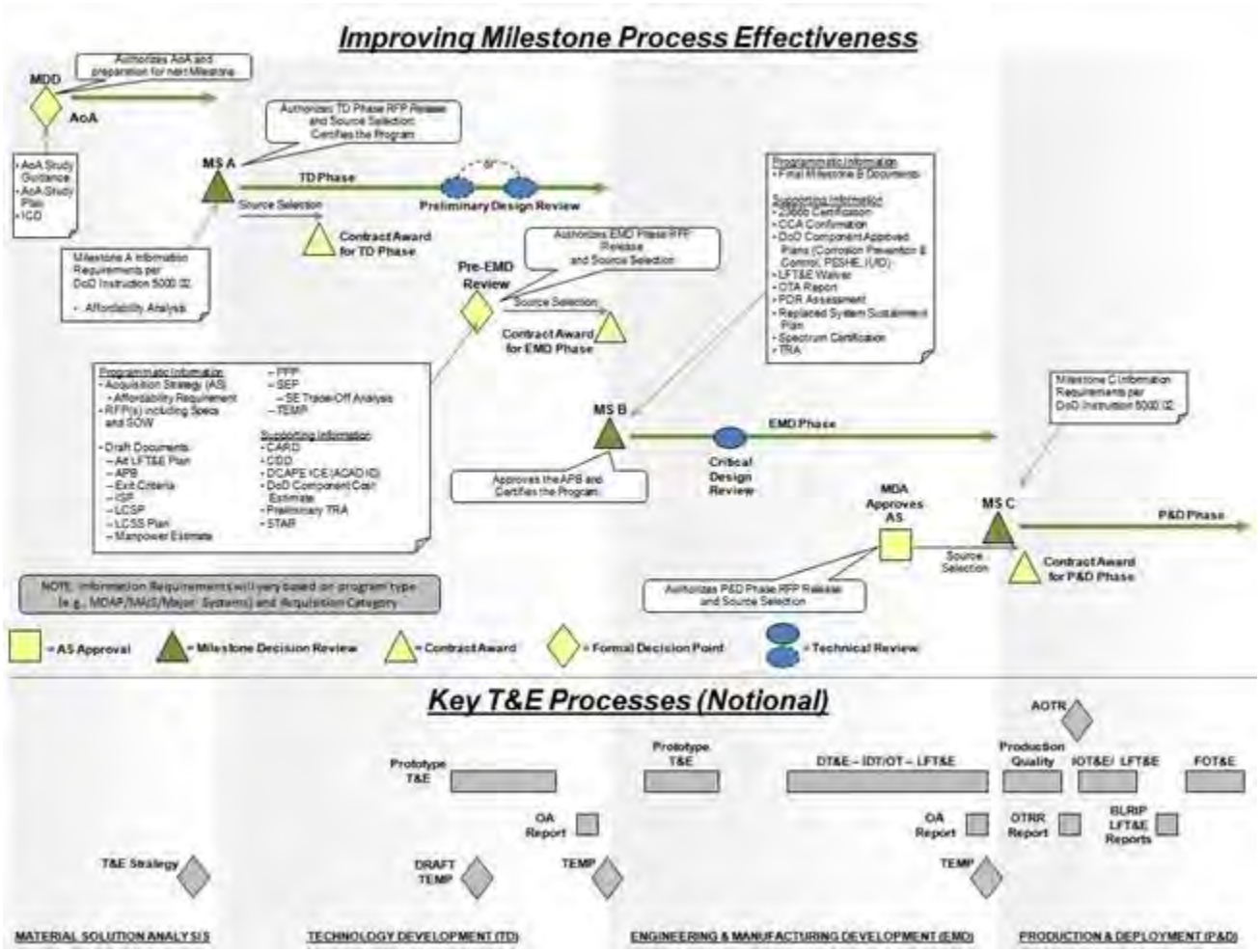
9.5.3. Early Involvement

T&E early involvement advises program offices on the testability of requirements, scoping the T&E program and resources for inclusion in the technology and acquisition strategies, contractual requirements, and other upfront actions helping the acquisition program succeed. This requires the active engagement of skilled T&E personnel in the requirements and acquisition processes to get the up-front right, particularly in terms of definitional precision in describing the operational context, mission and system measures, integration of DT and OT, and the construct for translating performance results into mission effectiveness terms. Developing a framework to accomplish those objectives enhances the efficiencies and effectiveness of T&E programs, and results in less conflict during T&E planning and execution.

An integral element of the Defense Acquisition System (DoDI 5000.02), T&E has a role across the entire lifecycle as depicted in the following Figure 9.5.3.F1. The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart (v5.3.4, 15 Jun 2009) outlines the key activities in the systems acquisition processes that must work in concert to deliver the capabilities required by the warfighters: the

requirements process (JCIDS; the acquisition process (Defense Acquisition System); and program and budget development (Planning, Programming, Budgeting, and Execution (PPBE) process).

Figure 9.5.3.F1: Key T&E Processes across the Lifecycle T&E Perspective



NOTE: A larger version of the process is available by clicking on the image above.

Key sources of T&E information, used during the formulation of a Materiel Solution, include the capabilities-based assessment (CBA), Analysis of Alternatives (AOA), JCIDS documents, etc. Items of particular interest to the T&E community include:

- Mission description, scenarios, Concept of Operations (CONOPS), performance attributes and effectiveness metrics, targets and threats, operational environments, etc.
- Mission to task decomposition and scenario-based task performance standards.
- Task to system/sub-system associations and functionality.
- Alignment of mission Measures of Effectiveness (MOEs) with system

performance attributes and measures.

The requirements process defines and subsequently refines a programs operational capability requirements (system attributes) and operational environments (mission attributes) throughout the development process in the CBA, Initial Capabilities Document (ICD), CDD, and CPD.

Critical to the developers, testers, and representative of the COCOM Area of Responsibility (AOR) for operational employment ,the pedigree of operational context across the lifecycle and the design of the operational context of the system should remain the same as the evaluated operational context,. If the operational context changes over the course of development, those changes should be documented in both the AOA and JCIDS updates.

9.5.3.1. Defining Mission Measures: Early Involvement JCIDS (Measures of Effectiveness (MOE) and Measures of Performance (MOP))

JCIDS processes are currently undergoing a significant revision, with the expectation of releasing the new policy in late FY 2011. The current JCIDS process has evolved from a joint mission-based process, focused on evaluating MOE and MOP in a mission context to deliver a capability to an operational environments-based process focused on evaluating system performance attributes to deliver a required capability, as seen in excerpt from the current JCIDS policy below:

- The JCIDS primary objective ensures the identification of the capabilities required by the joint Warfighter with their associated operational performance criteria in order to successfully execute the missions assigned.
- The JCIDS process supports the acquisition process by identifying and assessing capability needs and associated performance criteria used as a basis for acquiring the right capabilities, including the right systems.
- The CDD primary objective specifies the operational technical performance attributes of the system delivering the capability to fill the gaps identified in the ICD.
- The CPD primary objective describes the actual performance of the system delivering the required capability.

- If the system does not meet all of the threshold levels for the KPPs, the Joint Requirements Oversight Council (JROC) will assess whether or not the system remains operationally acceptable.
- The CDD and CPD identify the attributes contributing most significantly to the desired operational capability in threshold-objective format. Whenever possible, state attributes in terms reflecting the range of military operations the capabilities must support and the joint operational environment intended for the system (family of systems (FoS) or SoS).
- Other compatibility and interoperability attributes (e.g., databases, fuel, transportability, and ammunition) might need identification to ensure a

capability's effectiveness.

The CJCSI 3170.01H Joint Capabilities Integration and Development System, dated January 10, 2012 complements the JCIDS instruction. Additionally:

- DOT&Es role with respect to the ICD is included in the JCIDS Manual: DOT&E will advise on the testability of chosen capability attributes and metrics so that the systems performance measured in operational testing can be linked to the CBA.
- The JCIDS manual further states The ICD will include a description of the capability, capability gap, threat, expected joint operational environments, shortcomings of existing systems, the capability attributes and metrics, joint Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF), and policy impact and constraints for the capabilities.

Director of Operational Test and Evaluation (DOT&E) (DoDD 5141.02).

- Assist the CJCS in efforts to ensure the specification of expected joint operational mission environment, mission-level MOE, and KPPs in JCIDS documents in terms verifiable through testing or analysis.

Note: the JCIDS policy no longer requires or discusses MOPs and MOEs; however, the JCIDS derives and documents performance attributes from analysis that supported the CBA and the AOA. Additionally, the CBA, AOA, and MOPs and MOEs remain essential metrics needed for evaluation of those performance attributes.

- Measure of Effectiveness (MOE) The data used to measure the military effect (mission accomplishment) that comes from the use of the system in its expected environment. That environment includes the system under test and all interrelated systems, that is, the planned or expected environment in terms of weapons, sensors, command and control, and platforms, as appropriate, needed to accomplish an end-to-end mission in combat.
- Measures of Performance (MOPs) System-particular performance parameters such as speed, payload, range, time-on-station, frequency, or other distinctly quantifiable performance features. Several MOPs may be related to the achievement of a particular MOE.

Further, the OTAs and DOT&E have a requirement to address effectiveness in their evaluations. In the memorandum Reporting of Operational Test and Evaluation (OT&E) Results , dated January 6, 2010, DOT&E states:

- The data used for evaluation are appropriately called measures of effectiveness, because they measure the military effect (mission accomplishment) that comes from the use of the system in its expected environment. This statement of policy precludes measuring operational effectiveness and suitability solely on the basis of system-particular performance parameters.
- . . . "performance attributes (*sic*) are often what the program manager is

required to deliver they are not the military effect or measure of operational effectiveness required for achieving the primary purpose of a mission capability".

- It is therefore unacceptable in evaluating and reporting operational effectiveness and suitability to parse requirements and narrow the definition of mission accomplishment so that MOP are confused with MOE.

9.5.3.2. Defining the Operational Context: Early Involvement - CBA: Operational Context (Scenarios, Missions and Objectives, Environments, etc.)

The JCIDS process begins with the CBA, which provides the bases for JCIDS to articulate the systems performance attributes required by the warfighters. Any DoD organization may initiate a CBA. See the Manual for the Operation of the Joint Capabilities Integration and Development System , dated July 31, 2009 for CBA information.

9.5.3.3. Analysis of Alternatives

For potential and designated ACAT I and IA programs, the Director, Cost Assessment and Program Evaluation (CAPE) should draft, for MDA approval, AoA study guidance for review at the Materiel Development Decision. Following approval, the guidance should be issued to the DoD Component designated by the MDA, or for ACAT IA programs, to the office of the Principal Staff Assistant responsible for the mission area. According to DoDI 5000.02, Enclosure 7 , dated December 8, 2008, the DoD Component or the Principal Staff Assistant shall designate responsibility for completion of the study plan and the AoA; neither of which may be assigned to the PM. The study plan shall be coordinated with the MDA and approved by the CAPE prior to the start of the AoA. The final AoA shall be provided to the CAPE not later than 60 days prior to the DAB or Information Technology Acquisition Board milestone reviews. The CAPE shall evaluate the AoA and provide an assessment to the Head of the DoD Component or Principal Staff Assistant and to the MDA. In this evaluation, the CAPE, in collaboration with the OSD and Joint Staff, shall assess the extent to which the AoA:

a) Illuminated capability advantages and disadvantages.

b) Considered joint operational plans.

c) Examined sufficient feasible alternatives.

d) Discussed key assumptions and variables and sensitivity to changes in these.

e) Calculated costs.

f) Assessed the following:

1. Technology risk and maturity.
2. Alternative ways to improve the energy efficiency of DoD tactical systems with

end items that create a demand for energy, consistent with mission requirements and cost effectiveness.
3. Appropriate system training to ensure that effective and efficient training is provided with the system.

9.5.3.4. Defining Critical Technical Parameters (CTPs)

T&E programs will have hundreds or thousands of technical parameters needing capture to support data analysis and evaluations; however, every technical parameter is not a CTP. CTPs measure critical system characteristics that, when achieved, enable the attainment of desired operational performance capabilities in the mission context. CTP do not simply restate the KPPs and/or KSAs. Each CTP must have a direct or significant indirect correlation to a KPP and or KSA that measures a physical characteristic essential to evaluation of the KPP or KSA. The 2011 JCIDS Manual, The Director, Operational Test & Evaluation (DOT&E) will advise on the testability of chosen capability attributes and metrics so that the systems performance measured in operational testing can be linked to the CBA. The ICD will include a description of the capability, capability gap, threat, expected joint operational environments, shortcomings of existing systems, the capability attributes and metrics, joint DOTMLPF, and policy impact and constraints for the capabilities.

CTPs should focus on critical design features or risk areas (e.g., technical maturity, reliability, availability, and maintainability (RAM) issues, physical characteristics or measures) that if not achieved or resolved during development will preclude delivery of required operational capabilities. CTPs will likely evolve/change as the system matures during EMD. Resolve existing CTPs and identify new CTPs as the system progresses during development. Identify any CTPs not resolved prior to entering LRIP and establish an action plan to resolve them prior to the FRP Decision Review.

The Program T&E Lead has responsibility for coordinating the CTP process with the Programs Chief or Lead Systems Engineer, with assistance from the appropriate test organization subject matter experts and lead OTA. The evaluation of CTPs proves important in projecting maturity of the system and to inform the PM as to whether the system is on (or behind) the planned development schedule or will likely (or not likely) achieve an operational capability, but are not sufficient in projecting mission capability. The projection of mission capability requires an evaluation of the interoperability of systems and sub-systems in the mission context, when used by a typical operator, CTPs associated with the systems/sub-systems provide a basis for selecting entry or exit criteria demonstrated for the major developmental test phases.

9.5.4. Test and Evaluation Strategy (Milestone A)

9.5.4.1. Description

The TES describes the concept for tests and evaluations throughout the program life cycle, starting with Technology Development and continuing through EMD into Production and Deployment. The TES evolves into the TEMP at Milestone B. Development of a TES requires early involvement of testers, evaluators, and others as a program conducts pre-system acquisition activities. These personnel provide the necessary technical, operational, and programmatic expertise to ensure nothing is overlooked in laying out a complete strategy. The TES approval process is explained in 9.5.4.3.

The TES must remain consistent with the Technology Development Strategy (TDS) and Initial Capabilities Document (ICD) . The TES should address the identification and management of technology risk, the evaluation of system design concepts against the preliminary mission and sustainment requirements resulting from the analysis of alternatives, competitive prototyping, early demonstration of technologies in operationally relevant environments, and the development of an integrated test approach. The TES also satisfies the TDS test plan to ensure the completion of goals and exit criteria for the technology demonstrations in a relevant environment in accordance with section 2359a of title 10 USC . It also provides a road map for evaluations, integrated test plans, and resource requirements necessary to accomplish the TD phase objectives.

The TES begins by focusing on TD phase activities, and describes the demonstration of component technologies under development in an operationally relevant environment to support the program's transition into the EMD Phase. It contains hardware and software maturity success criteria used to assess key technology maturity for entry into EMD. For programs following an evolutionary acquisition strategy with more than one developmental increment, the TES describes the application of T&E and M&S to each planned increment to provide the required operational effectiveness, suitability, and survivability or operational security, as would be required of a program containing only one increment. TES development supports the initial Milestone A decision. The TEMP subsumes the TES for all increments thereafter, unless a follow-on increment requires a new Milestone A decision. TES development establishes an early consensus among T&E WIPT member organizations on the programs scope for testing and evaluation, with particular consideration given to needed resources to support PPB&E process

activities. The TES requires the inclusion of cost estimates beginning with program initiation and continuing through development and production, including nonrecurring and recurring research and development (R&D) costs for prototypes, engineering development equipment and/or test hardware (and major components thereof). Additionally, the TES fully identifies and estimates contractor T&E and Government support to the test program. Estimate any support, such as support equipment, training, data, and military construction. Include the cost of all related R&D (such as redesign and test efforts necessary to install equipment or software into existing platforms). See DoD 5000.4-M , "Cost Analysis Guidance Procedures," Table C2.T2, "Defense Acquisition Program Life-Cycle Cost Categories Research and Development," for a more specific list of R&D costs. The basis for the T&E resources required in the Cost Analysis Requirements Description comes from the TES cost information.

9.5.4.2. TES Content and Format

The following content and format provides all necessary information for a TES, and assists in the transition to a TEMP at Milestone B.

PART I INTRODUCTION

1.1. Purpose. State the purpose of the TES. Reference the documentation initiating the TES (i.e., ICD, AoA, CONOPS).

1.2. Mission Description. Briefly summarize the mission need described in the capability requirements documents in terms of the capability it will provide to the Joint Forces Commander. Briefly summarize the CONOPS, and include a high level operational concept graphic **(** OV-1) or similar diagram.

1.3. System Description. Describe the system or prototype configurations. Identify key features, technologies, and components, both hardware and software for the planned Technology Development phase.

1.3.1. System Threat Assessment. Succinctly summarize the threat environment in which the system or components will operate. Reference the appropriate DIA- or DoD Component-validated threat documents.

1.3.2. Program Background. Briefly discuss any background information. Reference the AoA, the materiel development decision, and any previous tests or evaluations that have an effect on the T&E strategy.

1.3.3. Key Capabilities. Identify the system attributes that support key capabilities from the ICD. Identify the T&E-related TD Phase exit criteria.

1.3.3.1. Key Interfaces. Identify interfaces with existing or planned systems architectures (to the extent known at Milestone A) that are required for mission

accomplishment.

1.3.3.2. Special Test Requirements. Identify unique system characteristics or support concepts that will necessitate development of special test and evaluation assets or techniques.

1.3.3.3. SE Requirements. Summarize SE-based information driving the Technology Development phase and prototype development. Reference the SEP and other applicable source documents.

PART II TEST and EVALUATION PROGRAM MANAGEMENT AND SCHEDULE

2.1. T&E Management. Discuss the test and evaluation role of participating organizations. Describe the role of contractor and governmental personnel. Provide organizational construct that includes organizations such as the T&E WIPT or Service equivalent.

2.2. T&E Data Strategy. Describe the strategy and methods for collecting, validating, and sharing data as it becomes available from the contractors, DT&E, and oversight organizations.

2.3. Integrated Test Program Schedule. Provide the overall time sequencing of the major events with an emphasis on the TD phase. Include event dates such as major decision points, preliminary design reviews, prototypes and test article availability, and phases of DT&E.

PART III TEST AND EVALUATION STRATEGY

3.1. T&E Strategy Introduction. This section should summarize an effective and efficient approach to the T&E program.

3.2. Evaluation Framework. Describe the overall concept of the T&E program with an emphasis on decisions in the Technology Development phase and information required to draft the CDD. Specific areas of evaluation should include Technology Readiness Level (TRL) and prototype testing. Include a Top-Level Evaluation Framework matrix that shows the correlation between decisions, the primary capabilities, critical technologies, critical technical parameters, and other key test measures.

3.3. Developmental Evaluation Approach. The discussion should be related to the TD phase, including a focus on ICD issues. If applicable, discuss the T&E supporting the reliability growth approach.

3.3.1. Developmental Test Objectives. Summarize the planned objectives and state the methodology to test the technology attributes defined by the TDS.

3.3.2. Modeling & Simulation. Describe the key models and simulations and their

intended use. Identify who will perform M&S verification, validation, and accreditation.

3.3.3. Test Limitations. Discuss any test limitations that may significantly affect the evaluator's ability to draw conclusions about the TRL and capabilities.

3.4. Operational Evaluation Approach. Discuss the approach during the TD phase to providing operational insights from the user perspective, including resolution of the ICD issues. Include reliability growth testing, if appropriate.

3.4.1. Mission-Oriented Approach. Describe the approach to evaluate the system performance at the appropriate TRLs.

3.4.2. Operational Test Objectives. Summarize the planned objectives and state the methodology to test the technology attributes defined by the TDS.

3.4.3. M&S. Describe the key models and simulations and their intended use. Identify who will perform M&S verification, validation, and accreditation.

3.4.4. Test Limitations. Discuss any test limitations that may significantly affect the evaluator's ability to draw conclusions about the TRL and capabilities.

3.5. Future Test and Evaluation. Summarize all remaining significant T&E that has not been discussed yet, extending through the acquisition life cycle. Test events after Milestone B will be described in detail in the Milestone B TEMP update.

PART IV RESOURCE SUMMARY

4.1. Introduction. Testing will be planned and conducted to take full advantage of existing DoD investment in ranges, facilities, and other resources wherever practical. Describe all key test and evaluation resources, both government and contractor, that will be used during the course of the TD phase. Include long-lead items for the next phase, if known.

4.1.1. Test Articles. Identify the prototypes and test articles.

4.1.2. Test Sites and Instrumentation. Identify the test ranges and facilities to be used for testing.

4.1.3. Test Support Equipment. Identify test support, analysis equipment, and personnel required to conduct testing.

4.1.4. Threat Representation. Identify the type, number, availability, fidelity requirements, and schedule for representations of the threat (to include threat targets) to be used in testing.

4.1.5. Test Targets and Expendables. Specify the type, number, availability, and

schedule for test targets and expendables, (e.g. targets, weapons, flares, chaff, sonobuoys, countermeasures).

4.1.6. Operational Force Test Support. Specify the type and timing of aircraft flying hours, ship steaming days, and on-orbit satellite contacts/coverage, and other operational force support.

4.1.7. Simulations, Models and Testbeds. Specify the models and simulations to be used. Identify opportunities to simulate any of the required support. Identify the resources required to validate and accredit their usage, responsible agency, and timeframe.

4.1.8. Joint Mission Environment. Describe the live, virtual, or constructive components or assets necessary to create an acceptable environment to evaluate TRLs and mission capabilities.

4.1.9. Special Requirements. Identify requirements for non-instrumentation capabilities or instrumentation and analysis tools that require development or upgrades.

4.2. Test and Evaluation Funding Summary. Provide initial estimates of DT&E, OT&E, and LFT&E costs.

9.5.4.3. TES Approval Process

For programs under OSD T&E oversight, the PM or leader of the concept development team, with the T&E WIPT providing support, submits the DoD Component/Defense Agency-approved TES to OSD for staffing and approval before Milestone A. The PM should submit the TES at least 45 days prior to Milestone A to support the decision. The DOT&E and the DASD(DT&E) approve the TES for all programs on the OSD T&E Oversight List. For programs not on the OSD T&E Oversight List, the CAE, or designated representative, approves the TES.

9.5.5. Test and Evaluation Master Plan

9.5.5.1. Strategy for Test and Evaluation

9.5.5.2. Evaluation Framework

9.5.5.3. TEMP Format

9.5.5.4. Other Milestone TEMPs and Updates

9.5.5. Test and Evaluation Master Plan

The TEMP serves as the overarching document for managing a T&E program. PMs should develop a draft TEMP for the pre-EMD review and a formal TEMP for Milestone

B, based on the AT&L memo Improving Milestone Process Effectiveness, dated June 23, 2011. Prior to each subsequent Defense Acquisition System Milestone, the PMs must submit an updated TEMP. The TEMP should include sufficient detail to support development of other test related documents.

PMs develop a TEMP and subsequent updates meeting the following objectives:

- Accomplish all certification requirements necessary for the conduct of T&E.
- Provide an event-driven T&E schedule.
- Ensure the T&E strategy aligns with and supports the approved acquisition strategy to provide adequate, risk-reducing T&E information to support decisions.
- Integrate DT&E and OT&E objectives into an efficient test continuum for use in the TEMP to maximize efficiencies during test execution, and increase the test sample size while minimizing test resource requirements.
- Identify and describe design, technical, integration, operational, safety, and security risks . The T&E strategy should naturally flow from the user mission requirements and concept of operations (CONOPS), systems engineering processes of requirements analysis, functional allocation, and design synthesis.
- Serve as the basis for T&E budgetary estimates identified in the Cost Analysis Requirements Description (required by DoD 5000.4-M Cost Analysis Guidance and Procedures, dated December 11, 1992).
- Identify test strategies to efficiently identify technology limitations and capabilities of alternative concepts to support early cost performance tradeoff decisions.
- Provide data and analytic support to certify the system ready for IOT&E . The DT&E report discussed below provides this data.
- Assess technical progress and maturity against critical technical parameters (CTPs), key system attributes (KSAs), KPPs, and critical operational issues (COIs) as documented in the TEMP and test plans. CTPs can be used to assess completion of a major phase of developmental testing such as ground or flight testing; and determine readiness to enter the next phase of testing, whether developmental or operational.
- To mitigate technical risk, the required assessment of technical progress should also include reliability, maintainability and supportability desired capabilities, software functionality, and technical and manufacturing risks.
- Include reliability growth curves at Pre-EMD and report progress to plan at future updates.
- Include adequate measures to support the programs reliability growth plan and requirements for a RAM Cost Rationale Report defined in DOD RAM Cost Rationale Manual, for MS B and C. For more information, read DTM 11003 , Reliability Analysis, Planning, Tracking, and Reporting, dated December 2, 2011.
- Some technical parameters can be expressed as either a rate of change or a simple specific value in assessing level of success. For example, the rate at which a system accuracy or reliability is increasing, or simply the success rate of a system meeting a certain accuracy or reliability threshold. The PM may use a combination of both to tailor the test strategy to support decision requirements.
- Utilize M&S and ground test activities, to include integration laboratories,

hardware-in-the-loop simulation, and installed-system test facilities prior to conducting full-up, system-level and end-to-end testing in open-air realistic environments. Programs normally limit DT&E of military medical devices to airworthiness certification and environmental testing to ensure the device does not fail due to the austere or harsh environments imposed by the operational environment or interfere with the aircrafts operational environment. This can often be integrated into, or performed alongside, the requisite OT.

- Perform V&V in the use of M&S and the systems engineering process.
- Stress the system under test to at least the limits of the Operational Mode Summary/Mission Profile, and for some systems, beyond the normal operating limit's to ensure the robustness of the design. This testing will reduce risk for performance in the expected operational environments.
- Provide safety releases (to include formal Environment, Safety, and Occupational Health (ESOH) risk acceptance), in concert with the user and the T&E community, to the developmental and operational testers prior to any test using personnel.
- Demonstrate the maturity of the production process through Production Qualification Testing (PQT) of low-rate initial production (LRIP) assets prior to full-rate production (FRP). The focus of this testing is on the contractor's ability to produce a quality product, since the design testing should have been completed.
- Provide data and analytic support to the Milestone C decision to enter LRIP.
- For weapons systems, use the System Threat Assessment (STA) or System Threat Assessment Report (STAR) as a basis for scoping a realistic test environment.
- For IT & NSS, use DIA, North American Industry Class System (NAICS), or other applicable standard as a basis for scoping a realistic test environment.
- Conduct Information Assurance (IA) testing on any system that collects, stores, transmits, and processes unclassified or classified information; The extent of IA testing depends upon the assigned Mission Assurance Category and Confidentiality Level. DoDI 8500.2 , "Information Assurance (IA) Implementation," dated February 6, 2003, mandates specific IA Control Measures a system should implement as part of the development process.
- In the case of IT systems, including NSS , support the DoD Information Assurance Certification and Accreditation Process and Joint Interoperability Certification process.
- Discover, evaluate, and mitigate potentially adverse electromagnetic environmental effects (E3) .
- Support joint interoperability assessments required to certify system-of-systems interoperability.
- For business systems, the TEMP identifies certification requirements needed to support the compliance factors established by the Office of the Under Secretary of Defense (Comptroller) (USD(C)) for financial management, enterprise resource planning, and mixed financial management systems.
- Demonstrate performance against threats and their countermeasures as identified in the Defense Intelligence Agency (DIA) or component-validated threat document. Any impact on technical performance by these threats should be

identified early in technical testing, rather than in operational testing where their presence might have serious repercussions.
- Assess SoS Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) prior to OT&E to ensure interoperability under loaded conditions will represent stressed OT&E scenarios.

9.5.5.1. Strategy for Test and Evaluation

PMs should structure a T&E program strategy to provide knowledge to reduce risk in acquisition and operational decisions. The evaluations of all available and relevant data and information from contractor and government sources develop that knowledge. The evaluation should focus on providing essential information to decision makers, specifically with regard to attainment of technical performance attributes and an assessment of the systems missions operational effectiveness, operational suitability, and survivability or operational security. The evaluation framework supports estimates for test resource requirements and provides a basis for determining test program adequacy and assessing risk margins within the T&E plans and events.

The PM should structure the strategy to provide essential information to decision-makers, assess attainment of technical performance parameters, and determine whether systems are operationally effective, suitable, survivable, and safe for intended use. The conduct of T&E, integrated with M&S, should facilitate learning, assess technology maturity and interoperability, facilitate integration into fielded forces, and confirm performance against documented capability needs and adversary capabilities as described in the system threat assessment.

In other words, the evaluation should describe the links between key program and user decisions, as well as the developmental and operational tests that requiring evaluation for those decisions. It correlates the knowledge required concerning KPPs/ KSAs, CTPs, key test measures (i.e., MOEs and Measure of Suitability (MOSs)), and the planned test methods, key test resources, facility, or infrastructure needs. The framework discussion should also identify major risks or limitations to completing the evaluations. The TEMP should clearly reflect what key questions the evaluations will answer for the program and user, and at what key decision points. This layout and discussion provides a rationale for the major test objectives and the resulting major resource requirements shown in the Resources portion of the TEMP.

The evaluation should also discuss the intended maturation of key technologies within the overall system, the evaluation of capabilities in a mission context, and evaluations needed to support required certifications or to comply with statute(s). Separate evaluation plans should provide details for the PMs overall evaluation strategy (e.g., System Evaluation Plan (Army), Operational Test and Evaluation plan, LFT&E plan).

The DT&E section describes the evaluation of the maturation of a system or capability, and should address the overall approach to evaluate the development of system capabilities, in operationally relevant environments. The approach should cover CTPs,

key system risks, and any certifications required (weapon safety, interoperability, etc.). The evaluation of technology maturity should support the TDS.

The evaluation of system maturity should support the acquisition strategy. The amount of development in the acquisition strategy will drive the extent of the discussion. For example, if a non-developmental item (i.e., Commercial-Off-The-Shelf (COTS) or Government-off-the-shelf (GOTS)) then there may not be much, if any, maturation of the system required. If a new technology effort, pushing the state-of-the-art or capabilities significantly improved over what is currently being achieved in the operational environment, then it may require a significant amount of effort in maturing or developing the system or it's support system, and therefore more decisions requiring knowledge from evaluations. In assessing the level of evaluations necessary, give equal consideration to the maturity of the technologies used, the degree to which system design (hardware and software) has stabilized, as well as the operational environment for the employment of the system. Using COTS items in a new environment can result in significant capability changes, potentially eliminating a true COTS item from a system maturity perspective.

The system maturation discussions should also cover evaluations for production qualification, production acceptance, and sustainment of the system. The Defense Contract Management Agency (DCMA) representatives and procedures may cover the production evaluations at the contractors manufacturing plant, or may require the T&E effort to establish and mature the processes. Therefore, the appropriate level of evaluation could range from none, for normal DCMA practices, to minimal for first article qualification checks, to more extensive evaluations based upon PQT results for new or unique manufacturing techniques, especially with new technologies. The sustainment evaluation discussions should address key risks or issues in sustaining or assessing the system capability in operational use. The sustainment evaluation discussion should address the overall T&E logistics effort, maintenance (both corrective and preventative), servicing, calibration, and support aspects.

The discussion of mission context evaluations addresses the approach to evaluate operational effectiveness and operational suitability of the system for use by typical users in the intended mission environments. This should also include joint operations issues. These evaluations provide a prediction of how well the system will perform in field use as well as in IOT&E, and may reduce the scope of the IOT&E, but will not replace or eliminate the need for IOT&E.

COIs also prove relevant to this discussion. COIs act as key operational effectiveness or operational suitability issues requiring examination in OT&E to determine the systems capability to perform its mission. COIs must be relevant to the required capabilities and of key importance to the systems operationally effectiveness, operationally suitability and survivability, and represent a significant risk if not satisfactorily resolved.

The strategy for T&E must include those evaluations required by statute, specifically IOT&E, survivability or operational security, and lethality. The IOT&E discussion should

describe the approach to conduct the independent evaluation of the system, including official resolution of COIs. The discussion of the approach to evaluate the survivability or operational security /lethality of the system should show how it will influence the development and maturation of the system design. The discussion should include a description of the overall live fire evaluation strategy for the system (as defined in section 2366 of title 10 USC); critical live fire evaluation issues; and any major evaluation limitations.

9.5.5.2. Evaluation Framework

The Evaluation Framework Matrix describes in table format the most important links and relationships between the types of testing conducted to support the entire acquisition program. It also shows the linkages between the KPPs/KSAs, CTPs, key test measures (i.e., MOEs, MOSs), planned test methods, key test resources (i.e., facility and infrastructure), and the decisions supported. Table 9.5.5.2.T1. depicts Top-Level Evaluation Framework Matrix from the TEMP format annex (and shown below) shows a notional Evaluation Framework Matrix. Programs may also use equivalent Service-specific formats identifying the same relationships and information. **Note:** the Evaluation Framework Matrix provides a tabular summary of the evaluation strategy.

Table 9.5.5.2.T1. Top-Level Evaluation Framework Matrix

Key Requirements and T&E Measures				**Test Methodologies/Key Resources (M&S, SIL, MF, ISTF, HITL, OAR)**	**Decision Supported**
Key Reqs	**COIs**	**Key MOEs/ MOSs**	**CTPs & Threshold**		
KPP#1:	**COI #1.** Is the XXX effective for	**MOE 1.1.**	Engine thrust	Chamber measurement Observation of performance profiles OAR	PDR CDR
	COI #2. Is the XXX suitable for		Data upload time	Component level replication Stress and Spike testing in SIL	PDR CDR
	COI #3. Can the XXX be	**MOS 2.1.**			MS-C FRP
		MOE 1.3.			Post-CDR FRP

		MOE 1.4.	Reliability based on growth curve	Component level stress testing Sample performance on growth curve Sample performance with M&S augmentation	PDR CDR MS-C
KPP #2		**MOS 2.4.**	Data link		MS-C SRR
KPP #3	**COI #4.** Is training.	**MOE 1.2.**		Observation and Survey	MS-C FRP
KSA #3.a	**COI #5.** Documentation	**MOS 2.5.**			MS-C FRP

The Evaluation Framework Matrix acts as a key tool used to capture all major parts of a complete T&E program, identify gaps in coverage, and ensure more efficient integrated testing. Programs must include it in Part III of the TEMP and base it on the strategy for T&E (aka evaluation strategy) developed at Milestone A. The Evaluation Framework Matrix should succinctly enumerate the top-level, key values and information for all types of T&E. Updates should occur as the system matures and the updating of source documents (e.g., CDD/CPD, AS, STAR, SEP, ISP). Include demonstrated values for measures and parameters as the acquisition program advances from milestone to milestone and as the updating of the TEMP.

Three major sections comprise the Evaluation Framework Matrix: Key Requirements and T&E Measures; Test Methodologies/Key Resources; and Decisions Supported. When filled in, readers can scan the matrix horizontally and see all linkages from the beginning of a program (i.e., from the requirement document) to the decision supported. Each requirement should associate with at least one or more T&E issues and measures. However, T&E measures can exist without an associated key requirement or COI/ COI Criteria (COIC). Hence, some cells in Table 9.5.5.2.T1. may be void.

Key Requirements and T&E Measures These include KPPs and KSAs and the top-level T&E issues and measures for evaluation. The top-level T&E issues would typically include COIs and COIC, CTPs, and key MOEs/MOSs. This should also include SoS issues. Each measure should be associated with one or more key requirements. However, there could be T&E measures without an associated key requirement or COI/COIC. Hence, some cells in Table 9.5.5.2.T1. of the TEMP may be void. A simple test to determine if this section of the matrix is minimally adequate is to confirm that each decision supported has at least one T&E measure associated with it, and each key requirement also has at least one T&E measure associated with it. Outside of that, only

include the T&E issues and measures that drive size or scope of the T&E program.

Test Methodologies/Key Resources These identify test methodologies or key resources necessary to generate data for evaluations to support decisions. The content of this column should indicate the key methodologies or significant resources required. Test methodology refers to high-level descriptions of methods used to obtain the data. For example, modeling and simulation, system integration lab, or open-air range, each represents a different methodology for obtaining test data. Where multiple methodologies are acceptable, it is necessary to show the preferred methodology utilized. Short notes or acronyms should be used to identify the methodology. Models or simulations should be identified with the specific name or acronym.

Decisions Supported these are the major design, developmental, manufacturing, programmatic, acquisition, or employment decisions driving the need for knowledge to be obtained through T&E. These decisions include acquisition milestones, design reviews, certifications, safety releases, production acceptance, and operational employment/deployment. The operational employment/deployment decisions include those made by operators and maintainers that drive the need for validated operating and maintenance manuals. The decisions supported column would not contain each decision an operator or maintainer would make, but just the overall level of knowledge needed for operating or maintenance data or instructions, or those that steer significant or top-level decisions. The key determinant for what to include in this section is whether the decision supported (or knowledge requirement) drives trade space for performance, cost or schedule, or the size or scope of the T&E program. Only those decisions that facilitate program decisions or the size or scope of the T&E program should be included.

If portions of any T&E activity are missing, those become immediately evident. For example, if a KPP for reliability, availability, and maintainability (RAM) is listed, then there must be a supporting COI (or criterion in the set of COIC), along with CTPs and MOSs, to show that RAM will be fully evaluated in DT&E and OT&E. Specifically in the case of RAM measures, many acquisition programs included little to no RAM testing in DT&E and subsequently failed Suitability in OT&E (i.e., were rated "Not Suitable" by DOT&E). Had the TEMPs for those programs contained a full Evaluation Framework Matrix, the weak or missing RAM areas may have been identified early and properly tested before systems reached OT&E. Increasing the visibility of all key measures will help ensure these areas are developed and properly tested in DT&E and are ready for OT&E.

The Evaluation Framework Matrix also aids integrated testing and systems engineering by providing a broad outline of the linkages and corresponding areas for each kind of T&E activity. Mutual support between tests can be planned based on these linkages. For example, DT&E can augment the high visibility areas in OT&E, and OT&E can "right-size" their T&E concept based on what they can use in DT&E. More synergy is possible where DT and OT measures are the same or similar, or where the same T&E resources (test articles and/or facilities) are used. Data sharing protocols can be

developed early to aid test planning. DOD Information Assurance Certification and Accreditation Process(s) (DIACAP's) Certification & Accreditation (C&A) requirements can be folded in early. Redundancy and gaps can be spotted and eliminated. Greater visibility and transparency between T&E activities will generate countless ways to enhance integration. The discussion of the evaluation strategy can fill in all the details.

Table 9.5.5.2.T2. provides key inputs within the TEMP.

Table 9.5.5.2.T2 Key Inputs within the TEMP

TEMP	**Milestone**	
	B **(Updated from MS A when developed)**	**C** **(Updated from MS B)**
Part I, Introduction		
	Include Purpose	
	Include Mission Description	
	Include System Description	
	Include System Threat Assessment	
	Include Program Background	
	Include Key Capabilities / SE Requirements	
Part II, Management & Schedule		
	Include T&E Management / Organizational Construct	
	Include Common T&E Database Requirements (for integrated testing)	
	Include Deficiency Reporting	
	Include TEMP Update	
	Include Integrated Test Program Schedule within the TEMP, updated prior to each MS.	
Part III, T&E Strategy		
	Evaluation Framework Matrix (cross referenced with; COIs (or COIC), KPPs, CTPs, KSAs, MOPs, MOEs, & MOSs)	
	Should describe planned DT&E, OT&E and LFT&E in detail. Include overview and use of integrated test (CT, DT&E, & OT&E) and list out those events requiring stand-alone (or dedicated) Government DT&E and OT&E. Delineate test limitations (Annotate by DT&E, LFT&E, or OT&E).	
	A list of supporting interfaces, consistent with the ISP/TISP. SV-5b should be included with each interface cross-referenced to any planned EMD phase T&E or C&A activities utilizing each interface.	Provide for operational evaluation of mission-level interoperability across key interfaces.

	Plan for the conduct of dedicated Government DT&E or integrated test (lead by Government personnel) to provide confidence that the system design solution is on track to satisfy the desired capabilities.	A listing of all test events within the dedicated IOT&E
	Identify Lead Government DT&E organization.	
	Plan for one full-up system level government DT&E event and at least one OA with intended operational users.	
	Reliability Growth Curve(s) (RGCs) reflecting the reliability growth plans at the appropriate level of analysis for the program	Updated RGC
	Listing of all commercial and NDIs	
	Provide a tabulation of factors	
	Determination of critical interfaces and information security	
	The TEMP should describe the T&E program in sufficient detail for decision makers to determine whether the planned activities are adequate to achieve the T&E objectives for the program.	
	Identify each test event as Contractor or Government DT&E	
	Identify M&S to be used and VV&A process. Annotate supporting usage (i.e., DT&E or OT&E)	
	T&E Support of Reliability Growth Plan	
	Plan for data collection	
	The TEMP should identify entrance and exit criteria and their associated test events or test periods.	
	The TEMP should consider the potential impacts on the environment and on personnel.	
Part IV, Resource Summary		
	The TEMP should describe the resources required in sufficient detail and aligned with Part III of the TEMP.	
	Programs should maximize the use DoD Government T&E capabilities and invest in Government T&E infrastructure unless an exception can be justified as cost-effective to the Government.	

9.5.5.3. TEMP Format

TEST AND EVALUATION MASTER PLAN

FOR

PROGRAM TITLE/SYSTEM NAME

ACRONYM

ACAT Level

Program Elements

Xxxxx

****

SUBMITTED BY

_____ _____

Program Manager DATE

CONCURRENCE

_____ _____

Program Executive Officer or Developing Agency DATE

(If not under the Program Executive Officer structure)

_____ _____

Operational Test Agency DATE

_____ _____

Users Representative DATE

DoD COMPONENT APPROVAL

_____ _____

DoD Component Test and Evaluation Director DATE

_____ _____

DoD Component Acquisition Executive (Acquisition Category I) DATE

Milestone Decision Authority (for less-than-Acquisition Category I)

Note: For Joint/Multi Service or Agency Programs, each Service or Defense Agency should provide a signature page for parallel staffing through its CAE or Director, and a separate page should be provided for OSD Approval

****

OSD APPROVAL

_____ _____

DASD(DT&E) DATE

_____ _____

D,OT&E DATE

TABLE OF CONTENTS

APPENDIX B ACRONYMS

APPENDIX C POINTS OF CONTACT

ADDITIONAL APPENDICES AS NEEDED

1. PART I - INTRODUCTION

1.1. **Purpose**.

- State the purpose of the Test and Evaluation Master Plan (TEMP).
- Identify if this is an initial or updated TEMP.
- State the Milestone (or other) decision the TEMP supports.
- Reference and provide hyperlinks to the documentation initiating the TEMP (i.e., Initial Capability Document (ICD), Capability Development Document (CDD), Capability Production Document (CPD), Acquisition Program Baseline (APB), Acquisition Strategy Report (ASR), Concept of Operations (CONOPS)).
- State the Acquisition Category (ACAT) level, operating command(s), and if listed on the OSD T&E Oversight List (actual or projected)

1.2. **Mission Description**.

- Briefly summarize the mission need described in the program capability requirements documents in terms of the capability it will provide to the Joint Forces Commander.
- Describe the mission to be accomplished by a unit equipped with the system using all applicable CONOPS and Concepts of Employment.
- Incorporate an OV-1 of the system showing the intended operational environment.
- Also include the organization in which the system will be integrated as well as
- [Include] significant points from the Life Cycle Sustainment Plan, the Information Support Plan, and Program Protection Plan.
    - Provide links to each document referenced in the introduction.
- For business systems, include a summary of the business case analysis for the program.

1.3 **. System Description**.

- Describe the system configuration.
- Identify key features and subsystems, both hardware and software (such as architecture, system and user interfaces, security levels, and reserves) for the planned increments within the Future Years Defense Program (FYDP).

1.3.1. System Threat Assessment.

- Succinctly summarize the threat environment (to include cyber-threats) in which

the system will operate.
- Reference the appropriate DIA or component-validated threat documents for the system.

1.3.2. Program Background.

- Reference the Analysis of Alternatives (AoA), the APB and the materiel development decision to provide background information on the proposed system.
- Briefly describe the overarching Acquisition Strategy (for space systems, the Integrated Program Summary (IPS)), and the Technology Development Strategy (TDS).
- Address whether the system will be procured using an incremental development strategy or a single step to full capability.
- If it is an evolutionary acquisition strategy, briefly discuss planned upgrades, additional features and expanded capabilities of follow-on increments.
    - The main focus must be on the current increment with brief descriptions of the previous and follow-on increments to establish continuity between known increments.

1.3.2.1. Previous Testing.

- Discuss the results of any previous tests that apply to, or have an effect on, the test strategy.

1.3.3. Key Capabilities.

- Identify the Key Performance Parameters (KPPs) and Key System Attributes (KSAs) for the system.
    - For each listed parameter, provide the threshold and objective values from the CDD/CPD and reference the paragraph.

1.3.3.1. Key Interfaces.

- Identify interfaces with existing or planned systems architectures that are required for mission accomplishment.
- Address integration and modifications needed for commercial items.
- Include interoperability with existing and/or planned systems of other Department of Defense (DoD) Components, other Government agencies, or Allies.
- Provide a diagram of the appropriate DoD Architectural Framework (DoDAF) system operational view from the CDD or CPD.

1.3.3.2. Special test or certification requirements.

- Identify unique system characteristics or support concepts that will generate special test, analysis, and evaluation requirements

    - (e.g., security test and evaluation and Information Assurance (IA) Certification and Accreditation (C&A),
    - post deployment software support,
    - resistance to chemical, biological, nuclear, and radiological effects;
    - resistance to countermeasures;
    - resistance to reverse engineering/exploitation efforts (Anti-Tamper);
    - development of new threat simulation, simulators, or targets.

1.3.3.3. Systems Engineering (SE) Requirements.

- Reference all SE-based information that will be used to provide additional system evaluation targets driving system development.
    - Examples could include hardware reliability growth and software maturity growth strategies.
    - The SEP should be referenced in this section and aligned to the TEMP with respect to SE Processes, methods, and tools identified for use during T&E.

2. PART II TEST PROGRAM MANAGEMENT AND SCHEDULE

2.1 **T&E Management**.

- Discuss the test and evaluation responsibilities of all participating organizations (such as developers, testers, evaluators, and users).
- Describe the role of contractor testing in early system development.
- Describe the role of government developmental testers to assess and evaluate system performance.
- Describe the role of the Operational Test Agency (OTA) /operational testers to confirm operational effectiveness, operational suitability and survivability.

2.1.1. T&E Organizational Construct.

- Identify the organizations or activities (such as the T&E Working-level Integrated Product Team (WIPT) or Service equivalent, LFT&E IPT, etc.) in the T&E management structure, to include the sub-work groups, such as a modeling & simulation, or reliability.
- Provide sufficient information to adequately understand the functional relationships. Reference the T&E WIPT charter that includes specific responsibilities and deliverable items for detailed explanation of T&E management.
    - These items include TEMPs and Test Resource Plans (TRPs) that are produced collaboratively by member organizations.

2.2. **Common T&E Database Requirements**.

- Describe the requirements for and methods of collecting, validating, and sharing

data as it becomes available from the contractor, Developmental Test (DT), Operational Test (OT), and oversight organizations, as well as supporting related activities that contribute or use test data (e.g., information assurance C&A, interoperability certification, etc.).
- Describe how the pedigree of the data will be established and maintained. The pedigree of the data refers to understanding the configuration of the test asset, and the actual test conditions under which the data were obtained for each piece of data.
- State who will be responsible for maintaining this data.

2.3. **Deficiency Reporting**.

- Briefly describe the processes for documenting and tracking deficiencies identified during system development and testing.
- Describe how the information is accessed and shared across the program.
- The processes should address problems or deficiencies identified during both contractor and government test activities.
- The processes should also include issues that have not been formally documented as a deficiency (e.g., watch items).

2.4. **TEMP Updates**.

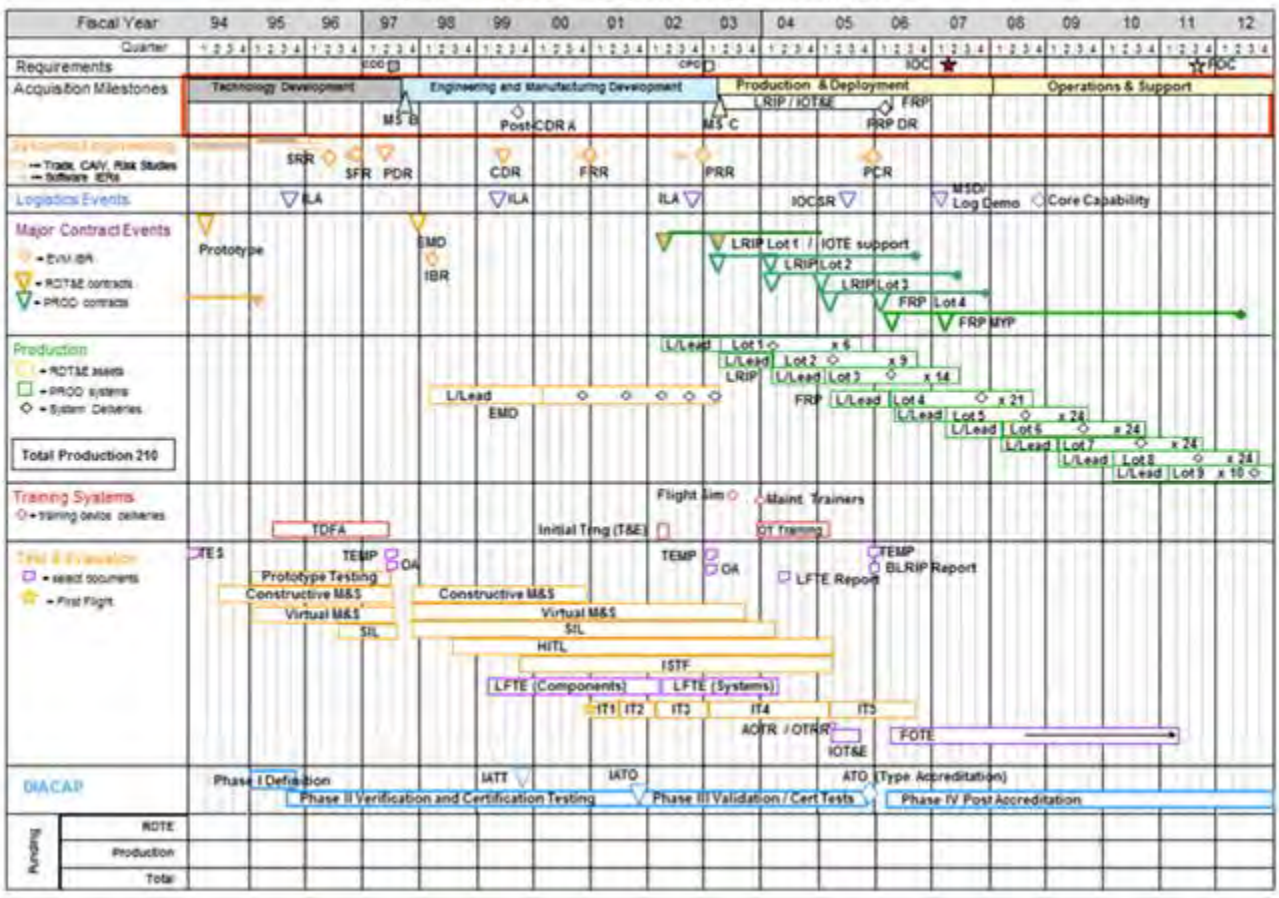
- Reference instructions for complying with DoDI 5000.02 required updates or identify exceptions to those procedures if determined necessary for more efficient administration of document.
- Provide guidelines for keeping TEMP information current between updates.
- For a Joint or Multi-Service TEMP, identify references that will be followed or exceptions as necessary.

2.5. **Integrated Test Program Schedule**.

- Display (see Figure 2.1) the overall time sequencing of the major acquisition phases and milestones (as necessary, use the NSS-03-01 time sequencing).
    - Include the test and evaluation major decision points, related activities, and planned cumulative funding expenditures by appropriation by year.
    - Include event dates such as
        - Major decision points as defined in DoD Instruction 5000.02, e.g., operational assessments,
        - Preliminary and critical design reviews,
        - Test article availability; software version releases;
        - Appropriate phases of DT&E; LFT&E; Joint Interoperability Test Command (JITC) interoperability testing and certification date to support the MS-C and Full-Rate Production (FRP) Decision Review (DR).
        - Include significant Information Assurance certification and accreditation event sequencing, such as Interim Authorization to

Test (IATT), Interim Authorization to Operate (IATO) and Authorization to Operate (ATO).
    - Also include operational test and evaluation;
    - Low-Rate Initial Production (LRIP) deliveries;
    - Initial Operational Capability (IOC); Full Operational Capability (FOC);
    - Statutorily required reports such as the Live-Fire T&E Report and Beyond Low-Rate Initial Production (B-LRIP) Report.
- Provide a single schedule for multi-DoD Component or Joint and Capstone TEMPs showing all related DoD Component system event dates.

Figure 2.1 SAMPLE Integrated Program Test Schedule



3. PART III TEST AND EVALUATION STRATEGY

3.1 T&E Strategy .

- Introduce the program T&E strategy by briefly describing how it supports the acquisition strategy as described in Section 1.3.2. This section should summarize an effective and efficient approach to the test program.
- The developmental and operational test objectives are discussed separately

below; however this section must also address how the test objectives will be integrated to support the acquisition strategy by evaluating the capabilities to be delivered to the user without compromising the goals of each major kind of test type.
- Where possible, the discussions should focus on the testing for capabilities, and address testing of subsystems or components where they represent a significant risk to achieving a necessary capability.
- As the system matures and production representative test articles are available, the strategy should address the conditions for integrating DT and OT tests.
- Evaluations shall include a comparison with current mission capabilities using existing data, so that measurable improvements can be determined.
    - If such evaluation is considered costly relative to the benefit's gained, the PM shall propose an alternative evaluation strategy.
    - Describe the strategy for achieving this comparison and for ensuring data are retained and managed for future comparison results of evolutionary increments or future replacement capabilities.
- To present the programs T&E strategy, briefly describe the relative emphasis on methodologies (e.g., Modeling and Simulation (M&S), Measurement Facility (MF), Systems Integration Laboratory (SIL), Hardware-In-the-Loop Test (HILT), Installed System Test Facility (ISTF), Open Air Range (OAR)).

3.2. Evaluation Framework .

- Describe the overall evaluation approach focusing on key decisions in the system lifecycle and addressing key system risks, program unique Critical Operational Issues (COIs) or Critical Operational Issue Criteria (COIC), and Critical Technical Parameters (CTPs).
- Specific areas of evaluation to address are related to the:

(1) Development of the system and processes (include maturation of system design)

(2) System performance in the mission context

(3) OTA independent assessments and evaluations

(4) Survivability and/or lethality

(5) Comparison with existing capabilities, and

(6) Maturation of highest risk technologies

- Describe any related systems that will be included as part of the evaluation approach for the system under test (e.g., data transfer, information exchange requirements, interoperability requirements, and documentation systems).

- Also identify any configuration differences between the current system and the

system to be fielded.
    - Include mission impacts of the differences and the extent of integration with other systems with which it must be interoperable or compatible.
- Describe how the system will be evaluated and the sources of the data for that evaluation.
    - The discussion should address the key elements for the evaluations, including major risks or limitations for a complete evaluation of the increment undergoing testing.
    - The reader should be left with an understanding of the value-added of these evaluations in addressing both programmatic and warfighter decisions or concerns.
    - This discussion provides rationale for the major test objectives and the resulting major resource requirements shown in Part IV - Resources.
- Include a Top-Level Evaluation Framework matrix that shows the correlation between the KPPs/KSAs, CTPs, key test measures (i.e., Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs)), planned test methods, and key test resources, facility or infrastructure needs.
    - When structured this way, the matrix should describe the most important relationships between the types of testing that will be conducted to evaluate the Joint Capabilities Integration and Development System (JCIDS)-identified KPPs/KSAs, and the programs CTPs.
    - Figure 3.1 shows how the Evaluation Framework could be organized. Equivalent Service-specific formats that identify the same relationships and information may also be used.
    - The matrix may be inserted in Part III if short (less than one page), or as an annex.
    - The evaluation framework matrix should mature as the system matures. Demonstrated values for measures should be included as the acquisition program advances from milestone to milestone and as the TEMP is updated.

The suggested content of the evaluation matrix includes the following:

- Key requirements & T&E measures These are the KPPs and KSAs and the top-level T&E issues and measures for evaluation. The top-level T&E issues would typically include COIs/Critical Operational Issues and Criteria (COICs), CTPs, and key MOEs/MOSs. System-of-Systems and technical review issues should also be included, either in the COI column or inserted as a new column. Each T&E issue and measure should be associated with one or more key requirements. However, there could be T&E measures without an associated key requirement or COI/COIC. Hence, some cells in figure 3.1 may be empty.
- Overview of test methodologies and key resources These identify test methodologies or key resources necessary to generate data for evaluating the COIs/COICs, key requirements, and T&E measures. The content of this column should indicate the methodologies/resources that will be required and short notes or pointers to indicate major T&E phases or resource names. M&S should be

identified with the specific name or acronym.

- Decisions Supported These are the major design, developmental, manufacturing, programmatic, acquisition, or employment decisions most affected by the knowledge obtained through T&E.

Figure 3.1, Top-Level Evaluation Framework Matrix

Key Requirements and T&E Measures				**Test Methodologies/Key Resources (M&S, SIL, MF, ISTF, HITL, OAR)**	**Decision Supported**
Key Reqs	**COIs**	**Key MOEs/ MOSs**	**CTPs & Threshold**		
KPP#1:	**COI #1.** Is the XXX effective for	**MOE 1.1.**	Engine thrust	Chamber measurement Observation of performance profiles OAR	PDR CDR
	COI #2. Is the XXX suitable for		Data upload time	Component level replication Stress and Spike testing in SIL	PDR CDR
	COI #3. Can the XXX be	**MOS 2.1.**			MS-C FRP
		MOE 1.3.			Post-CDR FRP
		MOE 1.4.	Reliability based on growth curve	Component level stress testing Sample performance on growth curve Sample performance with M&S augmentation	PDR CDR MS-C
KPP #2		**MOS 2.4.**	Data link		MS-C SRR
KPP #3	**COI #4.** Is training.	**MOE 1.2.**		Observation and Survey	MS-C FRP
KSA #3.a	**COI #5.** Documentation	**MOS 2.5.**			MS-C FRP

3.3. Developmental Evaluation Approach.

- Describe the top-level approach to evaluate system and process maturity, as well as, system capabilities and limitations expected at acquisition milestones and decision review points.

- The discussion should include logistics, reliability growth, and system performance aspects.
- Within this section, also discuss:

1) rationale for CTPs (see below for a description of how to derive CTPs),

2) key system or process risks,

3) any certifications required (e.g. weapon safety, interoperability, spectrum approval, information assurance),

4) any technology or subsystem that has not demonstrated the expected level of technology maturity at level 6 (or higher), system performance, or has not achieved the desired mission capabilities for this phase of development,

5) degree to which system hardware and software design has stabilized so as to determine manufacturing and production decision uncertainties,

6) key issues and the scope for logistics and sustainment evaluations, and

7) reliability thresholds when the testing is supporting the systems reliability growth curve.

- **CTPs are measurable critical system characteristics that, if not achieved, preclude the fulfillment of desired operational performance capabilities.** While not user requirements, CTPs are technical measures derived from desired user capabilities. Testers use CTPs as reliable indicators that the system is on (or behind) the planned development schedule or will likely (or not likely) achieve an operational capability.

- Limit the list of CTPs to those that support the COIs. Using the system specification as a reference, the chief engineer on the program should derive the CTPs to be assessed during development.

3.3.1. Mission-Oriented Approach.

- Describe the approach to evaluate the system performance in a mission context during development in order to influence the design, manage risk, and predict operational effectiveness and operational suitability.

- A mission context focuses on how the system will be employed. Describe the

rationale for the COIs or COICs.

3.3.2. Developmental Test Objectives.

- Summarize the planned objectives and state the methodology to test the system attributes defined by the applicable capability requirement document (CDD, CPD, CONOPs) and the CTPs that will be addressed during each phase of DT as shown in Figure 3.1, Top-Level Evaluation Framework matrix and the Systems Engineering Plan.

- Subparagraphs can be used to separate the discussion of each phase.
- For each DT phase, discuss the key test objectives to address both the contractor and government developmental test concerns and their importance to achieving the exit criteria for the next major program decision point.
- If a contractor is not yet selected, include the developmental test issues addressed in the Request For Proposals (RFPs) or Statement of Work (SOW).
- Discuss how developmental testing will reflect the expected operational environment to help ensure developmental testing is planned to integrate with operational testing.
- Also include key test objectives related to logistics testing.
- All objectives and CTPs should be traceable in the Top-Level Evaluation Framework matrix to ensure all KPPs/KSAs are addressed, and that the COIs/COICs can be fully answered in operational testing.
- Summarize the developmental test events, test scenarios, and the test design concept.
- Quantify the testing sufficiently (e.g., number of test hours, test articles, test events, test firings) to allow a valid cost estimate to be created.
- Identify and explain how models and simulations, specific threat systems, surrogates, countermeasures, component, or subsystem testing, Testbeds, and prototypes will be used to determine whether or not developmental test objectives are achieved.
- Identify the DT&E reports required to support decision points/reviews and OT readiness.
- Address the systems reliability growth strategy, goals, and targets and how they support the Evaluation Framework.
- Detailed developmental test objectives should be addressed in the System Test Plans and detailed test plans.

3.3.3. Modeling & Simulation (M&S).

- Describe the key models and simulations and their intended use.
- Include the developmental test objectives to be addressed using M&S to include any approved operational test objectives.
- Identify data needed and the planned accreditation effort.
- Identify how the developmental test scenarios will be supplemented with M&S, including how M&S will be used to predict the Sustainment KPP and other

sustainment considerations.
- Identify who will perform M&S verification, validation, and accreditation. Identify developmental M&S resource requirements in Part IV.

3.3.4. Test Limitations.

- Discuss any developmental test limitations that may significantly affect the evaluator's ability to draw conclusions about the maturity, capabilities, limitations, or readiness for dedicated operational testing.
    - Also address the impact of these limitations, and resolution approaches.

3.4. Live Fire Test and Evaluation Approach.

- If live fire testing is required, describe the approach to evaluate the survivability/lethality of the system, and (for survivability LFT&E) personnel survivability of the systems occupants.
- Include a description of the overall live fire evaluation strategy to influence the system design (as defined in Title 10 U.S.C. 2366), critical live fire evaluation issues, and major evaluation limitations.
- Discuss the management of the LFT&E program, to include the shot selection process, target resource availability, and schedule.
- Discuss a waiver, if appropriate, from full-up, system-level survivability testing, and the alternative strategy.

3.4.1. Live Fire Test Objectives.

- State the key live fire test objectives for realistic survivability or lethality testing of the system.
- Include a matrix that identifies all tests within the LFT&E strategy, their schedules, the issues they will address, and which planning documents will be submitted for DOT&E approval and which will be submitted for information and review only.
- Quantify the testing sufficiently (e.g., number of test hours, test articles, test events, test firings) to allow a valid cost estimate to be created.

3.4.2. Modeling & Simulation (M&S).

- Describe the key models and simulations and their intended use.
- Include the LFT&E test objectives to be addressed using M&S to include operational test objectives. Identify data needed and the planned accreditation effort.
- Identify how the test scenarios will be supplemented with M&S.
- Identify who will perform M&S verification, validation, and accreditation. Identify M&S resource requirements in Part IV

3.4.3. Test Limitations.

- Discuss any test limitations that may significantly affect the ability to assess the systems vulnerability and survivability.
    - Also address the impact of these limitations, and resolution approaches.

3.5. Certification for Initial Operational Test and Evaluation (IOT&E).

- Explain how and when the system will be certified safe and ready for IOT&E.
- Explain who is responsible for certification and which decision reviews will be supported using the lead Services certification of safety and system materiel readiness process.
- List the DT&E information (i.e., reports, briefings, or summaries) that provides predictive analyses of expected system performance against specific COIs and the key system attributes - MOEs/MOSs.
- Discuss the entry criteria for IOT&E and how the DT&E program will address those criteria.

3.6. Operational Evaluation Approach.

- Describe the approach to conduct the independent evaluation of the system.
- Identify the periods during integrated testing that may be useful for operational assessments and evaluations.
- Outline the approach to conduct the dedicated IOT&E and resolution of the COIs.
    - COIs must be relevant to the required capabilities and of key importance to the system being operationally effective, operationally suitable and survivable, and represent a significant risk if not satisfactorily resolved. A COI/COIC is typically phrased as a question that must be answered in the affirmative to properly evaluate operational effectiveness (e.g., "Will the system detect the threat in a combat environment at adequate range to allow successful engagement?") and operational suitability (e.g., "Will the system be safe to operate in a combat environment?"). COIs/COICs are critical elements or operational mission objectives that must be examined.
    - COIs/COICs should be few in number and reflect total operational mission concerns. Use existing documents such as capability requirements documents, Business Case Analysis, AoA, APB, war fighting doctrine, validated threat assessments and CONOPS to develop the COIs/COICs.
    - COIs/COICs must be formulated as early as possible to ensure developmental testers can incorporate mission context into DT&E.
    - If every COI is resolved favorably, the system should be operationally effective and operationally suitable when employed in its intended environment by typical users.

3.6.1. Operational Test Objectives.

- State the key MOEs/MOSs that support the COIs/COICs.

- Ensure the operational tests can be identified in a way that allows efficient DOT&E approval of the overall OT&E effort in accordance with Title 10 U.S.C. 139(d).
- Describe the scope of the operational test by identifying the test mission scenarios and the resources that will be used to conduct the test.
- Summarize the operational test events, key threat simulators and/or simulation(s) and targets to be employed, and the type of representative personnel who will operate and maintain the system.
- Identify planned sources of information (e.g., developmental testing, testing of related systems, modeling, simulation) that may be used to supplement operational test and evaluation.
- Quantify the testing sufficiently (e.g., number of test hours, test articles, test events, test firings) to allow a valid cost estimate to be created.

3.6.2. Modeling & Simulation (M&S).

- Describe the key models and simulations and their intended use.
- Include the operational test objectives to be addressed using M&S. Identify data needed and the planned accreditation effort.
- Identify how the operational test scenarios will be supplemented with M&S.
- Identify who will perform the M&S verification, validation, and accreditation.
- Identify operational M&S resource requirements in Part IV.

3.6.3. Test Limitations.

- Discuss test limitations including threat realism, resource availability, limited operational (military; climatic; Chemical, Biological, Nuclear, and Radiological (CBNR), etc.) environments, limited support environment, maturity of tested systems or subsystems, safety, that may impact the resolution of affected COIs.
- Describe measures taken to mitigate limitations.
- Indicate if any system contractor involvement or support is required, the nature of that support, and steps taken to ensure the impartiality of the contractor providing the support according to Title 10 U.S.C. 2399.
- Indicate the impact of test limitations on the ability to resolve COIs and the ability to formulate conclusions regarding operational effectiveness and operational suitability. Indicate the COIs affected in parenthesis after each limitation.

3.7. Other Certifications.

- Identify key testing prerequisites and entrance criteria, such as required certifications (e.g. DoD Information Assurance Certification and Accreditation Process (DIACAP) Authorization to Operate, Weapon Systems Explosive Safety Review Board (WSERB), flight certification, etc.)

3.8. Reliability Growth.

- Since reliability is a driver during system development, identify, in tabular form, the amount of operating time being accrued during the each of the tests listed in the Figure 2.1.
    - Table should contain the system configuration, operational concept, etc. Reference and provide hyperlinks to the reliability growth planning document.

3.9. Future Test and Evaluation.

- Summarize all remaining significant T&E that has not been discussed yet, extending through the system life cycle.
    - Significant T&E is that T&E requiring procurement of test assets or other unique test resources that need to be captured in the Resource section.
    - Significant T&E can also be any additional questions or issues that need to be resolved for future decisions.
    - Do not include any T&E in this section that has been previously discussed in this part of the TEMP.

4. PART IV-RESOURCE SUMMARY

4.1. Introduction.

- In this section, specify the resources necessary to accomplish the T&E program.
- Testing will be planned and conducted to take full advantage of existing DoD investment in ranges, facilities, and other resources wherever practical.
- Provide a list in a table format (see Table 4.1) including schedule (**Note:** ensure list is consistent with figure 2.1 schedule) of all key test and evaluation resources, both government and contractor, that will be used during the course of the current increment. Include long-lead items for the next increment if known.
- Specifically, identify the following test resources and identify any shortfalls, impact on planned testing, and plan to resolve shortfalls.

4.1.1. Test Articles.

- Identify the actual number of and timing requirements for all test articles, including key support equipment and technical information required for testing in each phase of DT&E, LFT&E, and OT&E.
    - If key subsystems (components, assemblies, subassemblies or software modules) are to be tested individually, before being tested in the final system configuration, identify each subsystem in the TEMP and the quantity required.
- Specifically identify when prototype, engineering development, or production models will be used.

4.1.2. Test Sites and Instrumentation.

- Identify the specific test ranges/facilities and schedule to be used for each type of testing.
- Compare the requirements for test ranges/facilities dictated by the scope and content of planned testing with existing and programmed test range/facility capability.
- Identify instrumentation that must be acquired specifically to conduct the planned test program.

4.1.3. Test Support Equipment.

- Identify test support equipment and schedule specifically required to conduct the test program.
- Anticipate all test locations that will require some form of test support equipment. This may include test measurement and diagnostic equipment, calibration equipment, frequency monitoring devices, software test drivers, emulators, or other test support devices that are not included under the instrumentation requirements.

4.1.4. Threat Representation.

- Identify the type, number, availability, fidelity requirements, and schedule for all representations of the threat (to include threat targets) to be used in testing.
- Include the quantities and types of unit's and systems required for each of the test phases. Appropriate threat command and control elements may be required and utilized in both live and virtual environments.
- The scope of the T&E event will determine final threat inventory.

4.1.5. Test Targets and Expendables.

- Specify the type, number, availability, and schedule for all test targets and expendables, (e.g. targets, weapons, flares, chaff, sonobuoys, smoke generators, countermeasures) required for each phase of testing.
- Identify known shortfalls and associated evaluation risks.
- Include threat targets for LFT&E lethality testing and threat munitions for vulnerability testing.

4.1.6. Operational Force Test Support.

- For each test and evaluation phase, specify the type and timing of aircraft flying hours, ship steaming days, and on-orbit satellite contacts/coverage, and other operational force support required.
- Include supported/supporting systems that the system under test must interoperate with if testing a system-of-systems or family-of-systems.

- Include size, location, and type unit required.

4.1.7. Models, Simulations, and Testbeds.

- For each test and evaluation phase, specify the models and simulations to be used, including computer-driven simulation models and hardware/software-in-the-loop Testbeds.
- Identify opportunities to simulate any of the required support.
- Identify the resources required to validate and accredit their usage, responsible agency and timeframe.

4.1.8. Joint Mission Environment.

- Describe the live, virtual, or constructive components or assets necessary to create an acceptable environment to evaluate system performance against stated joint requirements.
- Describe how both DT and OT testing will utilize these assets and components.

4.1.9. Special Requirements.

- Identify requirements and schedule for any necessary non-instrumentation capabilities and resources such as: special data processing/data bases, unique mapping/charting/geodesy products, extreme physical environmental conditions or restricted/special use air/sea/landscapes.
- Briefly list any items impacting the T&E strategy or government test plans that must be put on contract or which are required by statute or regulation. These are typically derived from the JCIDS requirement (i.e., Programmatic Environment, Safety and Occupational Health Evaluation (PESHE) or Environment, Safety and Occupational Health (ESOH)).
- Include key statements describing the top-level T&E activities the contractor is responsible for and the kinds of support that must be provided to government testers.

4.2. Federal, State, and Local Requirements.

- All T&E efforts must comply with federal, state, and local environmental regulations.
- Current permit's and appropriate agency notifications will be maintained regarding all test efforts.
- Specify any National Environmental Policy Act documentation needed to address specific test activities that must be completed prior to testing and include any known issues that require mitigations to address significant environmental impacts.
- Describe how environmental compliance requirements will be met.

4.3. Manpower/Personnel and Training.

- Specify manpower/personnel and training requirements and limitations that affect test and evaluation execution. Identify how much training will be conducted with M&S.

4.4. Test Funding Summary.

- Summarize cost of testing by FY separated by major events or phases and within each Fiscal Year (FY) DT and OT dollars.
    - When costs cannot be estimated, identify the date when the estimates will be derived.

Table 4.1 Test Sites and Instrumentation Example

Fiscal Year		06	07	08	09	10	11	12	TBD
TEST EVENT TEST RESOURCE		IT-B1	IT-B2	IT-B2 / IT-C1	IT-C1	IT-C1	IT-C2	OT-C1	OT-D1
Integration Lab		X	X	X	X	X	X		
Radar Integration Lab		X	X	X	X	X	X		
Loads (flights)									
Operating Area #1 (flights)			X (1)	X (1)				X (1)	X (2)
Operating Area #2 (flights)			50 (1)	132 (1)	60	100	140	X (1)	X (2)
Northeast CONUS Overland (flights)			10					X (1)	X (2)
SOCAL Operating Areas (flights)					X		X		
Shielded Hangar (hours)				160			160		
Electromagnetic Radiation Facility (hours)				40			40		
Arresting Gear (Mk 7 Mod 3)(events)					10		10		
NAS Fallon					5	5	A/R	X (1)	X (2)
Link-16 Lab, Eglin AFB								X	
NAWCAD WD, China Lake Range								X	
Eglin AFB ESM Range								X	

1. Explanations as required.

2. Enter the date the funding will be available.

9.5.5.4. Other Milestone TEMPs and Updates

An updated TEMP is required as part of entry criteria for entering each acquisition phase, and at any time a major programmatic change occurs. For example, an updated TEMP may be required due to a change resulting in a CDR or configuration change, change to the acquisition strategy, or changes to capability requirements.

9.5.6. Contractual

9.5.7. Government T&E Program Support

9.5.6. Contractual

All contract preparation documents (RFP, statement of work) and contract documents (contract, Contract Data Requirements List (CDRL)) are to identify contractor requirements for conducting DT&E, and supporting government DT&E, OT&E, and LFT&E events. At a minimum, contract documents should provide for data rights to contractor performed DT&E, identification of M&S to be used, and the V&V methodology to be used. For more information, read the OSD "Incorporating Test and Evaluation into Department of Defense Acquisition Contracts" , dated October 2011.

9.5.7. Government T&E Program Support

The Department's program support implementation strategy includes establishment of key leadership positions (KLPs) that have a significant level of responsibility and authority and have proven key to the success of programs or efforts. The Services and Defense Agencies may designate any position which meets the criteria. However, the following have been identified as mandatory KLPs in Section 805, P.L. 111-84, National Defense Authorization Act for FY 2010 ; or have significant levels of responsibility and authority, proving essential for the success of a program:

- PEO/Deputy PEO
- PM (ACAT I, IA and II)
- DPM (DPM) (ACAT I)
- Senior Contracting Official
- MDAP/MAIS positions (ACAT I and IA) when the function is required based on the phase or type of acquisition program:
    - Program Lead SE
    - Program Lead Cost Estimator
    - Program Lead Contracting Officer
    - Program Lead Logistician (Product Support Manager)
    - Program Lead Business Financial Manager
    - Program Lead T&E
    - Program Lead Production, Quality, and Manufacturing
    - Program Lead IT

In general, the Service/Defense Agency should fill the "program lead" positions with military members at the lieutenant colonel/colonel or commander/Navy captain levels or by the civilian equivalent. Program leads advise the PM/DPM and may be matrixed to the program office. Although program leads may report to a higher-level functional (i.e., command/center functional lead or his or her direct report), these positions must be designated as KLPs. Program lead KLPs must be designated in the position category associated with the lead function. For example, "lead logistician" positions must be designated as positions in the "Life Cycle Logistics" position category.

Services/Defense Agencies will submit KLP metrics at Senior Steering Boards, in accordance with DoDI 5000.55 "Reporting Management Information on DoD Military and Civilian Acquisition Personnel and Positions," dated September 11, 1991. Mandatory metrics include KLP fill rates and qualification rates of workforce members assigned to KLPs.

9.5.8. System Readiness for Operational Test and Evaluation (OT&E)

9.5.8.1. Operational Test Readiness Process

9.5.8.2. System Readiness for IOT&E

9.5.8. System Readiness for Operational Test and Evaluation (OT&E)

9.5.8.1. Operational Test Readiness Process

DoD Components should develop and institutionalize processes to determine a systems performance and readiness for operational assessments and tests. These processes should focus on ensuring systems are in a realistic configuration and have demonstrated technical and production maturity under the expected operating conditions. Successful execution of these processes should enable the gathering of relevant and appropriate data, during integrated testing, to satisfy early operational test objectives prior to dedicated, operational testing.

9.5.8.2. System Readiness for IOT&E

For programs on the OSD T&E Oversight List for OT&E, the DoD CAE is required to evaluate and determine materiel system readiness for IOT&E. The intent of this requirement is to ensure systems do not enter IOT&E before they are sufficiently mature. Scarce resources are wasted when an IOT&E is halted or terminated early because of technical problems with the System Under Test (SUT); problems that should have been resolved prior to the start of IOT&E.

Prior to CAE determination of readiness for IOT&E, programs must have an independent AOTR for all ACAT I and IA programs, as well as any special interest programs designated by the DASD(DT&E). The AOTR will focus on the technical and materiel readiness of the program to proceed into IOT&E. Assessment results are

based on capabilities demonstrated in DT&E and earlier OAs. As outlined in DoDI 5000.02, Enclosure 6, paragraphs 4.b and 4.c, a DT&E report of results and the progress assessment shall be provided to the DASD(DT&E) and the DOT&E prior to the AOTR. That report can be a written document or a briefing to the DASD(DT&E) and DOT&E representatives, and should include the following: an analysis of the systems progress in achieving CTPs, satisfaction of approved IOT&E entrance criteria, a technical risk assessment, level of software maturity and status of software trouble reports, and predicted IOT&E results, including the impacts of any shortcomings on the systems expected performance during IOT&E. Provide the report at least 20 days prior to the CAE's determination of system readiness. This will allow OSD time to formulate and provide its recommendation to the CAE. All appropriate developmental and operational T&E organizations should be invited to the IOT&E readiness review.

The goal of the AOTR is to assess the risk associated with the system's ability to meet operational suitability and effectiveness goals, identify system and subsystem maturity levels, assess programmatic and technical risk, and provide risk mitigation recommendations. The results of the AOTR will be provided to the USD(AT&L), DOT&E, and CAE. As outlined in DoD Instruction 5000.02, Enclosure 6, paragraphs 4.b and 4.c, the CAE shall consider the results of the AOTR prior to making a determination of materiel readiness for IOT&E.

9.6. T&E Reporting

9.6.1. Milestone B Reporting

9.6.2. Milestone C Reporting

9.6. T&E Reporting

Programs on the OSD T&E Oversight List report to the appropriate OSD oversight organization(s) on a periodic or event-driven basis. Reports are required from the program office, the proposed lead DT&E Organization, and the lead OTA to assist OSD in preparation for the Milestone Decision Authority (MDA) review of system development and operational progress and risk, and for congressionally mandated annual reports.

9.6.1. Milestone B Reporting

The risk associated with a Milestone B decision, should be based on reports to the DASD(DT&E) and the DOT&E to permit assessments from the TD Phase for: (1) technology maturity, (2) performance of Critical Technology Element (CTEs) to meet CTPs or other performance parameter thresholds, and (3) adequacy of executing the test plan submitted for the TD Phase. The assessment (for TRLs for all CTEs) will be based on objective evidence gathered during events such as tests, demonstrations, pilots, or physics-based simulations. Based on the requirements, identified capabilities, system architecture, software architecture, CONOPS, and/or the concept of

employment, the IRT (Integrated Requirements Team) will define operationally relevant environments and determine which TRL is supported by the objective evidence. This metric would evaluate the adequacy of the test/demonstration approach used for determining the CTPs for each CTE; i.e., the confidence the DASD(DT&E) has that the CTE was appropriately stressed and the TRL was accurately assessed. This confidence will be based on a number of factors assessed by comparing test and/or evaluation reports with the approved TEMPs. Some of those factors may include adequacy of:

- Operationally relevant environment and/or end-to-end mission simulation
- Instrumentation/facility/range/threat representation
- Skills of test personnel
- Number of test articles
- Interfaces and integration
- Human Systems Integration considerations
- Government participation
- Use of design of experiments; e.g., sample size determination
- M&S VV&A
- Support vehicles/systems/services
- Highest fidelity test resource used in the DoD test process

9.6.2. Milestone C Reporting

Development of an OSD position on the risk of a Milestone C approval for initiating the Production and Deployment (P&D) Phase should be based on: (1) the DT&E results from the preceding EMD phase, including consideration of how thoroughly the system was stressed during EMD (mission-oriented context and operationally realistic environments); and (2) adequacy of the DT&E planning for the remaining P&D phase. EMD phase DT results and evaluations extracted from DT&E reports, OA results if the OTA conducted one, and action officer observations from monitoring EMD phase DT&E and participating in Program Support Review(s) (PSRs), WIPT meetings, test readiness reviews, and data analysis working group meetings to provide the basis for assessing whether Milestone C entrance criteria were met. Reporting should permit OSD to determine the adequacy of the TEMP the PM submits for Milestone C, knowledge of the mission and operating environment requirements, and knowledge of both T&E infrastructure capabilities (including threat surrogates) and the projected threat at the time of program IOC, and provide the basis for assessing the adequacy of P&D phase DT&E planning. The assessment based on DT&E results should speak directly to the maturity of the system being developed and its readiness to advance to the P&D phase; the assessment based on P&D Phase DT&E planning speaks directly to the adequacy of the planned DT&E to deliver a system that will succeed in IOT&E, and for assessing and articulating the risk associated with an acquisition program proceeding into LRIP and the P&D phase.

Reporting should demonstrate, based on the DT&E and OA results of EMD, the degree of compliance for:

- Acceptable performance in DT&E and OA
- Mature software capability
- Acceptable interoperability
- Acceptable operational supportability
- IA certification and acceptance

9.7. Special Topics

9.7.1. Network Centric Operations

9.7.2. Modeling and Simulation in T&E

9.7.3. Validation of Threat Representations (targets, threat simulators, or M&S)

9.7.4. Mission-oriented Context

9.7. Special Topics

9.7.1. Network Centric Operations

Implementation of the Department's transformation strategy, calling for shifting to an information-age military, will result in fewer platform-centric and more net-centric military forces. This requires increased information sharing across networks. The net-centric concept applies to a DoD enterprise-wide information management strategy that includes not only military force operations but also all defense business processes, such as personnel actions, fuel purchases and delivery, commodity buying, deployment and sustainment activities, acquisition and development. Key tenets of the strategy include: handle information only once, post data before processing it, users access data when it is needed, collaborate to make sense of data, and diversify network paths to provide reliable and secure network capabilities.

The shift away from point-to-point system interfaces to net-centric interfaces brings implications for the T&E community. The challenge to the test community will be to represent the integrated architecture in the intended operational environment for test. Furthermore, the shift to net-centric capabilities will evolve gradually, no doubt with legacy point-to-point interfaces included in the architectures. PMs, with PEO support, are strongly encouraged to work with the operating forces to integrate operational testing with training exercises, thereby bringing more resources to bear for the mutual benefit of both communities. It is imperative the T&E community engages the user community to assure that test strategies reflect the intended operational and sustainment/support architectures and interfaces within which the intended capabilities are to be tested and evaluated.

9.7.2. Modeling and Simulation in T&E

For T&E, the appropriate application of M&S is an essential tool in achieving both an

effective and efficient T&E program. T&E is conducted in a continuum of Live, Virtual, Constructive (LVC) environments. DoD Components have guidelines for use of M&S in acquisition, especially T&E. These guidelines are intended to supplement other resources. The PM should have an M&S subgroup to the T&E WIPT that develops the program's M&S strategy that should be documented in the programs SEP and the TES / TEMP . Some DoD components require planning for M&S to be documented in a separate M&S Support Plan. This M&S strategy will be the basis for program investments in M&S. M&S should be planned for utility across the programs life cycle, modified and updated as required to ensure utility as well as applicability to all increments of an evolutionary acquisition strategy. A program's T&E strategy should leverage the advantages of M&S. M&S planning should address which of many possible uses of M&S the program plans to execute in support of T&E. M&S can be used in planning to identify high-payoff areas in which to apply scarce test resources. Rehearsals using M&S can help identify cost effective test scenarios and reduce risk of failure. During conduct of tests, M&S might provide adequate surrogates to provide stimulation when it is too impractical or too costly to use real world assets. This impracticality is particularly likely for capability testing or testing a system that is part of a system-of-systems, or for hazardous/dangerous tests or in extreme environments, or for testing the systems supportability. M&S can be used in post-test analysis to help provide insight and for interpolation or extrapolation of results to untested conditions.

To address the adequacy and use of M&S in support of the testing process the program should involve the relevant OTA in planning M&S to ensure support for both DT and OT objectives. This involvement should begin early in the programs planning stages.

An initial goal for the T&E WIPT is to assist in developing the programs M&S strategy by helping integrate a programs M&S with the overall T&E strategy; plan to employ M&S tools in early designs; use M&S to demonstrate system integration risks; supplement live testing with M&S stressing the system; and use M&S to assist in planning the scope of live tests and in data analysis.

Another goal for the T&E WIPT is to develop a T&E strategy identifying ways to leverage program M&S which could include how M&S will predict system performance, identify technology and performance risk areas, and support in determining system effectiveness and suitability. For example, M&S should be used to predict sustainability or KSA drivers. The T&E WIPT should encourage collaboration and integration of various stakeholders to enhance suitability (see section 5.2.3).

A philosophy for interaction of T&E and M&S is to use the model-test-fix-model. Use M&S to provide predictions of system performance, operational effectiveness, operational suitability, and survivability or operational security and, based on those predictions, use tests to provide empirical data to confirm system performance and to refine and further validate the M&S. This iterative process can be a cost-effective method for overcoming limitations and constraints upon T&E. M&S may enable a comprehensive evaluation, support adequate test realism, and enable economical,

timely, and focused tests.

Computer-generated test scenarios and forces, as well as synthetic stimulation of the system, can support T&E by creating and enhancing realistic live test environments. Hardware-in-the-loop simulators enable users to interact with early system M&S. M&S can be used to identify and resolve issues of technical risk, which require more focused testing. M&S tools provide mechanisms for planning, rehearsing, optimizing, and executing complex tests. Integrated simulation and testing also provides a means for examining why results of a physical test might deviate from pre-test predictions. Evaluators use M&S to predict performance in areas impractical or impossible to test.

All M&S used in T&E must be accredited by the intended user (PM or OTA). Accreditation can only be achieved through a rigorous VV&A process as well as an acknowledged willingness by the user to accept the subject M&S for their application requirements. Therefore, the intended use of M&S should be identified early so resources can be made available to support development and VV&A of these tools. The OTA should be involved early in this process to gain confidence in the use of M&S and possibly use them in support of OT. DoDI 5000.61 , "DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)," dated December 9, 2009, provides further guidance on VV&A.

The following is provided to help the M&S subgroup to the T&E WIPT think through the planning process to best incorporate M&S into the testing process. Additional guidance for M&S is available in section 4.5.8 .

- Document the intended use of models and simulations:
  - Decisions that will rely on the results of the M&S.
  - The test objectives/critical operational and sustainment issues the models and simulations will address.
  - The requirements for the use of the M&S.
  - Risk of use of M&S.
- Identify all M&S intended to support T&E including (but not limited to):
  - Type: LVC simulations, distributed simulations and associated architecture, federates and federations, emulators, prototypes, simulators, and stimulators;
  - Suitability of model use: Legacy systems, new developments, and modified or enhanced legacy M&S;
  - Management of M&S: Developed in-house, Federally Funded Research and Development Centers (FFRDC), industry, academia, and other Federal or non-Federal government organizations;
  - Source: COTS and GOTS M&S;
  - Facilities: hardware-in-the loop, human-in-the-loop, and software-in-the-loop simulators; land-based, sea-based, air-and space-based test facilities;
  - Threat models, simulations, simulators, stimulators, targets, threat systems, and surrogates;

    - Synthetic countermeasures, Testbeds, environments, and battlespaces;
    - M&S whether embedded in weapon systems, implemented as stand-alone systems, or integrated with other distributed simulations; and
    - Test assets, test planning aids, and post-test analysis tools that address other than real time characteristics.
- Infrastructure needed to conduct the test(s), to include networks, integration software, and data collection tools:
    - Provide descriptive information for each M&S resource:
        - Title, acronym, version, date;
        - Proponent (the organization with primary responsibility for the model or simulation);
        - Assumptions, capabilities, limitations, risks, and impacts of the model or simulation;
        - Availability for use to support T&E; and
        - Schedule for obtaining.
- Identify the M&S data needed to support T&E:
    - Describe the input data the M&S needs to accept;
    - Describe the output data the M&S should generate;
    - Describe the data needed to verify and validate the M&S; and
    - Provide descriptive information for each data resource:
        - Data title, acronym, version, date;
        - Data producer (organization responsible for establishing the authority of the data);
        - Identify when, where, and how data was or will be collected;
        - Known assumptions, capabilities, limitations, risks, and impacts;
        - Availability for use to support T&E; and
        - Schedule for obtaining.
- For each M&S and its data, describe the planned accreditation effort based on the assessment of the risk of using the model and simulation results for decisions being made:
    - Explain the methodology for establishing confidence in the results of M&S;
    - Document historical source(s) of VV&A in accordance with DoDI 5000.61 ; and
    - Provide the schedule for accreditation prior to their use in support T&E.
- Describe the standards (both government and commercial) with which the M&S and associated data must comply; for example:
    - IT standards identified in the DoD IT Standards Registry (DISR);
    - Standards identified in the DoD Architecture Framework Technical Standards Profile (TV-1) and Technical Standards Forecast (TV-2);
    - M&S Standards and Methodologies (requires registration/login);
    - Data standards; and
    - VV&A standards:
        - IEEE Std 1516.4TM -2007, IEEE Recommended Practice for VV&A of a Federation-An Overlay to the High Level Architecture Federation Development and Execution Process;
        - IEEE Std 1278. 4TM -1997(R2002), IEEE Recommended Practice

for Distributed Interactive Simulation - VV&A;
- MIL-STD-3022 , DoD Standard Practice for Model & Simulation VV&A Documentation Templates, dated January 28, 2008.

M&S is an essential tool for achieving both an effective and efficient T&E program. T&E should be conducted in a continuum of LVC environments throughout a systems acquisition process. DoD Components have guidelines for the use of M&S in acquisition, especially T&E. The PM should have an M&S subgroup to the T&E WIPT that develops the program's M&S strategy which should be documented in the programs SEP and the TES / TEMP or in a separate M&S Support Plan.

M&S can be used in test planning to identify high-payoff areas in which to apply scarce test resources, and in dry-running a test to assess the sensitivity of test variables to the response variable being used, and to evaluate system operational effectiveness, operational suitability or survivability or operational security. During the conduct of tests, M&S can provide surrogates to provide stimulation when it is too impractical or too costly to use real world assets. This impracticality is particularly likely for capability testing or testing a system that is part of a system-of-systems, or for hazardous/dangerous tests or in extreme environments, or for testing the systems supportability. M&S can be used in post-test analysis to help provide insight, and for interpolation or extrapolation of results to untested conditions.

9.7.3. Validation of Threat Representations (targets, threat simulators, or M&S)

To ensure test adequacy, OT should only incorporate validated and accredited threat representations unless coordinated with DOT&E.

The following are the recommended validation guidelines:

- Threat representation validation supports the objective of ensuring that threat representations meet DT&E and OT&E credibility requirements. Validation of threat representations is defined as "the baseline comparison of the threat to the threat representation, annotation of technical differences, and impact of those differences on testing."
- Validation of threat representations is typically conducted by the DoD Component responsible for the threat representation and culminates in a validation report which documents the results. DOT&E approves the DoD Component-validated reports.
- Only current, DIA- or DoD Component-approved threat data should be used in the validation report. Specifications pertaining to the threat representation should accurately portray it’s characteristics and may be obtained from a variety of sources including the developer and/or government-sponsored testing. For new developments, validation data requirements should be integrated into the acquisition process to reduce the need for redundant testing.
- Incorporation of an Integrated Product and Process Development (IPPD) process for new threat representation developments is recommended. The objective of

the IPT is to involve DOT&E and its Threat Systems Office (TSO) early and continuously throughout the validation process. DoD Component organizations responsible for conducting threat representation validation should notify DOT&E of their intent to use an IPPD process and request DOT&E/TSO representation at meetings and reviews, as appropriate. The DOT&E representative will be empowered to provide formal concurrence or non-concurrence with these validation efforts as they are accomplished. After the IPPD process, DOT&E will issue an approval memorandum, concurring with the threat representation assessment.

- When a WIPT is not used, draft threat representation validation reports should be forwarded to the TSO for review. The TSO will provide recommendations for corrections, when necessary. Final reports are then submitted by the TSO for DOT&E approval.
- DOT&E approval confirms that an adequate comparison to the threat has been completed. It does not imply acceptance of the threat test asset for use in any specific test. It is the responsibility of the OTA to accredit the test resource for a specific test and for DOT&E to determine if the threat test resource proves adequate.

These guidelines do not address the threat representation verification or accreditation processes. Verification determines compliance with design criteria and requires different methods and objectives. Accreditation, an OTA responsibility, determines the suitability of the threat representation in meeting the stated test objectives. The data accumulated during validation should be the primary source of information to support the accreditation process.

9.7.4. Mission-oriented Context

A mission-oriented context to T&E means being able to relate evaluation results to an impact on the warfighters' ability to execute their mission-essential tasks. Including mission context during test planning and execution provides for a more rigorous test environment, and allows for the identification of design issues that may not be discovered in a pure developmental test environment. The results of testing in a mission-oriented context will allow these issues to be addressed earlier in the development phase of a component or system. Additionally, testing in a mission-oriented context will allow the developmental evaluators to predict system performance against the COIs evaluated in OT&E.

Testing in a mission-oriented context will also allow the OTA to participate earlier in the development cycle and use the results of integrated tests to make operational assessments. Integrated planning of tests is a key element in this process. This allows the data to be used by the developmental community to better predict system performance and allows the OTA to potentially reduce the scope of IOT&E while still providing an adequate evaluation of the COIs .

9.7.5. Testing in a Joint Operational Environment

The phrase testing in a joint environment originated in the U.S. Department of Defense 2006-2011 Strategic Planning Guidance for Joint Testing in Force Transformation. It refers to testing military systems as participating elements in overarching joint SoS. This testing in a joint operational environment initiative supports the departments long-term strategy to test as it fights. Joint operations have become the mainstay of Warfighting. Force transformation will require the T&E community to place a greater emphasis on testing joint war fighting capabilities developed in response to the JCIDS process. Future T&E must ensure combatant commanders can rely on equipment to operate together effectively without introducing problems to warfighters. For a detailed discussion of changes needed to bring about this vision of T&E, see the DepSecDefs Testing in a Joint Environment Roadmap , dated November 12, 2004. The proposals in this roadmap provide important enablers for acquiring new systems created with joint and testing legacy equipment and systems that are made joint.

The Joint Mission Environment (JME) is defined as, "a subset of the joint operational environment composed of force and non-force entities; conditions, circumstances and influences within which forces employ capabilities to execute joint tasks to meet a specific mission objective". It describes the expected operating environment of the system (or system of systems) under test, and includes all of the elements that influence the required performance the new capability must demonstrate. These include the particular mission requirements in which the system is being employed; physical factors such as the blue and opposing force structures; geographic and demographic aspects of the joint operating area, etc., as well as the interactions between these elements.

To be successful, testing in the JME cannot be a new step added at the end of operational T&E, nor can it replace current DT or OT. It does however represent a departure from the way DoD acquisition professionals plan and execute systems engineering, DT&E, and OT&E indeed the entire acquisition process. Testing in a JME involves the appropriate combination of representative systems, forces, threats and environmental conditions to support evaluations. These representations can be LVC, or distributed combinations thereof.

Testing in a JME applies throughout the life cycle of the system. Identification of a joint issue/problem early in a systems life (including as early as the conceptual phase) will reduce costs and issues. This applies to evaluating system performance, or how well

the system does what it is designed to do, as well as the systems contribution to the joint mission, or how DoD employs the system to achieve the mission. A systems interaction with the JME is evaluated along an evaluation continuum using constructive and virtual representations and live systems in various combinations.

The JME and associated joint capability requirements will be defined in the ICD, CDD, and the CPD. The evaluation plans for assessing these requirements will be articulated in the SEP and the TES at Milestone A. At the pre-EMD Review, evaluation plans for assessing these requirements will be articulated in the Pre-EMD draft documents (SEP, TEMP, and ISP). At Milestones B and C, they will be articulated in the SEP, TEMP, and ISP.. For each case, the selection of LVC systems that will be used to recreate the JME to support testing will depend on the purpose of the assessment and on the interactions the SUT will have with other elements in the JME.

This section also briefly addresses some additional areas as outlined in the Testing in a Joint Environment Methods and Processes (M&P) Implementation Plan originally produced by the M&P Working Group that was formed during the summer of 2004 to address testing in a joint environment. The areas of concern outlined below are: (1) Description of Joint Mission Environments, (2) How to use the Joint Mission Environment, (3) Testing in a Joint Mission Environment Program Management Office Support, and (4) Important Acquisition Program Responsibilities.

9.7.5.1. Description of Joint Mission Environments

The JCIDS will create requirements for effects and capabilities at the joint mission level. This means JCIDS will identify desired mission level effects that are shortfalls. Shortfalls are addressed by materiel and non-materiel solutions. Materiel or possible system (for a new/modified system or SoS) KPPs are then proposed to provide the desired mission level effect(s). Because of this, systems development should not begin and testing cannot occur without definition(s) of the JME and a defined joint mission associated with a shortfall to be addressed by a system or systems.

With respect to obtaining information for selected joint missions, users of the joint environment can start with the universal joint planning process to break down missions, but it is a process that starts at the Universal Joint Task List (UJTL) level and extends down to the COCOM level to plan joint task force operations and/or training events. However, this level of "fidelity" may not be available at the JCIDS ICD/CDD/CPD level because it is mission specific at the COCOM or Joint Task Force level.

The joint mission descriptions should set the stage for evaluation of a system(s) within a joint mission area and provide the tester what they need to plan the test. There are essential elements of the joint mission description necessary to plan, execute, and analyze assessments and T&E throughout a systems acquisition process.

Additionally, users of the joint environment determine and obtain representations for the threat, threat composition and disposition, and threat scheme of maneuver appropriate

for the selected joint mission/task. The currently approved Guidance for the Development of the Force (GDF) scenarios and/or the maturing Defense Planning Scenarios will provide the source of this information. There is also a Threat Scenarios Group from the U.S. Army Test & Evaluation Office working threat scenarios. In addition, coordination with the Service intelligence agencies and the DIA is critical. The threat must be system specific (specific to the platform under examination) and also mission specific (specific to the joint mission examined). The next step (after identification of the threat scenarios) is to determine what should be used to represent the threat; which can be a LVC representation.

Different Services should be referred to depending on the type of model needed for test. As the Services have generally focused their modeling efforts based on their usual area of operations. The Army and/or the National Geospatial-Intelligence Agency are the best sources for all terrain models. The Navy is the best source for all oceanographic (surface and subsurface) models, and the Air Force is the best source for air and space models. DoD M&S responsibilities are delineated in DoDD 5000.59 , DoD Modeling and Simulation (M&S) Management, dated August 8, 2007, and there are M&S Executive Agents with responsibilities defined by the DMSO. There should also be a standard set of environment/background models established for the JME.

9.7.5.2. How to use the Joint Mission Environment

Systems engineering and testing will require insertion of concepts and systems into the JME as a standard part of the acquisition process. Since this is a change of scope for previous assessments and tests, a process for how to use the joint mission environment needs established.

The ultimate goal for systems engineering and testing in a joint environment is the ability to insert any system into the applicable JME at any time during the life of a system. Two basic items will be examined through insertion into the JME. The first item is to ensure the systems to be acquired are interoperable with other systems. This includes not only how they interact and communicate as expected and required, but also understanding SoS dependencies. The second item goes beyond the system interaction and communications to examine what value the systems add to joint military capabilities. In other words, the second item is to assess the contribution of the system to the mission success.

Interoperability and contribution should be examined each time a system is inserted into the JME, including times when substantive changes or upgrades are made to an individual system. Users can determine which joint mission/task(s) to test for a system with a role in multiple missions.

Selection of the most stressing mission(s) and/or the mission(s) with the most interactions appears to be the most defensible approach. Test authorities must ensure that if another required mission involves a system interaction not included in the "most stressing" mission, the interaction is tested separately. Examining different joint

missions as the system progresses through the acquisition process is also a good approach especially if there appear to be multiple stressing missions. Another option is to consult with the intended joint users (COCOM & Service Combatant) and have them define representative mission tasks.

With respect to the criteria/process to determine the appropriate representation (live, virtual, or constructive) of players in each engineering (DT or OT) event, the supporting players that constitute the family-of-systems for the joint mission will have to be determined on a case-by-case basis. The goal is for the system being inserted into the JME to be the most mature representation available. However, it will always be a live system for IOT&E.

9.7.5.3. Joint Mission Environment (JME) Program Management Office

Scheduling all of the assets in the JME, especially live assets participating in exercises, will prove a complex undertaking. A management and scheduling capability must exist, and it is assumed the PM will establish a JME PMO (or equivalent) for this purpose. The JME PMO will coordinate all LVC assets, and the script of events, which is the plan for the specific JME missions incorporating acquisition systems under test in accordance with their schedules. Note that acquisition systems tend to have fixed decision points where unplanned delays could severely impact production. Finally, with a complex facsimile of a mission environment in place and acquisition systems scheduled to perform missions within it, additional programs may ask to "join in" the scheduled events, for testing, training exercises, or other special events. This is encouraged, but the testing needs of the sponsoring program must of course take precedence over the needs of other participants, and their participation should not interference with the core purpose of the JME events.

9.7.6. Information Assurance Testing

9.7.7. Interoperability Testing

9.7.8. Software Test and Evaluation (T&E)

9.7.9. Post Implementation Review (PIR)

9.7.10. System-of-Systems (SoS) Test and Evaluation (T&E)

9.7.11. Reliability Growth Testing

9.7.12. Evaluation of Test Adequacy

9.7.13. Medical Materiel T&E

9.7.14. FY 2012 National Defense Authorization Act (NDAA) Section 835

9.8. Best Practices

9.9. Prioritizing Use of Government Test Facilities for T&E

9.7.6. Information Assurance Testing

An integral part of the overall T&E process includes the T&E of IA requirements. DoDI 5000.02 , Operation of the Defense Acquisition System, dated December 8, 2008, directs the conducting of IA T&E during both DT&E and OT&E. To ensure IA testing adequately addresses system IA requirements, the PM must consider IA requirements that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. DoDI 8500.02 , Information Assurance (IA) Implementation, dated February 6, 2003, specifies baseline IA controls for DoD systems. PMs should ensure adequate testing of all applicable IA controls prior to testing in an operational environment or with live data, except for those programs requiring testing in an operational environment. In consultation with the PM or Systems Manager, the Designated Approving Authority (DAA) determines which programs require testing of IA controls in an operational environment. In addition to baseline IA controls, some capabilities documents (e.g., ICD, CDD, and CPD) may also specify unique IA requirements, such as a specific level of system availability. PMs may also identify additional IA requirements as a result of the risk management process, or as directed by the DoD Components. They should also consider the impact of the DoD Information Assurance Certification and Accreditation Process (DIACAP) on the systems overall T&E cost and schedule.

Prior to conducting operational tests programs must receive an Interim Authorization to Operate or Authorization to Operate from the cognizant DAA, followed by a corresponding authorization to connect (ATC) from the system or network manager providing the system connection (e.g. DISA).

Significant C&A activities and events should be visible on the integrated test schedule to ensure appropriate coordination of events. The DoD Component IA program regularly and systematically assess the IA posture of DoD Component-level information systems, and DoD Component-wide IA services and supporting infrastructures through combinations of self-assessments, independent assessments and audit's, formal testing and certification activities, host and network vulnerability or penetration testing, and IA program reviews. The planning, scheduling, conducting, and independent validation of conformance testing should include periodic, unannounced in-depth monitoring and provide for specific penetration testing to ensure compliance with all vulnerability mitigation procedures; such as the DoD information assurance and vulnerability assessment or other DoD IA practices. Testing ensures the systems IA capabilities provide adequate assurance against constantly evolving threats and vulnerabilities.

PMs should consider the re-use and sharing of information to reduce rework and cycle

time. DoD memorandum for establishing DoD Information System Certification and Accreditation Reciprocity , dated June 11, 2009, mandated a mutual agreement among participating enterprises to accept each other's security assessments in an effort to reuse IS resources and/or accept each other's assessed security posture for the timely deployment of IS critical to attaining the Departments strategic vision of Net-Centricity. Additionally, DOT&E memorandum, Procedures for Operational Test and Evaluation (OT&E) of Information Assurance in Acquisition Programs , dated January 21, 2009 contains the OT&E strategy for IA assessment; addressing the test process, identification of required IA test resources and funding, and a reference to the appropriate threat documentation. For more information, see DAG Section 7.5 .

9.7.7. Interoperability Testing

All IT & NSS must undergo joint interoperability testing and evaluation for certification prior to fielding, in accordance with section 2223 of Title 10 USC , DoDI 5000.02 , DoDD 4630.05 , Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), dated April 23, 2007, DoDI 4630.8 , Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), dated June 30, 2004, CJCSI 3170.01H , and CJCSI 6212.01F , Interoperability and Supportability of Information Technology and National Security Systems, dated March 21, 2012. This includes IT & NSS compliance with technical standards, Net-Ready Key Performance Parameters (NR-KPP), solution architectures, and spectrum supportability requirements. Interoperability compliance with joint interoperability test certification requirements remains a continuous process throughout a systems life cycle. JITC bases a Joint interoperability test certification on test and evaluation results from operationally realistic test configurations as well as joint and coalition environments. It then provides input to the MDA and PM for a fielding decision. The PM must plan, program, budget, execute and provide resources according to agreed-to costs, schedules, and test plans. Interoperability requirements impact a programs schedule and costs, so PMs must provide adequate time and funding for Interoperability and Supportability (I&S), NR-KPP, test certification, and Spectrum Supportability Risk Assessments (SSRA). Additional information can be found in Chapter 7.6.4.

Joint interoperability certification testing involves system-of-systems and family-of-systems simulated/live events, and verifies the actual net-centric interoperability characteristics. Additionally, certification testing validates the capability's interoperability, ensuring it proves sufficient in support of a fielding decision. As with most other aspects of a system, PMs should consider net-readiness during early consideration for design and test. The PM should include the strategy for evaluating net-readiness in the TEMP. One important aspect includes developing a strategy for testing each system in the context of the system-of-systems or family-of-systems architecture in which the system operates.

Early assessments and testing opportunities reduce interoperability risk as well as minimize the impact of interoperability requirements on schedule and program costs.

Early identification and resolution of interoperability issues minimizes negative impact to the joint, multi-national, interagency, and Warfighter community. Interoperability testing of all IT & NSS follows the NR-KPP development process. Net-ready attributes determine specific measurable and testable criteria for interoperability, and operationally effective end-to-end information exchanges. The NR-KPP identifies operational, net-centric requirements with threshold and objective values that determine its measure of effectiveness (MOE) and measure of performance (MOP). Architectures provide a foundation to effectively evaluate the probability of interoperability and net-centricity. The NR-KPP covers all communication, computing, and electromagnetic spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the Warfighter mission or joint business processes. Mandatory KPPs for all program increments include the NR-KPP.

JITC acts as the DoD organization responsible for joint interoperability testing and net-readiness certifications. Statute requires JITC to provide a system Net-Ready certification evaluation memorandum to the Director, Joint Staff J-8, throughout the system life cycle and regardless of acquisition category. Based on net-readiness evaluations and other pertinent factors, the Joint Staff J-8 issues a Net-Ready System Certification memorandum to the respective DoD Components as well as developmental and operational test organizations in support of the FRP Decision Review. JITC collaborates with the PM and lead DT&E organization during development of the TEMP, recommending interoperability T&E measures to ensure I&S testing satisfies all requirements during DT&E, OT&E, or IA T&E events. PMs should include JITC as a member of the T&E WIPT and ensure they participate in TEMP development. JITCs philosophy leverages test results from planned test events or exercises to generate the necessary data for joint test and net-ready certifications; combining valuable resources, eliminating redundancy, and ultimately ensuring one test. JITC evaluates the operational effectiveness of information exchanges using joint mission threads in an operational environment. JITC establishes processes to ensure operational tests include operationally mission-oriented interoperability assessments and evaluations using common outcome-based assessment methodologies to test, assess, and report on the impact interoperability and information exchanges have on a systems effectiveness and mission accomplishment for all acquisitions, regardless of ACAT level.

9.7.8. Software Test and Evaluation (T&E)

Software is a rapidly evolving technology that has emerged as a major component in most DoD systems. Within the DoD acquisition domain, the following are essential considerations for success in testing software; to include a security focused code audit/analysis as part of the Software Development Life Cycle (SDLC), IAW the Application Security and Development Security Technical Implementation Guide (STIG) , dated June 3, 2012:

- The T&E strategy should address evaluation of highest risk technologies in system design and areas of complexity in the system software architecture. The strategy should identify and describe:
    - Required schedule, materiel and expertise,
    - Software evaluation metrics for Resource Management, Technical Requirements and Product Quality, including Reliability,
    - Types and methods of software testing to support evaluation in unit, integration and system test phases across the life cycle,
    - Data and configuration management methods and tools,
    - Models and simulations supporting software T&E including accreditation status.
- A defined T&E process consistent with and complementing the software and system development, maintenance and system engineering processes, committed to continuous process improvement and aligned to support project phases and reviews, including an organizational and information flow hierarchy.
- Software test planning and test design initiated in the early stages of functional baseline definition and iteratively refined with T&E execution throughout allocated baseline development, product baseline component construction and integration, system qualification and in-service maintenance.
- Software T&E embedded with and complementary to software code production as essential activities in actual software component construction, not planned and executed as follow-on actions after software unit completion.
- Formal planning when considering reuse of COTS or GOTS, databases, test procedures and associated test data that includes a defined process for component assessment and selection, and T&E of component integration and functionality with newly constructed system elements.
- The following link provides additional information:
    - The Handbook of Software Reliability Engineering , published by IEEE Computer Society Press and McGraw-Hill Book Company (specifically, Chapter 13).

Medical devices and systems must comply with the SEP, in terms of Health Insurance Portability and Accountability Act (HIPAA) and DIACAP information protection procedures and measures. These procedures and measures ensure the software complies with the security standards specified in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104.191) as well as Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title VIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Public Law 111.5). Most medical devices will require IM/IT testing and validation of information security protocols. Given that requirement, programs should start test planning as early as possible. Programs must also validate FDA clearance prior to any medical software implementation.

9.7.9. Post Implementation Review (PIR)

Subtitle III of Title 40 of the United States Code (formerly known as Division E of the Clinger-Cohen Act) requires that Federal Agencies ensure that outcome-based performance measurements are prescribed, measured, and reported for IT (including NSS) programs. DoDI 5000.02 requires that PIRs be conducted for MAIS and MDAP programs in order to collect and report outcome-based performance information. The T&E community will participate in the planning, execution, analysis, and reporting of PIRs, whose results will be used to confirm the performance of the deployed systems and possibly to improve the test planning and execution for follow-on increments or similar systems. For further information, refer to the Acquisition Community Connection or Chapter 7 .

9.7.10. System-of-Systems (SoS) Test and Evaluation (T&E)

SoS testing can result in unexpected interactions and unintended consequences. T&E of SoS must not only assess performance to desired capability objectives, but must also characterize the additional capabilities or limitations due to unexpected interactions. The SoS concept should include the system in the broadest sense, from mission planning to sustainment. SoS is a new and evolving area for development, acquisition, and T&E. For further information refer to the Systems Engineering Guide for Systems of Systems , dated August 2008.

9.7.11. Reliability Growth Testing

Reliability growth testing supports improvements in system and component reliability over time through a systematic process of stressing the system to identify failure modes and design weaknesses. The emphasis in reliability growth testing is in finding failure modes. The reliability of the system is improved, or experiences growth, as the design is modified to eliminate failure modes. The reliability growth testing approach is sometimes referred to as Test-Analyze-Fix-Test (TAFT). A successful reliability growth program depends on a clear understanding of the intended mission(s) for the system, including the stresses associated with each mission and mission durations, and configuration control. Reliability growth testing should be a part of every development program and used to provide input to predicted sustainment needs and the reliability KSA. In addition, the results should be used in developing a realistic product support package. For further information, see the DoD Guide for Achieving Reliability, Availability, and Maintainability , dated August 3, 2005 and associated template . For more information, read DTM 11003, Reliability Analysis, Planning, Tracking, and Reporting , dated December2, 2011.

9.7.12. Evaluation of Test Adequacy

Operational Test and Evaluation adequacy encompasses both test planning and test execution. Considerations include the following:

- Realistic combat-like conditions
- Equipment and personnel under realistic stress and operations tempo
- Threat representative forces
- End-to-end mission testing
- Realistic combat tactics for friendly and enemy
- Operationally realistic environment, targets, countermeasures
- Interfacing systems
- Articles off production line preferred
- Production representative materials and process
- Representative hardware and software
- Representative logistics, maintenance manuals
- Sample size
- Size of test unit
- Threat portrayal
- Properly trained personnel, crews, unit
- Supported by typical support personnel and support package
- Missions given to unit's (friendly and hostile)
- Production representative system for IOT&E
- Adequate resources
- Representative typical users

9.7.13. Medical Materiel T&E

The acquisition and management of medical materiel must ensure quality, availability, and economy in meeting the clinical requirements of the Military Health Systems (MHS). Medical programs, by nature, consist almost exclusively of GOTS, COTS and NDI (non-developmental item) items; and with the inclusion of other government agencies participation (i.e., FDA) follow a similar acquisition strategy to other T&E programs. PMs must not disregard T&E of COTS, NDI, and GFE. The operational effectiveness, operational suitability, and operational capabilities of these items and any military-unique applications must be tested and evaluated before a FRP or fielding decision. The ITT will plan to take maximum advantage of pre-existing T&E data to reduce the scope and cost of government testing.

The PM governs medical materiel procurement as a program with significant oversight, consisting of performance-based requirements composed by an IPT or a high performance team (HPT). Whether Joint or Service-specific, the FDA must clear medical materiel for use, if applicable, and comply with the FDAs rules governing manufacturing. Medical devices must also comply with the SEP in terms of the HIPAA and DIACAP information protection procedures and measures.

PMs, Joint and Service procurement agencies, Service/Defense Agency T&E activities, and other governmental organizations assist with development of operational testing and performance evaluation criteria for medical materiel evaluation; for both developmental and non-developmental programs, as stipulated in DoDI 6430.02 , Defense Medical Materiel Program, dated August 17, 2011. Testing of medical devices,

due to the reliance on COTS items, may not involve the rigorous DT&E imposed on other systems. Unless developed for military use, PMs normally limit DT&E to airworthiness and environmental testing to ensure the device does not fail due to austere or harsh conditions imposed by the operational environments or interfere with the aircrafts operating environment. Programs can integrate this testing, or perform it alongside, operational testing events to determine the operational effectiveness and operational suitability of the device. Often, this usability question can identify the difference between various devices of like construction or capability.

Lead DT&E test organizations can perform medical item testing, as delineated by the individual Service/Defense Agency, and may not require the approval or input of the Service/Defense Agency OTA. Defer to Service/Defense Agency guidelines for these processes.

9.7.14. FY 2012 National Defense Authorization Act (NDAA) Section 835

Based on the FY 2012 NDAA , Section 835, a Chief Developmental Tester will be designated for MDAP and MAIS programs. PMs for MDAP programs shall designate a government test agency as the Lead DT&E organization. All of these designations shall be made as soon as practical after the Materiel Development Decision (MDD). They shall be maintained until the program is removed from OSD T&E oversight or as agreed.

The Chief Developmental Tester position shall be performed by a properly qualified member of the Armed Forces or full-time employee of the DoD. The Chief Developmental Tester shall be in a T&E acquisition-coded position, designated as a Key Leadership Position, assigned or matrixed to the MDAP or MAIS program office, unless otherwise specified within the TEMP. The Chief Developmental Tester for a program shall be responsible for coordinating the planning, management, and oversight of all DT&E activities; maintaining insight into contractor activities; overseeing the T&E activities of other participating Government activities; and helping the PM make technically informed, objective judgments about contractor and Government T&E planning and results.

The Lead DT&E organization shall be separate from the program office. The Lead DT&E organization shall be responsible for providing technical expertise on T&E issues to the Chief Developmental Tester; conducting DT&E activities as directed by the Chief Developmental Tester; assist the Chief Developmental Tester in providing oversight of contractors; and assist the PM and Chief Developmental Tester in reaching technically informed, objective judgments about contractor and Government T&E planning and results.

9.8. Best Practices

Best practices as derived from lessons learned are available and continuously updated

at the DAU Best Practices Clearinghouse .

9.9. Prioritizing Use of Government Test Facilities for T&E

Programs shall use DoD Government T&E capabilities and invest in Government T&E infrastructure unless an exception can be justified as cost-effective to the Government. PMs shall conduct a cost-benefit analysis for exceptions to this policy and document the assumptions and results of the CBA in an approved TEMP before proceeding.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 10 - Decisions, Assessments, and Periodic Reporting

10.0. Overview

10.0.1. Purpose

This Chapter discusses major program decisions, executive-level decision forums, program assessments, and periodic reporting. Generically, it prepares the Program Manager and Milestone Decision Authority to execute their respective oversight responsibilities.

10.0.2. Contents

The chapter starts with overviews of the major decision points and executive-level review forums associated with a program. It also discusses Integrated Product Teams (IPTs) . Other topics include Exit Criteria , Independent Assessments , Information Sharing and Department of Defense (DoD) Oversight , Management Control , Program Plans , and Periodic Reports for Major Acquisition Programs and Major Automated Information Systems programs. The chapter also includes an overview of the Defense Acquisition Management Information Retrieval System and a discussion of Special Interest Programs . The chapter closes with discussions of Should-Cost and Acquisition Program Transition Workshops .

10.1. Decision Points

10.1.1. Types of Decision Points

There are two types of decision points for Major Defense Acquisition Programs and Major Automated Information Systems: milestone decisions and other decision review points. Each such point results in a decision to initiate, continue, advance, change direction in, or terminate a project or program work effort or phase. The type and number of decision points may be tailored to program needs. The Milestone Decision Authority approves the program structure, including the type and number of decision points, as part of the program (technology development or acquisition) strategy .

Major decision points (including milestone decisions) authorize entry into the major

acquisition process phases:

- Material Development Decision -- entry into Materiel Solution Analysis ;
- Milestone (MS) A entry into Technology Development ;
- Pre-EMD Review
- Milestone B entry into Engineering and Manufacturing Development ;
- Milestone C entry into Production & Deployment (Low Rate Initial Production (LRIP) for Major Defense Acquisition Programs and Major Programs, Production or Procurement for non-major programs that do not require LRIP, or Limited Deployment for operational testing for Major Automated Information Systems or software with no production components); and
- Full Rate Production or Full Deployment.

The statutory and regulatory information requirements specified in DoD Instruction 5000.02 support these major decision points.

10.1.1.1. Defense Business System (DBS) Decision Points

The BCL acquisition business model described in DTM-11-009, 12/09/2011 and described in Chapter 12 governs the decision process for DBSs. Although the major milestones have the same names as those in the standard defense acquisition decision framework, the phases are different:

- Material Development Decision -- entry into Investment Management;
- Milestone (MS) A entry into Prototyping;
- Authorization to Proceed
- Pre-Engineering Development
- Milestone B entry into Engineering Development ;
- Milestone C entry into Limited Fielding; and
- Full Deployment.

Additionally, the principles of BCL can be applied at the increment and at the release level. (There may be multiple releases within an increment.) Multiple increments may also be approved concurrently if they have well defined and approved requirements, are fully funded, and have appropriate entrance and exit criteria. For Increment two (2) and beyond, the Milestone Decision Authority must grant Authorization to Proceed (ATP) and document it in an Acquisition Decision Memorandum (ADM). ATP serves as the initiation of the 5-year period for time-certain delivery of capability to ensure compliance with section 2445(c) of title 10, United States Code .

10.1.1.2. Decision Reviews

Decision reviews assess progress and authorize (or halt) further program activity. The review process associated with each decision point typically addresses the program affordability and cost effectiveness; program progress, risk, and trade-offs; strategy, including maintaining competition and the business arrangement (contract type and

incentive structure), program funding, and the development of exit criteria for the next phase or effort.

The regulatory information required to support both milestone decision points and other decision reviews should be tailored to support the review, but must be consistent with the requirements specified in DoD Instruction 5000.02 .

10.1.2. Decision Point Certifications

The Milestone Decision Authority for an MDAP signs a certification memorandum for record prior to Milestone A and Milestone B as specified in sections 2366a and 2366b of title 10, United States Code.

10.1.2.1 Milestone A Certification Requirements

A major defense acquisition program may not receive Milestone A approval until the Milestone Decision Authority certifies, after consultation with the Joint Requirements Oversight Council on matters related to program requirements and military needs, to the following, without modification, from 10 USC 2366a , as amended by Public law 111-23, "Weapon Systems Acquisition Reform Act of 2009" , and the FY 2012 NDAA :

1. that the program fulfills an approved initial capabilities document;
2. that the program is being executed by an entity with a relevant function as identified by the Secretary of Defense;
3. that a determination of applicability of core depot-level maintenance and repair capability has been made;
4. that an analysis of alternatives has been performed consistent with the study guidance developed by the Director of Cost Assessment and Program Evaluation;
5. a cost estimate for the program has been submitted, with the concurrence of the Director, Cost Assessment and Program Evaluation, and the level of resources required to develop, procure, and sustain the program is consistent with the priority level assigned by the Joint Requirements Oversight Council; and
6. *[only include if the system duplicates a capability already provided by an existing system]* the duplication provided by this system and (name of existing system) program is necessary to appropriate.

See Figure 10.1.2.1.F1 for a sample Milestone A certification memorandum.

Figure 10.1.2.1.F1. Sample Required Statement for Milestone Decision Authority Certification Memorandum Prior to Milestone A Approval .

MEMORANDUM FOR THE RECORD

SUBJECT: Milestone A Certification for _____Program

As required by section 2366a of title 10, United States Code, I have consulted with the Joint Requirements Oversight Council (JROC) on matters related to program requirements and military needs for the (*name of program*) and certify that:

(1) the program fulfills an approved initial capabilities document;

(2) the program is being executed by an entity with a relevant function as identified by the Secretary of Defense;

(3) a determination of applicability of core depot-level maintenance and repair capabilities has been made;

(4) an analysis of alternatives has been performed consistent with the study guidance developed by the Director, Cost Assessment and Program Evaluation (DCAPE);

(5) a cost estimate for the program has been submitted, with the concurrence of the DCAPE, and the level of resources required to develop, procure, and sustain the program is consistent with the priority level assigned by the JROC; and

(6) *[only include if the system duplicates a capability already provided by an existing system]* the duplication provided by this system and (*name of existing system*) program is necessary and appropriate.

10.1.2.2 Milestone B Certification Requirements

A major defense acquisition program may not receive a Milestone B approval until the Milestone Decision Authority certifies, without modification, from 10 USC 2366b of title 10, United States Code and as amended by Public law 111-23, "Weapon Systems Acquisition Reform Act of 2009" , and the FY 2012 NDAA , that:

1. I have received a business case analysis and certify on the basis of the analysis that:
    1. the program is affordable when considering the ability of the Department of Defense to accomplish the program's mission using alternative systems;
    2. appropriate tradeoffs among cost, schedule, and performance objectives have been made to ensure that the program is affordable when

considering the per unit cost and total acquisition cost in the context of the total resources available during the period covered by the future-years defense program submitted during the fiscal year in which the certification is made;

3. reasonable cost and schedule estimates have been developed to execute, with the concurrence of the Director, Cost Assessment and Program Evaluation, the product development and production plan under the program;
4. funding is available to execute the product development and production plan under the program, through the period covered by the future-years defense program submitted during the fiscal year in which the certification is made, consistent with the estimates described in subparagraph (C) for the program; and

2. I have received the results of the preliminary design review and conducted a formal post-preliminary design review assessment, and certify on the basis of such assessment that the program demonstrates a high likelihood of accomplishing it's intended mission; and
3. I further certify that:
    1. appropriate market research has been conducted prior to technology development to reduce duplication of existing technology and products:
    2. the Department of Defense has completed an analysis of alternatives with respect to the program;
    3. the Joint Requirements Oversight Council has accomplished it's duties with respect to the program pursuant to section 181(b) of title 10 United States Code , including an analysis of the operational requirements for the program;
    4. the technology in the program has been demonstrated in a relevant environment as determined by the Milestone Decision Authority on the basis of an independent review and assessment by the Assistant Secretary of Defense, Research and Engineering;
    5. life-cycle sustainment planning, including corrosion prevention and mitigation planning, has identified and evaluated relevant sustainment costs, throughout development, production, operation, sustainment, and disposal of the program, and any alternatives, and that such costs are reasonable and have been accurately estimated;
    6. an estimate has been made of the requirements for core depot-level maintenance and repair capabilities, as well as the associated logistics capabilities and the associated sustaining workloads required to support such requirements; and
    7. the program complies with all relevant policies, regulations, and directives of the Department of Defense.

See Figure 10.1.2.2.F1 for a sample Milestone B certification memorandum.

Figure 10.1.2.2 F1. Sample Required Statement for Milestone Decision Authority Certification Memorandum Prior to Milestone B Approval

MEMORANDUM FOR THE RECORD

SUBJECT: Milestone B Certification for _____ Program

As required by section 2366b of title 10, United States Code,

1. I have received a business case analysis and certify on the basis of the analysis that:

(A) the program is affordable when considering the ability of the Department of Defense to accomplish the program's mission using alternative systems;

(B) appropriate tradeoffs among cost, schedule, and performance objectives have been made to ensure that the program is affordable when considering the per unit cost and total acquisition cost in the context of the total resources available during the period covered by the future-years defense program submitted during the fiscal year in which the certification is made;

(C) reasonable cost and schedule estimates have been developed to execute, with the concurrence of the Director, Cost Assessment and Program Evaluation, the product development and production plan under the program;

(D) funding is available to execute the product development and production plan under the program, through the period covered by the future-years defense program submitted during the fiscal year in which the certification is made, consistent with the estimates described in subparagraph (C) for the program; and

2. I have received the results of the preliminary design review and conducted a formal post-preliminary design review assessment, and certify on the basis of such assessment that the program demonstrates a high likelihood of accomplishing it’s intended mission; and
3. development, production, operation, sustainment, and disposal of the program, and any alternatives, and that such costs are reasonable and have been accurately estimated; I further certify that:
    1. appropriate market research has been conducted prior to technology development to reduce duplication of existing technology and products:
    2. the Department of Defense has completed an analysis of alternatives with respect to the program;
    3. the Joint Requirements Oversight Council has accomplished it’s duties with respect to the program pursuant to section 181(b) of title 10 United States Code, including an analysis of the operational requirements for the program;
    4. the technology in the program has been demonstrated in a relevant environment as determined by the Milestone Decision Authority on the basis of an independent review and assessment by the Assistant Secretary of Defense, Research and Engineering;

5. life-cycle sustainment planning, including corrosion prevention and mitigation planning, has identified and evaluated relevant sustainment costs, throughout
6. an estimate has been made of the requirements for core depot-level maintenance and repair capabilities, as well as the associated logistics capabilities and the associated sustaining workloads required to support such requirements; and
7. the program complies with all relevant policies, regulations, and directives of the Department of Defense.

10.2. Executive Review Forums

The following paragraphs address Department of Defense review forums and assessment reviews associated with major decision points in the acquisition lifecycle and other acquisition events requiring senior level review.

10.2.1. Defense Acquisition Board (DAB)

The DAB is the Departments senior-level review forum for critical acquisition decisions concerning Acquisition Category (ACAT) ID programs. The DAB is also the principal review forum enabling the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) to fulfill Chapter 144A of title 10, United States Code responsibilities concerning ACAT IAM Major Automated Information System programs. The use of any other forum for USD(AT&L) review of ACAT ID or IAM programs is

discouraged.

10.2.1.1. Defense Acquisition Board (DAB) Composition

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) is the Milestone Decision Authority (MDA) for Acquisition Category (ACAT) ID programs (and ACAT IAM programs that have not been delegated). The USD(AT&L) chairs the DAB.

DAB members are the following executives: the Vice Chairman of the Joint Chiefs of Staff; the Secretaries of the Military Departments; the Under Secretary of Defense (Policy); the Under Secretary of Defense (Comptroller); the Under Secretary of Defense (Personnel & Readiness); the Under Secretary of Defense (Intelligence); the DoD Chief Information Officer; the Director, Operational Test & Evaluation; the Director, Cost Assessment and Program Evaluation; the Deputy Chief Management Officer (for Defense Business Systems only), and Director, Acquisition Resources & Analysis (as the DAB Executive Secretary).

DAB advisors include the Assistant Secretary of Defense (Acquisition); Assistant Secretary of Defense (Logistics & Material Readiness); Assistant Secretary of Defense (Research and Engineering); Deputy Under Secretary of Defense (Installations and Environment); DoD Deputy General Counsel (Acquisition & Logistics); DoD Component Acquisition Executives; the relevant Overarching Integrated Product Team (OIPT) Leader(s); Director, National Geospatial-Intelligence Agency; Deputy Director, Cost Assessment; Director, Defense Pricing; Director, Systems Engineering, Director, Developmental Test & Evaluation; Deputy Assistant Secretary of Defense (Manufacturing and Industrial Base Policy); Director International Cooperation; Assistant Secretary of Defense (Legislative Affairs); Director, Performance Assessments and Root Cause Analysis; Cognizant Program Executive Officer(s) and Program Manager(s). The USD(AT&L) may request that other department officials participate in reviews, as required.

10.2.1.2. Conduct of Defense Acquisition Board (DAB) Reviews

DAB Reviews are conducted for ACAT ID and IAM programs at major decision points, including; the Materiel Development Decision, the Technology Development decision, the pre-Engineering and Manufacturing Development (EMD) review, the EMD decision, the Production decision, the Full-Rate Production decision Review/Full Deployment decision Review, at Interim Program Reviews, and at other times as necessary. Whenever possible, these reviews should take place in the context of the existing Integrated Product Team and acquisition milestone decision review processes. An Acquisition Decision Memorandum (ADM) signed by the USD(AT&L) or other delegated decision authority documents the decision(s) and program direction resulting from the review. Any memorandum the USD(AT&L) signs concerning ACAT ID or IAM programs is referred to as an ADM and must be staffed by the DAB Executive Secretary (Director,

Acquisition Resources and Analysis).

The USD(AT&L) is the Defense Acquisition Executive (DAE) and generally chairs the DAB unless he has otherwise delegated the chair for a particular program or event. However, ACAT ID and IAM decision and program reviews should be referred to as "DAB Reviews" or "DAB Meetings" and not "DAE Reviews."

10.2.1.3. Defense Acquisition Board (DAB) Presentation

The DAB review is intended to be a measured, intellectual examination of unresolved issues. Issues that have previously been resolved need not be discussed. Issue deliberation should focus on the risks and opportunities associated with the potential courses of action and evidentiary arguments should be supported by critical, objective, factual data.

The OIPT Leader is expected to shape the DAB briefing to ensure that it captures and objectively represents the unresolved issues still requiring discussion, the data to support such discussion, and all other critical information necessary to conduct a successful DAB review-above all, information pertaining to the affordability and cost effectiveness of the program. At the beginning of each DAB, the OIPT leader will state the decision sought (or other purpose for the review) and immediately tee up the unresolved issues. The OIPT leader will ensure that evidentiary arguments (pro and con) are presented and supporting data will be presented by the appropriate principal DAB member or advisor. Following the discussion of the issues and the affordability and cost effectiveness of the program, the remaining mandatory information charts will be presented and reviewed.

A notional set of DAB Milestone Decision briefing charts is available for use. It is expected that, except for the limited number labeled mandatory, these charts will be used as a guide only and will be appropriately tailored for the specific program and decision under consideration. A set of information checklists is also available to aid in functional reviews of required information during the DAB preparation process.

10.2.1.4. Acquisition Decision Memorandum (ADM) Coordination and ADM Action Item Tracking

The decisions and direction resulting from of each milestone and other major decision point reviews must be documented in an ADM. All ACAT ID and ACAT IAM ADMs are written by the office of the Director, Acquisition Resources and Analysis (ARA) and the pertinent Overarching Product Team (OIPT) Leader. ARA staffs all ADMs for coordination. Prior to release for formal staffing, ARA submits each ADM to the Principal Deputy Under Secretary for Defense (Acquisition, Technology, and Logistics) (PDUSD(AT&L)) or the Under Secretary for Defense (Acquisition, Technology, and Logistics) for initial review.

All ADM-directed actions are tracked and monitored by the OIPT leaders and reported

for closure, compilation, and summation in the recently established Defense Acquisition Executive (DAE) Action Tracker (DAT) automated system (https://ebiz.acq.osd.mil/DAT). ARA maintains the DAT system and will periodically review the status of overdue ADM actions with the PDUSD(AT&L), the Component Acquisition Executives, the Assistant Secretary of Defense (Acquisition), and the OIPT Leaders.

10.2.1.5. Preparation for Defense Acquisition Board (DAB) Reviews

Programs must be adequately reviewed far enough ahead of a DAB meeting so that all issues associated with the desired decision can be identified and, optimally, resolved prior to the DAB review. Any issues that cannot be resolved prior to the DAB review should be well defined and presented with the relevant data needed to decide on a course of action among the available alternatives. Resolving any remaining issues should be the focus of the DAB meeting itself.

Early in the DAB preparation process, the Assistant Secretary of Defense (Acquisition) (ASD(A)) will conduct a DAB Planning Meeting (DPM) with the Overarching Integrated Product Team (OIPT) Leader and a service or agency representative to discuss the pending decision and any open issues that may be anticipated to exist at the time of the DAB.

In order to ensure DAB reviews focus on issues and the data that affects issue resolution, the Principal Deputy Under Secretary of Defense (Acquisition, Technology, and Logistics) (PDUSD(AT&L)) or the Under Secretary of Defense (Acquisition Technology, and Logistics) (USD(AT&L)) will hold a DAB Readiness Meeting (DRM) as soon as possible after the final pre-DAB OIPT meeting-approximately one work week before each scheduled DAB. The DRM will focus on the purpose of the DAB, discuss and consider any outstanding issues on the specific program(s), and determine the readiness of the program(s) to proceed to a DAB for a discussion/decision.

Based upon the results of the DRM, the PDUSD(AT&L) or the USD(AT&L) will determine the whether to proceed as scheduled; to postpone the DAB while additional information is obtained, or whether the decision may be made and documented in an Acquisition Decision Memorandum without convening a formal DAB meeting (a.k.a. a paper DAB). If there are no issues associated with the requested decision, then a formal meeting should not be necessary.

10.2.1.5.1. Preparation Timeline for Defense Acquisition Board (DAB) Reviews

The nominal timeline (in business days) to support the DPM, DRM and DAB is listed below:

0 DAB

-3 DAB Read-ahead submitted

-5 DRM

-10 OIPT Report submitted

-20 OIPT conducted

-30 Final Document Check to Support OIPT

-40 DAB Planning Meeting

-45 Submittal of Final Documents Due to OSD

The OIPT Chair will conduct meetings and form working groups as needed to support the DAB preparation process.

10.2.1.5.2. Defense Acquisition Board (DAB) Planning Meeting (DPM)

The DPM is a short informal meeting conducted by the Assistant Deputy Secretary of Defense (Acquisition) (ASD(A)) approximately two months before the scheduled DAB review. The DPM serves as a heads up for that upcoming review and provides an opportunity to ensure that the Overarching Integrated Product Team (OIPT) Lead and the Component Acquisition Executive (CAE) staff are prepared to adequately cover any concerns that the Under Secretary of Defense, Acquisition Technology, and Logistics may have at the DAB review.

The purpose is to give the CAE and the OIPT Lead time to examine such potential issues and any actions needed to deal with major concerns that have already been raised. Content for the DPM will be at the discretion of the OIPT Chair and service (or agency) presenting the program for DAB review.

The OIPT chair, in coordination with the relevant service or agency will schedule this meeting, which will nominally be at least two to three months before the DAB is scheduled.

Attendance at the DPM is limited to the OIPT lead plus one staff member, two or three people representing the pertinent CAE(s), and the DAB Executive Secretary plus one staff member--unless otherwise directed, or approved, by the ASD(A).

10.2.1.5.3. Defense Acquisition Board (DAB) Readiness Meeting (DRM)

The DRM is a small, informal meeting conducted by the Principal Deputy Under Secretary of Defense, Acquisition Technology, and Logistics (PDUSD(AT&L)) or the Under Secretary of Defense, Acquisition Technology, and Logistics (USD(AT&L)) approximately two weeks before the DAB review and after the Overarching Integrated

Product Team (OIPT) meeting. The purpose of the DRM is for the PDUSD(AT&L) or the USD(AT&L) to review the OIPT results to understand any remaining open issues that the DAB would have to consider and-to review the proposed DAB presentation, including materials/data necessary to resolve any issues that would be presented to the DAB to support the decision.

Content for the DRM will be specific to the decision sought for the particular program and will be issue-focused. The actual briefing material and backup material for the DAB itself should be ready for review-with the presentation in final form. The proposed DAB brief and the OIPT Leaders report should be included in the DRM read ahead.

Attendance at the DRM is limited to the OIPT lead plus one staff member, two or three people representing the pertinent CAE(s), and the DAB Executive Secretary plus one staff member--unless otherwise directed, or approved, by the Assistant Secretary of Defense (Acquisition). (On an as required basis, other OSD representatives may also be requested to attend to discuss unresolved issues planned to be addressed at the DAB review.)

The DRM is not intended to be a decision meeting; however, in some cases, it may lead to a recommendation or decision to conduct a "paper DAB" review.

10.2.2. Joint Requirements Oversight Council (JROC)

10.2.3. Functional Capabilities Boards (FCBs)

10.2.4. Defense Business System Management Committee (DBSMC)

10.2.5. Investment Review Boards (IRBs)

10.2.6. DoD Component Program Decision Review Processes

10.2.7. Configuration Steering Boards (CSBs)

10.2.2. Joint Requirements Oversight Council (JROC)

The Joint Requirements Oversight Council (JROC) reviews and approves capabilities documents designated as JROC interest and supports the acquisition review process. The JROC is composed of the Vice Chairman of the Joint Chiefs of Staff, who is the Chairman of the Council; the Service Vices/Assistant Commandant; and Combatant Commanders (or Deputies) when matters related to the area of responsibility or functions of that command will be under consideration by the Council.

In accordance with the CJCS Instruction 3170.01 , the Joint Staff reviews all Joint Capabilities Integration and Development System (JCIDS) documents and assigns a Joint Potential Designator. The JROC validates capability needs. The JROC also validates the key performance parameters when it approves the associated capabilities

document. The JROC charters Functional Capabilities Boards (FCBs). The boards are chaired by a JROC-designated chair and, for appropriate topics, co-chaired by a representative of the Milestone Decision Authority.

10.2.3. Functional Capabilities Boards (FCBs)

Functional Capabilities Boards are the lead coordinating bodies to ensure that the joint force is best served throughout the JCIDS and acquisition processes. The JCIDS process encourages early and continuous collaboration with the warfighter and acquisition communities to ensure that new capabilities are conceived and developed in the joint warfighting context. The JROC, at its discretion, may review any JCIDS issues which may have joint interest or impact. The JROC will also review programs at the request of, and make recommendations as appropriate to, the Secretary of Defense, Deputy Secretary of Defense, and the Under Secretary of Defense (Acquisition, Technology, and Logistics).

10.2.4. Defense Business System Management Committee (DBSMC)

The DBSMC was established by the Secretary of Defense under authority delegated pursuant to section 186 of title 10, United States Code and in accordance with DoDI 5105.18 ,

The DBSMC advises the DBSMC Chair who is responsible for approving Certification Authority (CA) certification of funds associated with Defense Business System modernization efforts.

10.2.5. Investment Review Boards (IRBs)

IRBs are boards established by an Under Secretary or Assistant Secretary of Defense under authority delegated pursuant to section 2222(f) of title 10 United States Code to conduct the Defense Business System (DBS) review process required by section 2222(g) of the same title.

The IRBs are responsible for advising the Milestone Decision Authority. Required acquisition decision documentation is submitted to the IRB membership no later than 30 calendar days prior to the IRB. IRBs review :

- Problem Statements, which shall be approved by the IRB Chair;
- Requirements changes and technical configuration changes for programs in development that have the potential to impact cost and schedule; and
- The Business Case to determine that business process reengineering (BPR) efforts have been undertaken.

The DoD Components are required to establish or employ decision bodies with similar responsibilities for DBS that do not meet the Major Automated Information System

threshold.

10.2.6. DoD Component Program Decision Review Processes

The OSD-level decision review processes discussed in this section of the Guidebook deal specifically with ACAT ID and ACAT IAM programs, selected Pre-Major Defense Acquisition Programs/Pre-Major Automated Information System Programs, and Under Secretary of Defense (Acquisition, Technology, and Logistics) Special Interest Programs. DoD Component Acquisition Executives will develop tailored procedures that meet statutory intent for programs under their cognizance.

10.2.7. Configuration Steering Boards (CSBs)

Section 814 of P.L. 110-417 requires each Department of Defense Component Acquisition Executive (CAE) to establish and chair a CSB with broad executive membership including senior representatives from the Offices of the Under Secretary of Defense (Acquisition, Technology, and Logistics), the Joint Staff, the Chief of Staff and Comptroller of the Armed Force concerned, other Armed Forces where appropriate, the military deputy to the CAE, the Program Executive Officer (PEO), and other senior representatives of the Office of the Secretary of Defense and the military department concerned, as appropriate.

1. Each CSB must meet at least annually to review all requirements changes and any significant technical configuration changes for ACAT I and IA programs in development that have the potential to result in cost and schedule impacts to the program. Such changes will generally be rejected, deferring them to future blocks or increments. Changes shall not be approved unless funds are identified and schedule impacts mitigated.
2. Each Program Manager, in consultation with the cognizant PEO, must, on a roughly annual basis, identify and propose a set of descoping options, with supporting rationale addressing operational implications, to the CSB that reduce program cost or moderate requirements. If the program is an ACAT ID or IAM program, the CSB chair must recommend to the Milestone Decision Authority which of these options should be implemented. Final decisions on descoping option implementation shall be coordinated with the Joint Staff and military department requirements approval officials.

10.3. Integrated Product and Process Development (IPPD)

10.3.1. Role of Integrated Product Teams (IPTs)

10.3.2. Overarching Integrating Product Team (OIPT) Procedures and Assessment

10.3.2.1. Overarching Integrating Product Team (OIPT)

10.3. Integrated Product and Process Development (IPPD)

IPPD is the Department of Defense (DoD) management technique that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize design, manufacturing, and supportability processes. One of the key IPPD tenets is multidisciplinary teamwork through Integrated Product Teams .

IPPD facilitates meeting cost and performance objectives from product concept through production, including field support. The 10 tenets of IPPD can be summarized into the following 5 principles:

- Customer Focus
- Concurrent Development of Products and Processes
- Early and Continuous Life-Cycle Planning
- Proactive Identification and Management of Risk
- Maximum Flexibility for Optimization and Use of Contractor Approaches

10.3.1. Role of Integrated Product Teams (IPTs)

Defense acquisition works best when all of the DoD Components work together. Cooperation and empowerment are essential. Per Department of Defense Directive 5000.01 , the Department's acquisition community shall implement the concepts of Integrated Product and Process Development (IPPD) and IPTs as extensively as possible.

IPTs are an integral part of the Defense acquisition oversight and review process. For Acquisition Category (ACAT) ID and IAM programs, there are generally two levels of IPTs: the Working-Level Integrated Product Team (WIPT) and the Overarching Integrated Product Team (OIPT) . Each program should have an OIPT and at least one WIPT. WIPTs should focus on a particular topic such as cost/performance, program baseline, acquisition strategy, test and evaluation, or contracting. An Integrating

Integrated Product Team (IIPT), which is itself a WIPT, should coordinate WIPT efforts and cover all program topics, including those not otherwise assigned to another IPT. IPT participation is the primary way for any organization to participate in the acquisition program. IIPTs are essential for ACAT ID and IAM programs, in that they facilitate OSD Staff-level program insight into MDAPs and MAIS programs at the program level and provide the requisite input to the OIPT.

10.3.2. Overarching Integrating Product Team (OIPT) Procedures and Assessment

Normally, all Acquisition Category (ACAT) ID and IAM programs will have an OIPT to provide assistance, oversight, and review as the program proceeds through its acquisition life cycle.

10.3.2.1. Overarching Integrating Product Team (OIPT)

First and foremost, Office of the Secretary of Defense (OSD) OIPTs are teams expected to collectively assist the Defense Acquisition Executive (DAE) in making sound investment decisions for the Department and to ensure programs are structured and resourced to succeed. Success is defined as affordable, executable programs that provide the most value achievable for the resources invested by the Department.

OSD OIPTs are not decision bodies and their respective leaders do not supplant the authority and responsibilities of the Program Manager, Program Executive Officer, Component Acquisition Executive, or DAE. The acquisition chain of command is expected to thoroughly prepare programs for decisions and to execute those decisions. OSD OIPTs bring independent judgment and perspectives from various staff offices and provide a measure of due diligence in support of DAE decisions. They often bring different perspectives than the Components and should be concerned not only with the programmatic, technical, and business aspects of a program but also with critically examining and considering the program in the broader context to include joint portfolios, design and performance trade-space, overall risk (technology, integration/engineering, schedule, and cost), affordability, competitive opportunities, industrial base implications, and the nature of the business decision under consideration.

OSD OIPTs also have a key role in helping programs complete the requirements of the statutory and regulatory acquisition framework, much of which involves documentation the team members review in support of the decision process. Typically, these documents have been reviewed within a Service and at working levels of the OSD staff and Service staffs to ensure they reflect sound planning and assessments before they are submitted for final review. These documents should generally not be prepared solely for staff review and approval, but be intended primarily for use within the program as planning and management tools that are highly specific to the program and tailored to meet program needs. They should be prepared and reviewed with this goal in mind.

OSD OIPT meetings should be the culmination of the staffing process and lead to well-staffed and objectively presented decision options on any open issues for discussion at

the Defense Acquisition Board review and subsequent acquisition decisions. To work effectively, all OIPT members should attempt to resolve issues at the lowest possible level.

To perform their work, OSD OIPTs and their members should have access to all the data necessary to do their jobs effectively. Program offices and Component staffs are expected to provide data needed to resolve issues and to support DAE decisions in a timely manner.

10.3.2.2. Overarching Integrating Product Team (OIPT) Leaders

For those programs where the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Milestone Decision Authority, OIPTs are a well-established and integral part of the defense acquisition oversight and milestone decision review process. While OIPTs are not decision-making bodies, they provide a mechanism to coordinate and conduct staff preparation for USD(AT&L) program decisions and to help execute those decisions.

There are currently five OIPT leaders in the Office of the Secretary of Defense that are responsible for broadly defined portfolios of programs and capabilities. Programs with the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) as the Milestone Decision Authority are normally assigned to one of these OIPT leaders as the lead staff element with the broad responsibility for the program:

- Deputy Assistant Secretary of Defense (DASD) (Strategic and Tactical Systems)
- DASD (Space & Intelligence)
- DASD (Command, Control, Communications & Cyber)
- OIPT Leader for Defense Business Systems (Office of the Deputy Chief Management Officer)
- OIPT Leader for Nuclear, Chemical, & Biological Defense programs

10.3.2.2.1. Overarching Integrating Product Team (OIPT) Leaders Roles & Responsibilities

OSD OIPT leaders form and lead OIPTs to review the programs coming forward to the Defense Acquisition Board (DAB) for a Defense Acquisition Executive (DAE) decision. OIPT leaders also prepare content for discussions at DAB Planning Meetings and DAB Readiness Meetings in collaboration with the responsible Component, the DAB Executive Secretary, and any OIPT members with outstanding issues. OIPT Leaders are responsible for coordinating staff inputs, facilitating the resolution of issues at lower levels when possible, and for ensuring that objective and complete data is presented to the DAE in support of DAE decisions, including milestone decisions.

OSD OIPT leaders are expected, with the assistance of the OIPT members, to maintain good situational awareness of program execution status and, with the Component Acquisition Executives (CAEs) to keep the DAE informed of any program issues. The

Defense Acquisition Executive Summary (DAES) process serves as one mechanism to monitor programs and elevate issues. DAES meetings are forums for sharing and learning across the senior levels of the acquisition community. However, OIPT leaders and OIPT members should not delay surfacing problems awaiting a DAES cycle. Bad news does not get better with age and the earlier issues are addressed, the greater the opportunity to remediate them. Similarly, good outcomes and best practices should also be reported and widely shared. Monitoring program execution should not generate unnecessary meetings, but rather, the evolving tools, data, and monitoring mechanisms that the Components and the Office of the Secretary of Defense have in place should accomplish this function. In general, and consistent with their responsibilities, OIPT leaders (and all staff members) should work to minimize the overhead burden placed on Program Managers. The OIPT leaders are also expected to track and monitor to successful completion all Acquisition Decision Memorandum-directed actions and notify the DAE of issues or events that would affect their completion.

In cases where there is substantive disagreement between staff members and a Component, the OIPT leader is expected to work with the relevant staff and Component to ensure the data necessary to support a decision is made available to the DAE and to quickly elevate the issues to be brought forward for decisions. In general the staff, including the OIPT leader, does not have directive authority over programs and issues should be elevated for decision when there is a disagreement that cannot be readily resolved. The OIPT leader should expedite this process so that programs are not delayed due to disagreements over issues. The OIPT leader may make a recommendation on any issue, but his or her fundamental responsibility is to objectively represent the views of the OIPT members from across OSD and the Services.

10.3.2.3. Overarching Integrating Product Team (OIPT) Member Roles & Responsibilities

Office of the Secretary of Defense (OSD) OIPT members should be empowered to represent their organizations perspectives and make commitments on behalf of their technical domain, functional area, and organization.

OIPT members should proactively assist programs in implementing Better Buying Power Initiatives. In many cases, OIPT members will have knowledge of techniques or approaches that could promote competition, reduce costs, improve productivity, or reduce non-productive processes.

Members should raise issues at the earliest possible opportunity and work to resolve those issues expeditiously. It is a disservice to the programs and process for issues to remain hidden or for issues to arise unexpectedly at senior-level decision meetings such as the DAB. If an OIPT member feels an issue is not resolved satisfactorily, the DAE should be informed. OIPT members with differing views will be part of any discussion and afforded the opportunity to express their views with supporting information directly if desired. Any issue raised should be logically presented with appropriately detailed

technical or other relevant data to allow for an informed decision.

Table 10.3.2.3.T1 below is a list of nominal organizational members for a typical OSD OIPT. Membership can be adjusted as appropriate by OIPT leaders.

Table 10.3.2.3.T1. Notional OIPT Membership

Vice Chairman of the Joint Chiefs of Staff/J-8	Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
Office of the Under Secretary of Defense for Policy	Office of the Director for Chemical and Material Risk Management
Office of the Under Secretary of Defense (Comptroller)	Office of the Deputy Assistant Secretary of Defense (Manufacturing and Industrial Base Policy)
Office of the Under Secretary of Defense for Personnel and Readiness	Office of the Assistant Secretary of Defense for Logistics and Materiel Readiness
Office of the Under Secretary of Defense for Intelligence	Office of the Assistant Secretary of Defense for Operational Energy Plans and Programs
Office of the Director, Operational Test and Evaluation	Office of the Deputy Assistant Secretary of Defense Research
Office of the Director, Cost Analysis and Program Evaluation	Office of the Deputy Assistant Secretary of Defense Systems Engineering
Office of the Director, Acquisition Resources and Analysis	Cognizant Program Executive Officer(s)
Office of the Director, Defense Pricing	Cognizant Program Manager
Office of the Director, Defense Procurement and Acquisition Policy	Office of the Army Acquisition Executive
Office of the Director, Performance Assessment and Root Cause Analyses	Office of the Navy Acquisition Executive
Office of the Director, International Cooperation	Office of the Air Force Acquisition Executive
Office of the Chief Information Officer	

10.3.2.4. Overarching Integrating Product Team (OIPT) Products

The cognizant OIPT leader will provide a written report to the Defense Acquisition Executive not more than 10 business days after the OIPT meeting and not less than 15 business days prior to a scheduled Defense Acquisition Board (DAB) date (i.e., well before the DAB Readiness Meeting). The OIPT Report will document an integrated program assessment that takes OIPT members independent assessments into consideration. It will also provide a recommendation for the decision(s) to be made and

include a discussion of all unresolved issues. OIPT leaders will ensure all OIPT member perspectives and concerns (including dissenting views) are accurately represented. OIPT members, at their discretion, may provide attachments to the OIPT report reflecting their individual perspectives and recommendations and providing the basis for those views.

The OIPT leader will assist the Program Manager and Program Executive Officer in preparing program decision materials for the DAB. DAB briefings and supporting material should contain all the data necessary to support the pending decisions presented in a logical straightforward manner using the DAB templates as a starting point.

10.3.3. Integrating Integrated Product Team (IIPT) and Working-Level Integrated Product Team (WIPT) Procedures, Roles, and Responsibilities

The Program Manager (PM), or designee, in collaboration with the OSD staff specialists from the offices of the OIPT Leader and other key stakeholders for the assigned program, should collaboratively form IIPTs and WIPTs as necessary. IIPTs and WIPTs should meet only as required to help the program manager plan program structure and documentation and resolve issues. While there is no one-size-fits-all WIPT approach, the following basic tenets should apply:

- The PM is in charge of the program.
- IIPTs and WIPTs are advisory bodies to the PM.
- IIPTs are also advisory bodies to the OIPT.
- Direct communication between the program office and all levels in the acquisition oversight and review process is expected as a means of exchanging information and building trust.

10.3.3.1. Industry Participation

Industry representatives may be invited to a Working-Level Integrated Product Team (WIPT) or Integrating Integrated Product Team (IIPT) meeting to provide information, advice, and recommendations to the IPT; however, the following policy should govern their participation:

- Industry representatives will not be formal members of the IPT.
- Industry participation will be consistent with the Federal Advisory Committee Act .
- Industry representatives may not be present during IPT deliberations on acquisition strategy or competition sensitive matters, nor during any other discussions that would give them a marketing or competitive advantage.
- At the beginning of each meeting, the IPT chair should introduce each industry representative, including their affiliation, and their purpose for attending.
- The chair should inform the IPT members of the need to restrict discussions while industry representatives are in the room, and/or the chair should request the industry representatives to leave before matters are discussed that are

inappropriate for them to hear.

- Support contractors may participate in WIPTs and IIPTs, but unless specifically authorized by the organization they represent, they may not commit the staff organization they support to a specific position. The organizations they support are responsible for ensuring the support contractors are employed in ways that do not create the potential for a conflict of interest. Contractors supporting staff organizations may participate in Overarching Integrated Product Team (OIPT) discussions; however, they will not be permitted to represent the position of the supported organization and they may be asked to sign non-disclosure statements prior to deliberations.

Given the sensitive nature of OIPT discussions, industry representatives and support contractors may not be permitted to participate in certain OIPT discussions. However, the OIPT leader may permit contractors to make presentations to the OIPT, when such views will better inform the OIPT and will not involve the contractors directly in Government decision making.

10.4. Role of Exit Criteria

Each Milestone Decision Authority (MDA) should use exit criteria for ACAT I and ACAT IA programs during an acquisition phase. Prior to each milestone decision point and at other decision reviews, the Program Manager will develop and propose exit criteria appropriate to the next phase or effort of the program. The Overarching Integrated Product Team will review the proposed exit criteria and make a recommendation to the

MDA. Exit criteria approved by the MDA will be published in the Acquisition Decision Memorandum.

System-specific exit criteria normally track progress in important technical, schedule, or management risk areas. Unless waived, or modified by the MDA, exit criteria must be satisfied before the program may continue with additional activities within an acquisition phase or proceed into the next acquisition phase (depending on the decision with which they are associated). Exit criteria should not be part of the Acquisition Program Baseline (APB) and are not intended to repeat or replace APB requirements or the phase-specific entrance criteria specified in DoD Instruction 5000.02 . They should not cause program deviations.

10.5. Role of Independent Assessments

Assessments, independent of the developer and the user, provide a different perspective of program status. However, requirements for independent assessments (for example, Program Support Reviews , Assessments of Operational Test Readiness , independent cost estimates, and technology readiness assessments) must be consistent with statutory requirements, policy, and good management practice. Senior acquisition officials consider these assessments when making acquisition decisions. Staff offices that provide independent assessments should support the orderly and timely progression of programs through the acquisition process. Overarching Integrated Product Team access to independent assessments that provide additional program perspectives facilitates full and open discussion of issues.

10.5.1. Independent Cost Estimate

Section 2334 of title 10, United States Code , requires the Director, Cost Assessment and Program Evaluation (DCAPE) to conduct independent cost estimates (ICEs) on Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) programs for which the Under Secretary of Defense (Acquisition, Technology, and Logistics) is the Milestone Decision Authority. The statute also requires DCAPE to review Department of Defense (DoD) Component cost estimates and cost analyses conducted in connection with MDAPs and MAIS programs.

Further, the statute gives DCAPE the authority to prescribe the policies and procedures for the conduct of all cost estimates for DoD acquisition programs and issue guidance relating to the full consideration of life-cycle management and sustainability costs.

10.5.1.1. Independent Cost Estimate (ICE) for Major Defense Acquisition Programs (MDAPs)

The Director, Cost Assessment and Program Evaluation (DCAPE) conducts ICEs and cost analyses for MDAPs for which the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Milestone Decision Authority in advance

of:

(1) Any decision to enter low rate initial production, or full rate production.

(2) Any certification pursuant to sections 2366a , 2366b , or 2433a of title 10, United States Code.

(3) At any other time considered appropriate by the DCAPE or upon the request of the USD(AT&L).

10.5.1.2. Independent Cost Estimate (ICE) for Major Automated Information Systems (MAIS) Programs

The Director, Cost Assessment and Program Evaluation (DCAPE), conducts ICEs and cost analyses for MAIS programs for which the Under Secretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L)) is the Milestone Decision Authority in advance of:

(1) Any report pursuant to section 2445c(f) of title 10, United States Code.

(2) At any other time considered appropriate by the DCAPE or upon the request of the USD(AT&L).

10.5.1.3. Review of Cost Estimates

The Director, Cost Assessment and Program Evaluation (DCAPE) participates in the discussion of any discrepancies related to cost estimates for Major Defense Acquisition Programs (MDAPs) and Major Automation Information System (MAIS) programs, comments on deficiencies regarding the methodology or the execution of the estimates, concurs with the choice of the cost estimate used to support the Acquisition Program Baseline or any of the cost estimates identified in paragraphs 10.5.1.1. and 10.5.1.2. and participates in the consideration of any decision to request authorization of a multi-year procurement contract for a MDAP.

10.5.1.4. Cost Estimate Confidence Levels

The Director, Cost Assessment and Program Evaluation (DCAPE) and the Secretary of the Military Department concerned or the head of the Defense Agency concerned (as applicable) state the confidence level used in establishing the cost estimate for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs, ensure that the confidence level provides a high degree of confidence that the program can be completed without the need for significant adjustment to program budgets, and provides the rationale for selecting the confidence level. The confidence level statement shall be included in the Acquisition Decision Memorandum approving the Acquisition Program Baseline, and in any documentation of cost estimates for MDAPs or MAIS programs prepared in association with the events

identified in paragraphs 10.5.1.1. and 10.5.1.2. The confidence level statement shall also be included in the next Selected Acquisition Report prepared in compliance with section 2432 of title 10, United States Code , or in the next quarterly report prepared in compliance with section 2445c of title 10, United States Code .

10.5.2. Technology Maturity and Technology Readiness Assessments

A Technology Readiness Assessment (TRA) is a systematic, metrics-based process that assesses the maturity of, and the risk associated with, critical technologies to be used in Major Defense Acquisition Programs (MDAPs). It is conducted by the Program Manager (PM) with the assistance of an independent team of subject matter experts (SMEs). It is provided to the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) and will provide part of the basis upon which he advises the Milestone Decision Authority (MDA) at Milestone (MS) B or at other events designated by the MDA to assist in the determination of whether the technologies of the program have acceptable levels of risk-based in part on the degree to which they have been demonstrated (including demonstration in a relevant environment)-and to support risk-mitigation plans prepared by the PM.

A TRA is required by Department of Defense Instruction (DoDI) 5000.02 for MDAPs at MS B (or at a subsequent Milestone if there is no MS B). It is also conducted whenever otherwise required by the MDA. The TRA final report for MDAPs must be submitted to ASD(R&E) for review to support the requirement that ASD(R&E) provide an independent assessment to the MDA.

A TRA focuses on the programs critical technologies (i.e., those that may pose major technological risk during development, particularly during the Engineering and Manufacturing Development (EMD) phase of acquisition). Technology Readiness Levels (TRLs) can serve as a helpful knowledge-based standard and shorthand for evaluating technology maturity, but they must be supplemented with expert professional judgment.

The program manager should identify critical technologies, using tools such as the Work Breakdown Structure. In order to provide useful technology maturity information to the acquisition review process, technology readiness assessments of critical technologies and identification of critical program information (CPI) must be completed prior to Milestone Decision points B and C.

10.5.2.1. Assessment of MDAP Technologies

The TRA final report for MDAPs must be submitted to ASD(R&E) for review to support the requirement that ASD(R&E) provide an independent assessment to the Milestone Decision Authority.

10.5.2.2. Technology Readiness Levels (TRLs)

A summary table of TRL descriptions, Table **10.5.2.2.T1** follows:

Table 10.5.2.2.T1. TRL Descriptions

Technology Readiness Level	Description
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.

7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

The use of TRLs enables consistent, uniform, discussions of technical maturity across different types of technologies. Decision authorities will consider the recommended TRLs (or some equivalent assessment methodology, e.g., Willoughby templates) when assessing program risk. TRLs are a measure of technical maturity. They do not discuss the probability of occurrence (i.e., the likelihood of attaining required maturity) or the impact of not achieving technology maturity.

For additional information, see the on-line TRA Deskbook .

10.5.3. Preliminary Design Review (PDR) Review and Assessment

10.5.3.1. Preliminary Design Review (PDR) Report

10.5.4. Post-Preliminary Design Review (Post-PDR) Assessment Decision Review

10.5.5. Post-Critical Design Review (Post-CDR) Assessment

10.5.6. Independent Program Assessment (IPA)

10.5.7. Performance Assessments and Root Cause Analyses (PARCA)

10.5.7.1. Performance Assessments

10.5.7.2. Root Cause Analyses

10.5.8. Enterprise Risk Assessment Methodology (ERAM)

10.5.3. Preliminary Design Review (PDR) Review and Assessment

P.L. 111-23, the Weapon Systems Acquisition Reform Act of 2009 , established conduct of PDR before MS B as a mandatory requirement for all MDAPs. The Program Manager (PM) shall plan a Preliminary Design Review (PDR); PDR planning shall be reflected in the Technology Development Strategy (TDS), details should be provided in the Systems Engineering Plan (SEP), and shall be conducted consistent with the policies specified in DoD Instruction 5000.02 . The plan for PDR will be reflected in the TDS to be approved by the MDA at MS A. Post-PDR assessments will be conducted in association with MS B preparations and will be formally considered by the Milestone Decision Authority (MDA) at the MS B 2366b certification review.

PDRs before MS B for other than MDAPs will be approved by the MDA when consistent with TDS or Acquisition Strategy objectives. When the PDR is conducted before MS B, a post-PDR assessment will be conducted in association with the MS B review and formally considered by the MDA at the MS B review. If the PDR is conducted after MS B, the MDA will conduct a post-PDR assessment at a time reflected in the approved acquisition strategy.

If a PDR has not been conducted prior to Milestone B (non-MDAPs), the PM shall plan for a PDR as soon as feasible after program initiation. PDR planning shall be reflected in the Acquisition Strategy and conducted consistent with the policies specified in paragraph 5.d.(6) of DoD Instruction 5000.02 .

10.5.3.1. Preliminary Design Review (PDR) Report

The PDR Report shall be provided as a memorandum to the Milestone Decision Authority (MDA). When the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) is the MDA for a program, the PDR Report should b provided by a memorandum to the USD(AT&L), with copies to the Deputy Assistant Secretary of Defense (Systems Engineering) and the Overarching Integrated Product Team Leader.

The PDR Report should include:

1. A comprehensive list of the systems engineering products that make up the allocated baseline (to include the preliminary design specifications for all configuration items) and that were subject to review;
2. A list of the participants in the review including the PDR chair, applicable technical authorities, independent subject matter experts, and other key stakeholders;
3. A summary of the action Items from the review and their closure status/plan;
4. A risk assessment using the PDR risk assessment checklist (Found at Line 834 of the DOD PDR Checklist) or similar, and preliminary Environment, Safety, and Occupational Health hazard lists/assessments to determine readiness to commit

to full detail design; and
5. A recommendation from the PDR as to the approval of the program's system allocated baseline to support detail design.

The PDR Report shall be provided to the MDA prior to Milestone B and include recommended technical requirements trades based upon an assessment of cost, schedule, and performance risk.

10.5.4. Post-Preliminary Design Review (Post-PDR) Assessment Decision Review

When the system-level PDR is conducted after Milestone B (for non-MDAPs only), the Program Manager (PM) shall plan and the Milestone Decision Authority (MDA) shall conduct a formal Post-PDR Assessment Decision Review. The MDA shall conduct a formal program assessment and consider the results of the PDR and the PM's assessment in the PDR Report, and determine whether remedial action is necessary to achieve Acquisition Program Baseline objectives. The results of the MDA's Post-PDR Assessment shall be documented in an Acquisition Decision Memorandum. The Post-PDR assessment shall reflect any requirements trades based upon the PM's assessment of cost, schedule, and performance risk.

10.5.5. Post-Critical Design Review (Post-CDR) Assessment

The Milestone Decision Authority (MDA) may assess the programs design maturity and technical risks following the system-level Critical Design Review (CDR) .

1. The Office of the Deputy Assistant Secretary of Defense (Systems Engineering) (DASD(SE)) will participate in CDRs for Major Defense Acquisition Programs (MDAPs) and prepare a brief assessment of design maturity and technical risk which may require MDA attention. Consequently, MDAP Program Managers (PMs) shall be required to invite DASD(SE) engineers to their system-level CDRs and make CDR artifacts available. The draft CDR assessment will be coordinated with the PM prior to forwarding to the MDA.
    1. Unless directed otherwise by their Component MDA, the PMs for non-MDAP programs shall provide a Post-CDR Report to the MDA as that provides an overall assessment of design maturity and a summary of the system-level CDR results which shall include, but not be limited to:
        1. The names, organizations, and areas of expertise of independent subject matter expert participants and CDR chair;
        2. A description of the product baseline for the system and the percentage of build-to packages completed for this baseline;
        3. A summary of the issues and actions identified at the review together with their closure plans;
        4. An assessment of risk by the participants against the exit criteria for the Engineering & Manufacturing Development Phase; and
        5. Identification of those issues/risks that could result in a breach to the program baseline or substantively impact cost, schedule, or

performance.

2. All PMs shall continue to document CDRs in accordance with Component best practices.

The CDR risk assessment checklist is designed as a technical review preparation tool, and should be used as the primary guide for assessing risk during the review. This checklist is available on the Systems Engineering Community of Practice.

The MDA shall review the Post-CDR Report (or Assessment for an MDAP) and the PM's resolution/ mitigation plans and determine whether additional action is necessary to satisfy EMD Phase exit criteria and to achieve the program outcomes specified in the APB. The results of the MDA's Post-CDR Assessment Decision Review shall be documented in an ADM staffed by the DAB Executive Secretary.

10.5.6. Independent Program Assessment (IPA)

An IPA in this context is an independent, comprehensive, and systemic review of managerial and technical progress on a major program. IPAs are designed to identify program cost, schedule, and performance risks; formulate risk mitigation plans; and provide feedback both to the Program Manager and the Milestone Decision Authority (MDA).

For space programs, an IPA must be provided to support each milestone, at the Post-System Design Review Assessment, and at any other time as directed by the MDA. IPAs may also be used to assess other types of programs.

10.5.7. Performance Assessments and Root Cause Analyses (PARCA)

The Director, PARCA (D, PARCA) was established by the Weapon Systems Acquisition Reform Act of 2009 (section 103 of P.L. 111-23,) to conduct and oversee performance assessments and root cause analyses for Major Defense Acquisition Programs (MDAPs). (**Note:** D, PARCA has no program execution responsibility.)

10.5.7.1. Performance Assessments

Per section 103 P.L. 111-23, the Director, Performance Assessments and Root Cause Analyses (D, PARCA) is required to conduct assessments and analyses periodically or when requested by senior Department officials. At a minimum, the D, PARCA must also advise acquisition officials on performance issues regarding an MDAP that may arise:

- Prior to a critical cost breach (aka, Nunn-McCurdy) certification;
- Prior to entry into full-rate production; or
- In the course of consideration of any decision to request authorization of a multiyear procurement contract.

Also, per section 205 P.L. 111-23 , in the case of a program that receives a Nunn-

McCurdy certification, the D, PARCA must also assess the program not less often than semi-annually, in the year following a new milestone approval.

The D, PARCAs performance assessments evaluate the cost, schedule, and performance of MDAPs, relative to current metrics, including performance requirements, and baseline parameters. These assessments determine the extent to which the level of program cost, schedule, and performance relative to established metrics is likely to result in the timely delivery of a capability to the warfighter.

10.5.7.2. Root Cause Analyses

Per section 103 P.L. 111-23 , the Director, Performance Assessments and Root Cause Analyses (D, PARCA) is required to conduct Root Cause Analyses (RCAs) for MDAPs to determine the underlying cause or causes for shortcomings in cost, schedule, and performance including the role of unrealistic performance expectations, unrealistic baseline estimates for cost and schedule, immature technologies, unanticipated requirements changes, quantity changes, poor program management, funding instability, or any other matters. The RCAs are used to inform senior Departmental leadership of issues and are included as one-pagers in the Nunn McCurdy certification packages sent to Congress.

10.5.8. Enterprise Risk Assessment Methodology (ERAM)

The Business Capability Lifecycle (BCL) model for Defense Business Systems (DBS) utilizes an independent risk assessment, known as ERAM, as mandatory input to MS A and B decisions for Major Automated Information Systems (MAIS) DBS.

The ERAM assessment is a collaborative, forward-looking, end-to-end view of internal and external program risk that:

- Provides critical insight to decision makers
- Identifies risks (not issues) and corresponding mitigation strategies, in collaboration with key program personnel
- Focuses on execution and implementation rather than compliance

Additional ERAM assessments may be requested by an Investment Review Board Chair, the DBS Certification Authority, or the Milestone Decision Authority. (The Component Acquisition Executive is responsible for establishing procedures designed to assess risk for DBS that do not meet the MAIS thresholds.)

10.6. Information Sharing and DoD Oversight

10.6.1. Program Information

10.6.2. Life-Cycle Management of Information

10.6.3. Classification and Management of Sensitive Information

10.6.1. Program Information

It is Department of Defense (DoD) policy to keep reporting requirements to a minimum. Nevertheless, complete and current program information is essential to the acquisition process. Consistent with the tables of required regulatory and statutory information in DoD Instruction 5000.02 ; decision authorities require program managers and other participants in the defense acquisition process to present the minimum information necessary to understand program status and make informed decisions. The Milestone Decision Authority tailors program information case-by-case, as necessary. Integrated Product Teams facilitate the management and exchange of program information.

The Program Manager, the DoD Component, or the Office of the Secretary of Defense (OSD) staff prepares most program information. Some information requires approval by an acquisition executive or other senior decision authority. Other information is for consideration only. In most cases, information content and availability are more important than format.

Unless otherwise specified, all plans, waivers, certifications and reports of findings referred to in this Guidebook are exempt from licensing under one or more exemption provisions of DoD 8910.1-M .

10.6.2. Life-Cycle Management of Information

Program Managers (PMs) will comply with recordkeeping responsibilities under the Federal Records Act for the information collected and retained in the form of electronic records (See DoD Directive 5015.2 .). Electronic record-keeping systems should preserve the information submitted, as required by section 3101 of title 44, United States Code and implementing regulations. Electronic record-keeping systems should also provide, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted. PMs must consider the record-keeping functionality of any systems that store electronic documents and electronic signatures to ensure users have appropriate access to the information and can meet the Agency's record-keeping needs.

10.6.3. Classification and Management of Sensitive Information

Program Managers (PMs) must review their programs to identify and document critical program information (CPI) requiring protection (DoD Instruction 5200.39). (PMs) must also review their programs to identify controlled unclassified information (CUI). CUI includes "FOUO" information as defined in DoD Directive 5230.24 and information with other approved markings requiring dissemination controls that are exempt from mandatory disclosure under the Freedom of Information Act (e.g., DoD 5400.7-R , DoD Directive 5230.25 , and Export Control Act).

When necessary, PMs develop Security Classification Guides in accordance with DoD 5200.1-R.

10.7. Management Control

Program Managers (PMs) will implement internal management controls in accordance with DoD Directive 5000.01 and DoD Instruction 5000.02 . Acquisition Program Baseline (APB) parameters serve as control objectives. Program managers normally identify deviations from approved APB parameters and exit criteria as material weaknesses. PMs must focus on results, in consonance with most efficient and effective processes. PMs must also ensure that obligations and costs comply with applicable law. Further, they must safeguard assets against waste, loss, unauthorized use, and misappropriation; properly record and account for expenditures; maintain accountability over assets; and quickly correct identified weaknesses.

10.8. Program Plans

Program plans describe the detailed activities of the acquisition program. Except as specified by DoD Instruction 5000.02 , the Program Manager (in coordination with the

Milestone Decision Authority and Program Executive Officer) should determine the type and number of program plans needed to manage program execution.

10.9. Acquisition Program Baseline (APB)

Department of Defense Instruction (DoDI) 5000.02 requires every Program Manager (PM) to propose and document program goals prior to, and for approval at, program initiation for all Acquisition Category (ACAT) programs. For Major Defense Acquisition Programs (MDAPs), the APB satisfies the requirements in section 2435 of title 10 United States Code and section 2220 of title10 United States Code . DoDI 5000.02 mandates the use of an APB for all other ACAT programs. The APB documents the agreement between the PM, the Program Executive Officer, and the Milestone Decision Authority (MDA) and should reflect the approved program being executed.

A separate APB is required for each increment of an MDAP or MAIS program, and each sub-program of an MDAP. Increments can be used to plan concurrent or sequential efforts to deliver capability more quickly and in line with the technological maturity of each increment. (When an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established.)

Program goals consist of an objective value and a threshold value for each Key Performance Parameter and Key System Attribute parameter. Cost, schedule, and performance are intrinsically linked and the objective and threshold values of all program goals should be developed with these relationships in mind. The PM is responsible for managing the trade space between program objectives and thresholds within the bounds of cost, schedule, and performance.

Objective values represent the desired operational goal associated with a performance attribute beyond which any gain in utility does not warrant additional expenditure. Generally, the objective value is an operationally significant increment above the threshold. An objective value may be the same as the threshold when an operationally significant increment above the threshold is not useful.

Thresholds represent the minimum acceptable operational values below which the utility of the system becomes questionable. For performance, a threshold represents either a minimum or maximum acceptable value, while for schedule and cost, thresholds would normally represent maximum allowable values. The failure to attain program thresholds may degrade system performance, delay the program (possibly impacting related programs or systems), or make the program too costly. The failure to attain program thresholds, therefore, places the overall affordability of the program and/or the capability provided by the system into question.

As noted above, each APB parameter must have both an objective and a threshold. For each performance parameter, if no objective is specified, the threshold value will serve as the objective value, and if no threshold is specified, the objective value will serve as the threshold value. For schedule and cost parameters, there are specified default

threshold values. The default threshold for schedule is the objective value plus 6 months; the default threshold for cost is the objective value plus 10 percent of the objective value. Despite these guidelines, the PM may propose (with justification) an appropriate threshold value to optimize program trade space, subject to MDA and user approval.

The PM derives the APB from the users' performance requirements, schedule planning and requirements, and best estimates of total program cost consistent with projected funding. The sponsor of a capability needs document (i.e., Capability Development Document or Capability Production Document) provides an objective and a threshold for each attribute that describes an aspect of a system or capability to be developed or acquired. The PM will use this information to develop an optimal product within the available trade space. APB parameter values should represent the program as it is expected to be developed, produced and/or deployed, sustained and funded.

Per section 2435 of title 10 United States Code , the Department of Defense may not obligate funds for Major Defense Acquisition Programs after entry into Engineering and Manufacturing Development without an MDA-approved APB unless the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) specifically approves the obligation. DoD Instruction 5000.02 extends this policy to Major Automated Information System (MAIS) programs.

10.9.1. Acquisition Program Baseline (APB) Approval Process

The Milestone Decision Authority (MDA) is the approval authority for the APB. The APB requires the concurrence of the Program Executive Officer for all Acquisition Category (ACAT) programs, and the concurrence of the DoD Component Acquisition Executive for ACAT ID and IAM programs.

The Program Manager (PM), in coordination with the user/sponsor, prepares the APB for program initiation. The PM can propose a revision of the APB for approval at each major milestone review and as the program enters full rate production/deployment.

The PM may also *propose* , for consideration by the Milestone Decision Authority (MDA), a revision of the APB that reflects the result of a major program restructure that occurs between milestone events and is fully funded. The MDA will decide whether or not to approve such a proposal.

All ACAT ID and IAM program APBs and Joint Requirements Oversight Council Interest program APBs must be submitted to the office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))-specifically the office of the Director, Acquisition Resources and Analysis (ARA)-for action. ARA will coordinate ACAT ID and IAM APBs with the appropriate Department stakeholders, minimally including Defense Acquisition Board principals and advisors, prior to forwarding for MDA approval.

10.9.1.1. Trade-Offs

Maximizing Program Manager (PM) and contractor flexibility to make cost/performance trade-offs is essential to achieving cost objectives. The PM may treat the difference between an objective and its associated threshold as trade space if the combination values lie within the established thresholds and objectives. Additionally, as development trade space is exercised, the impacts between cost, schedule, and performance should be understood and considered so that values remain within their established objectives and thresholds.

The best time to reduce total ownership cost and program schedule is early in the acquisition process. Continuous cost/schedule/performance trade-off analyses can help attain cost and schedule reductions.

Cost, schedule, and performance may be traded within the "trade space" between the objective and the threshold without obtaining Milestone Decision Authority (MDA) approval. Making trade-offs outside the trade space (i.e., decisions that result in acquisition program parameter changes) require approval of both the MDA and the capability needs approval authority. Validated Key Performance Parameters may not be traded-off without approval by the validation authority. The PM and the user should work together on all trade-off decisions.

Configuration Steering Boards (CSBs) are a core part of managing the cost, schedule, and performance trade space for acquisition programs.

10.9.2. Acquisition Program Baseline (APB) Management

The Program Manager (PM) should immediately notify the Milestone Decision Authority (MDA) via a Program Deviation Report when the PM's current estimate exceeds one or more APB threshold value for cost, schedule, and/or performance.

Only the MDA can approve a revision to the APB. Before undertaking revisions to an APB for a Major Defense Acquisition Program (MDAP), consultation with office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))-specifically the office of Acquisition Resources and Analysis (ARA)-and the Overarching Integrated Product Team leader is recommended.

For MDAPs, both "original" and current APBs are maintained. The original APB cost estimate may be revised ***only if a breach occurs that exceeds the critical unit cost threshold for the program*** . The "critical" unit cost threshold, as it relates to the original APB, is defined to be an increase of at least 50 percent over the original Program Acquisition Unit Cost (PAUC) or the original Average Procurement Unit Cost (APUC) for the program. The "critical" unit cost threshold, as it relates to the current APB, is defined to be an increase of at least 25 percent over the current PAUC or current APUC for the program.

For MAIS programs, only a current APB is maintained, but the Original Estimate reported in the MAIS Annual Report (MAR) serves a similar purpose as an Original APB Baseline. (The MAR Original Estimate unlike the APB can be revised only after a Critical Change Report has been submitted to Congress. MAIS Critical Change thresholds are: cost parameter (Total Acquisition Cost or Total Lifecycle Cost) 25 percent or greater, schedule parameter of 12 months or greater, or failure to meet a key performance threshold.)

For both MDAP and MAIS programs, the current APB shall be revised at major milestone decisions, and at the full-rate production decision (full deployment decisions for MAIS). Other than these occasions, a revision to the current APB may be considered ***only at the discretion of the MDA*** and only if the revision is a result of a major program restructure that is fully funded and approved by the MDA, or that occurs as a result of a program deviation (breach), that is primarily the result of external causes beyond the control of the PM. A revision to the current APB ***shall not*** be authorized if it is proposed merely to avoid a reportable breach. The determination of whether to revise the APB will be made by the MDA.

For MDAPs, a "critical" unit cost breach triggers the section 2433a of title 10, United States Code (a.k.a "Nunn-McCurdy") certification process. In that case, both the current and original APBs shall be revised to reflect the same new APB values, assuming the program is certified. For MAIS programs, a Critical Change triggers the similar process implementing section 2445c of title 10, United States Code

10.9.3. Acquisition Program Baseline (APB) Content

The APB is a key management document which establishes the approved program's objective and threshold boundaries, and links cost, schedule and performance parameters. The Program Manager (PM) manages the program within that trade space.

10.9.3.1. Acquisition Program Baseline (APB) Cost

Cost figures should reflect realistic cost estimates of the total program and/or increment. Budgeted amounts should equal the total cost objectives in the APB. As the program progresses, the PM can refine procurement costs based on contractor actual (return) costs from Technology Development, Engineering and Manufacturing Development, and Low-Rate Initial Production.

The cost parameters of Acquisition Category (ACAT) IA programs are the same as those for ACAT I programs as noted in the next paragraph with the addition of Defense Working Capital Funds and Other Funding.

The APB should contain cost parameters (objectives and thresholds) for major elements of program life-cycle costs (or total ownership costs), as defined in Chapter 3 .

These elements include:

1. Research, development, test, and evaluation costs
2. Procurement costs (including the logistics cost elements required to implement the approved sustainment strategy)
3. Military construction costs
4. Operations and maintenance (O&M) costs (that support the production and deployment phase, as well as acquisition-related O&M costs, if any)
5. Total system quantity (to include both fully configured development and production unit's)
6. Program Acquisition Unit Cost defined as the total of all acquisition-related appropriations divided by the total quantity of fully configured end items
7. Average Procurement Unit Cost defined as total procurement cost divided by total procurement quantity (***Note:*** *This item and item 6 above do not usually apply to business information technology systems or other software-intensive systems with no production components* .)
8. Any other cost objectives established by the Milestone Decision Authority (e.g., ownership cost)

The objective parameters for cost are presented in both base-year and then-year dollars. The threshold parameters for cost are only presented in base-year dollars.

10.9.3.2. Acquisition Program Baseline (APB) Schedule

Schedule parameters should include, as a minimum, the projected dates for major decision points (such as Milestone A, Milestone B, Milestone C, Full Rate Production, and the system-level Preliminary Design Review and Critical Design Review), major testing events, and Initial Operational Capability. To be consistent with Chapter 144A of title 10, United States Code , the schedule parameters for Major Automated Information System programs should include: the dates of the Milestone A decision (or MDA approval of the preferred alternative if there was no Milestone A), the objective and threshold dates for Milestone B, Milestone C, Full Deployment Decision, and Full Deployment. If Milestones A, B and/or C are tailored out, the APB shall state the rationale for the tailoring. Full Deployment dates should be identified as TBD until the Full Deployment Decision ADM is signed.

The Full Deployment Decision ADM shall establish the Full Deployment objective and threshold dates, define an identifiable Full Deployment, and designate the acquisition official who will declare Full Deployment in writing. When Full Deployment is declared, the PM shall notify the MDA.

The PM may propose, and the MDA may approve, other, specific, critical, and system events.

10.9.3.3. Acquisition Program Baseline (APB) Performance

APB performance parameters should include the key performance parameters identified in the capability needs document(s) (i.e., Capability Development Document (CDD) and Capability Production Document (CPD)), and the values and meanings of objectives and thresholds should be consistent between the APB and the capability document. (See also CJCS Instruction 3170.01H) The number and specificity of performance parameters may change over the lifecycle of the acquisition, primarily at major milestones. At Milestone B (Engineering & Manufacturing Development decision), the APB should reflect the defined, operational-level measures of effectiveness or measures of performance to describe needed capabilities, minimally reflecting the CDD. As a program matures, system-level requirements may become better defined. Approaching the MS C decision, the APB should reflect the CPD. The MDA may also add performance parameters to the APB other than the Joint Requirements Oversight Council (JROC)-validated Key Performance Parameters .

OSD staff will review and comment on APBs for ACAT ID and IAM, Special Interest programs, and other programs designated by the Defense Acquisition Executive. The Joint Staff (J-8) will review the cost, schedule, and key performance parameter objective and threshold values in the APB for JROC Interest programs, and any other programs of significant joint interest (as determined by the J-8). The J-8 review will ensure that the objective and threshold values are consistent with the JROC-approved CDD, CPD, and prior JROC decision(s). The review will also ensure that the baseline provides the necessary warfighting capabilities affordably and within required time frames. (See also the CJCS Instruction 3170.01 H and the January 19, 2012 JCIDS Manual .)

10.9.4. Acquisition Program Baseline (APB) for an Evolutionary Acquisition Program

Evolutionary acquisition is a frequently used Department of Defense (DoD) strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in militarily useful increments, recognizing, up front, the need for future capability improvements.

Programs using an evolutionary acquisition strategy should design the APB consistent with the sponsor's capability document(s) and the applicable example approaches outlined in **Table 10.9.4.T1.**

Table 10.9.4.T1. APB Parameters under an Evolutionary Acquisition Strategy

CDD or CPD	APB
Capability Development Document (CDD) defines multiple increments of capability (CDD should assign each capability to a specific increment)	A separate APB for each increment
A separate CDD for each Increment	A separate APB for each increment
There is one Capability Production Document (CPD) for each production increment	The corresponding APB should be updated to reflect the parameters in the CPD for that production increment

10.9.4.1. Acquisition Program Baseline (APB) for an Increment

DoD Instruction 5000.02 requires the Milestone Decision Authority (MDA) to formally initiate each increment of an evolutionary acquisition program. Program initiation for follow-on increments may occur at Milestone B or C. Therefore, the program manager should develop APB documented goals for each program increment or sub-program. An Increment is a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained. Each Increment must have an Acquisition Program Baseline (APB) with its own set of threshold and objective values set by the user. (DODI 5000.02, Encl.2, 2.c.) In the context of an IS acquisition, this means that both threshold and objective values for cost, schedule, and performance parameters must be established for each Increment.

10.9.4.2. Acquisition Program Baseline (APB) for a Subprogram

When an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established for baseline development and reporting purposes. Section 2430A of title 10, United States Code stipulates that when one subprogram is designated within an MDAP, all remaining elements (increments or components) of the program shall also be appropriately organized into one or more other subprograms.

The decision whether to establish subprograms for an MDAP requires careful analysis and must be made on a case-by-case basis. Structuring an MDAP with subprograms should reflect the way the program is being managed, and represent the most efficient and informative way to convey information about a program to senior defense acquisition officials as well as to the Congress.

The law requires that the congressional defense committees be notified in writing of any proposed subprogram designation not less than 30 days before the date such

designation takes effect. The approval of an APB reflecting such designation will be considered the date that subprogram designation takes effect; therefore, notification to Congress must occur not less than 30 days before a subprogram APB is approved. Accordingly, DoD Components must notify the Director, Acquisition Resources and Analysis of all proposed APBs that reflect new or revised subprogram designation at least 60 days before the proposed APB is submitted to the Milestone Decision Authority for approval.

10.10. Periodic Reports

Periodic reports include only those reports required by statute or the Milestone Decision Authority (MDA). Except for the reports outlined in this section, the MDA tailors the scope and formality of reporting requirements.

10.10.1. Statutory Reporting for Major Defense Acquisition Programs (MDAPs)

10.10.1.1. Revised MDAP Definition

P. L. 111-23, Weapons Systems Acquisition Reform Act of 2009 , May 22, 2009, amended section 2430 of title 10 United States Code , revising the definition of a Major Defense Acquisition Program (MDAP) as follows. A MDAP is a DoD acquisition program that is not a highly sensitive classified program and:

(1) That is designated by the USD(AT&L) as a MDAP; or

(2) That is estimated to require an eventual total expenditure for research, development, test, and evaluation of more than $365 million (based on fiscal year 2000 constant dollars) or an eventual total expenditure for procurement, including all planned increments or spirals, of more than $3.19 billion (based on fiscal year 2000 constant dollars).

For the purposes of establishing a program as an MDAP, the following, as applicable, shall be considered:

(1) The estimated level of resources required to fulfill the relevant joint military requirement as determined by the JROC, pursuant to section 181 of title 10 United States Code;

(2) The cost estimate referenced in section 2366a(a)(4) of title 10 United States Code;

(3) The cost estimate referenced in section 2366b(a)(1)(C) of title 10 United States Code ; and

(4) The cost estimate within a baseline description as required by section 2435 of title 10 United States Code .

10.10.1.2. Designation of Subprograms within Major Defense Acquisition Programs (MDAPs)

The National Defense Authorization Act (NDAA) for FY 2009 amended section 2430 of title 10 United States Code to give the Department authority to designate subprograms within MDAPs.

The Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) (as delegated by the Secretary of Defense) may designate subprograms within an MDAP. That is, when an MDAP requires the delivery of two or more categories of end items that differ significantly in form and function, subprograms may be established for base-lining and reporting purposes. The law stipulates that when one subprogram is designated within an MDAP, all remaining elements (increments or components) of the program shall also be appropriately organized into one or more subprograms.

In the DoD acquisition environment, there are two primary instances when establishing subprograms within an MDAP may be advisable:

1. The first instance is a product of evolutionary acquisition when increments or blocks of capability are acquired in a sequential manner. With subprogram reporting, each of these increments can be baselined and tracked separately for cost (including unit cost), schedule, and performance purposes within a single MDAP without the risk of artificial cost growth or a critical cost (a.k.a, Nunn-McCurdy) breach occurring when a subsequent increment is initiated. In accordance with DoDI 5000.02, each evolutionary increment must have its own Milestone B (or Milestone C, if initiated at production) and its own Acquisition Program Baseline (APB). The requirement for a separate APB for each evolutionary increment is satisfied through the establishment of an APB containing subprograms. An example of this type of subprogram is the block upgrade of a missile system that provides significant increases in altitude and/or range.
2. The second instance is when there are major components of a program that are dissimilar and therefore cannot be combined in a rational way to produce a unit cost that is representative of the program. An example is the use of separate subprograms for satellites and ground-based receivers to improve visibility and unit cost reporting.

The decision whether to establish subprograms within an MDAP requires careful analysis and must be made on a case-by-case basis. Structuring an MDAP with subprograms should reflect the way the program is being managed, and represent the

most efficient and informative way to convey information about a program to senior defense acquisition officials as well as to Congress. For Acquisition Category (ACAT) ID MDAPs, the Defense Acquisition Executive will approve the designation of subprograms based on recommendations from the Overarching Integrated Product Team (OIPT). For ACAT IC MDAPs, the authority to designate subprograms is delegated to the respective DoD Component Milestone Decision Authority (MDA). In either case, the recommendations from the OIPT or the MDAs staff should also include appropriate guidance on how the relevant statutory and regulatory requirements of DoD Instruction 5000.02 should apply at the subprogram or program level (for example, how to structure the acquisition strategy or the independent cost estimate for a program with designated subprograms).

10.10.1.2.1. Subprogram Notification

The law requires that the Secretary of Defense (as delegated to the Under Secretary of Defense (Acquisition, Technology, and Logistics) must notify the congressional defense committees in writing of any proposed subprogram designation not less than 30 days before the date such designation takes effect. The approval of an Acquisition Program Baseline (APB) reflecting such designation will be considered the date that the subprogram designation takes effect; therefore, notification to Congress must occur not less than 30 days before a subprogram APB is approved.

Accordingly, DoD Components must notify the Director, Acquisition Resources and Analysis of all proposed APBs that reflect new or revised subprogram designations at least 60 days before the proposed APB is submitted to the Milestone Decision Authority for approval. Once a subprogram structure is established for a Major Defense Acquisition Program, the Defense Acquisition Executive Summary , Selected Acquisition Report, and Unit Cost Reports (quarterly and breach) will reflect that subprogram structure.

10.10.1.2.2. Subprogram Critical Cost Growth

In the event a subprogram experiences critical unit cost growth, the certification required for the program to continue shall be made at the program level-not the subprogram level.

10.10.1.2.3. Prohibition on Obligations (Subprograms)

The prohibition on obligations until the submission of the Selected Acquisition Report (SAR) for significant breaches, and the certification for critical breaches, will affect all major contracts of the program, not just those relating to the subprogram that breached.

10.10.1.3. Acquisition Program Baseline (APB) Reporting

10.10.1.3.1. Program Deviations

The Program Manager (PM) must maintain a current estimate of the program being executed (see definition of "current estimate" in section 10.10.1.3.2). The PM must immediately notify the Milestone Decision Authority when a baseline deviation occurs based upon the current estimate. A baseline deviation occurs when the current estimate is greater than the threshold. (See section 2433 of title 10 United States Code)

10.10.1.3.2. Current Estimate

The current estimate is the latest estimate of program acquisition cost and quantity, schedule milestone dates, performance characteristic values, and critical technical parameters of the approved program (i.e., the approved program as reflected in the currently approved Acquisition Program Baseline (APB), Acquisition Decision Memorandum, or in any other document containing a more current decision of the Milestone Decision Authority (MDA) or other approval authority). For cost, the current estimate is normally the President's Budget plus or minus known changes; for schedule, it is normally the program manager's best estimate of current schedule milestone dates; for performance it is normally the program's manager's best estimate of current performance characteristics values.

Program Managers (PMs) will report the current estimate of each APB parameter periodically to the MDA. PMs will report current estimates for ACAT I and IA programs quarterly in the Defense Acquisition Executive Summary. For all other programs, the cognizant MDA will direct the reporting frequency.

10.10.1.3.3. Program Deviation Reporting

When the Program Manager (PM) has reason to believe that the current estimate for the program indicates that a performance, schedule, or cost threshold value will not be achieved, he or she will immediately notify the Milestone Decision Authority (MDA) of the deviation. Within 30 days of the occurrence of the program deviation, the PM will submit a Program Deviation Report to the MDA providing the reasons for the program deviation and a recommendation for the actions that need to be taken to bring the program back within the baseline parameters (if this information was not included with the original notification). Within 90 d days of the occurrence of the program deviation, one of the following should have occurred: the program is back within Acquisition Program Baseline (APB) parameters; or an OIPT-level or equivalent Component-level review has been conducted to review the program and make recommendations to the MDA regarding the parameters that were breached. The MDA will decide, based on criteria in sections 2433 and 2435 of title 10 United States Code, whether it is appropriate to approve a revision to the APB. (Generally, APB changes will only be approved in conjunction with a major milestone decision or as a result of a critical cost (a.k.a. Nunn-McCurdy) breach. In limited circumstances, the MDA may choose to

approve a change to the current APB as a result of a major program restructure that is fully funded, or as a result of a program deviation--if the breach is primarily the result of external causes beyond the Program Managers control. A revision to the current APB ***will not*** be authorized if it is proposed merely to avoid a reportable breach.

If one of the above actions has not occurred within 90 days of the program deviation, the MDA should hold a formal program review to determine program status and the way ahead.

10.10.1.4. Selected Acquisition Report (SAR) Requirement

In accordance with section 2432 of tile 10, United States Code , the Secretary of Defense (as delegated to the Under Secretary of Defense (Acquisition, Technology, and Logistics shall submit a SAR to Congress for all Major Defense Acquisition Programs (MDAPs). The Program Manager will use the Defense Acquisition Management Information Retrieval system SAR module application to prepare the SAR.

10.10.1.4.1. Selected Acquisition Report (SAR) Content and Submission

A SAR provides Congress with the status of total program cost, schedule, and performance, as well as program unit cost and unit cost breach information for a specific program. Each SAR will also include a full life-cycle cost analysis for the reporting program, each of its evolutionary increments, as available, and for its antecedent program, if applicable. Required content for a SAR is defined in section 2432 of title 10 United States Code and is reflected in the SAR module of the Defense Acquisition Management Information System by which the SAR information is entered and submitted electronically.

The SAR for the quarter ending December 31 is the annual SAR. The Program Manager (PM) will submit the annual SAR within 45 days after the President transmits the following fiscal year's budget to Congress. Annual SARs will reflect the President's Budget and supporting documentation. The annual SAR is mandatory for all ACAT I programs.

The PM will submit quarterly exception SARs for the quarters ending March 31, June 30, and September 30 not later than 45 days after the quarter ends. Quarterly SARs are reported on an exception basis, as follows:

- The current estimate exceeds the Program Acquisition Unit Cost (PAUC) objective or the Average Procurement Unit Cost (APUC) objective of the currently approved Acquisition Program Baseline (APB) in base-year dollars by 15 percent or more;
- The current estimate exceeds the PAUC or APUC objective of the original APB in base-year dollars by 30 percent or more.
- The current estimate includes a 6-month, or greater, delay for any schedule parameter that occurred since the current estimate reported in the previous SAR;

- Milestone B or Milestone C approval occurs within the reportable quarter.

Quarterly exception SARs will report the current estimate of the program for cost, schedule, and performance (see definition of current estimate in section 10.10.1.3.2. above). Pre-Milestone B programs may submit Research, Development, Test, and Evaluation (RDT&E)-only reports, excluding procurement, military construction, and acquisition-related operations and maintenance costs. Department of Defense Components must notify the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) of the names of the programs for which they intend to submit RDT&E-only SARs 30 days before the reporting quarter ends. The USD(AT&L) must also notify Congress 15 days before the reports are due.

Whenever the USD(AT&L) proposes changes to the content of a SAR, he or she must submit notice of the proposed changes to the Armed Services Committees of the Senate and House of Representatives. The USD(AT&L) may consider the changes approved, and incorporate them into the SAR, 60 days after the committees receive the change notice.

Per section 2433(c)(2) of title10, United States Code , for any Major Defense Acquisition Program (MDAP) certified subsequent to a critical cost breach, the first SAR for the program submitted after the President submits a budget in the calendar year following the year in which the program was restructured must include a description of all funding changes made as a result of the growth in cost of the program, including reductions made in funding for other programs to accommodate such cost growth.

Per section 2366b of title 10, United States Code , the SAR for any MDAP receiving a waiver for one or more Milestone (MS) B certification criteria must prominently and clearly indicate that such program has not fully satisfied the certification requirements for MS B, until such time that the Milestone Decision Authority makes a determination that the program has satisfied all such certification requirements.

10.10.1.4.2. Selected Acquisition Report (SAR) Waivers

In accordance with section 2432 of title 10, United States Code , the Secretary of Defense may waive the requirement for submission of a SAR for a program for a fiscal year if:

- The program has not entered Engineering and Manufacturing Development;
- A reasonable cost estimate has not been established for the program; and,
- The system configuration for the program is not well defined.

As delegated by the Secretary of Defense, the Under Secretary of Defense (Acquisition, Technology, and Logistics) will submit a written notification of each waiver for a fiscal year to the Armed Services Committees of the Senate and House of Representatives not later than 60 days before the President submits the budget to Congress, pursuant to

section 1105 of title 31, United States Code in that fiscal year.

10.10.1.4.3. Selection Acquisition Report (SAR) Termination

The Under Secretary of Defense (Acquisition, Technology, and Logistics) will consider terminating reporting of SAR data when 90 percent of expected production deliveries or planned acquisition expenditures have been made, or when the program is no longer considered an ACAT I program in accordance with section 2432 of tile 10, United States Code .

10.10.1.5. Unit Cost Reports (UCR)

In accordance with section 2433 of title 10, United States Code , the Program Manager will prepare UCRs for all ACAT I programs submitting Selected Acquisition Reports, except pre-Milestone B programs that are reporting Research, Development, Test & Evaluation costs only.

10.10.1.5.1. Unit Cost Report (UCR) Content and Submission

The Program Manager (PM) will report the unit costs of the program to the Component Acquisition Executive on a quarterly basis through the electronic Defense Acquisition Executive Summary (DAES) submission process. The PM will submit the update in accordance with DAES submission procedures. Reporting will begin with submission of the initial Selected Acquisition Report (SAR), and terminate with submission of the final SAR. Content of the unit cost report is specified in section 2433 of title 10, United States Code.

Each report will include:

1. The program acquisition unit cost for the program (or for each designated major subprogram under the program).
2. In the case of a procurement program, the current estimate of the Program Acquisition Unit Cost and the Average Procurement Unit Cost (in base-year dollars) for the program (or for each designated major subprogram under the program);
3. Any earned value management cost and schedule variances, for each of the major contracts since entering the contract;
4. Any changes from program schedule milestones or program performances reflected in the baseline description established under section 2435 of title 10, United States Code that are known, expected, or anticipated by the program manager.
5. Any significant changes in the total program cost for development and procurement of the software component of the program or subprogram, schedule milestones for the software component of the program or subprogram, or expected performance for the software component of the program or subprogram

that are known, expected, or anticipated by the program manager.

10.10.1.5.1.1. Unit Cost Reporting (UCR) for the Software Component of a Major Defense Acquisition Program (MDAP)

Section 2433(b)(5) of title 10, United States Code requires reporting of any significant changes in the total program cost for development and procurement of the software component of the program or subprogram, schedule milestones for the software component of the program or subprogram, or expected performance for the software component of the program or subprogram that are known, expected, or anticipated by the program manager.

This is essentially a requirement to separately establish a cost and schedule baseline for the software component of a MDAP program or subprogram. However the definition of software component is not defined in the statute. Therefore, in the context of unit cost reporting, the definition of software development element for the Software Resources Data Report (SRDR) (see DoDI 5000.02, Enclosure 4, Table 4 Regulatory Contract Reporting Requirements) is used as the proxy for software component referenced in the statute. (Reporting of software efforts above $20M is required for the purposes of SRDRs as defined in DoD 5000.04-M-1 .)

Under this reporting framework, the Initial Government Report (IGR) and/or the contractors Initial Developer Report (IDR) should be used as the baselines to develop a cost and schedule software component estimate. (The IGR and IDR are established within 120 days of the contract award, or within 60 days of beginning a software release, and are updated at the completion of a software increment to reflect the actual resources incurred). Note that the SRDR includes only software resource requirements (staffing and schedule), not cost explicitly. However, PMs can, and should, use these parameters to compute a cost estimate.

The PMs software component estimate must be documented in the Acquisition Program Baseline and used as the basis for determining whether there are any significant changes in the total program cost for development and procurement of the software component of the program or subprogram, schedule milestones for the software component of the program or subprogram, or expected performance for the software component of the program or subprogram that are known, expected, or anticipated by the program manager. Any such changes must be addressed in the UCR.

Any PM with an APB for an MDAP (or it's subprogram) that does not currently include a software component estimate must complete the estimate and report it in the unit cost portion of the next program (or subprogram) SAR. A footnote must be included to indicate that this estimate will be the baseline against which future change in the software component cost will be compared.

10.10.1.5.2. Unit Cost Report (UCR) Breach Reporting

If the program manager of a major defense acquisition program determines at any time during a quarter that there is reasonable cause to believe that the Program Acquisition Unit Cost for the program (or for a designated major subprogram under the program) or the Average Procurement Unit Cost for the program (or for such a subprogram), as applicable, has increased by a percentage equal to or greater than the significant cost growth threshold or the critical cost growth threshold, the breach must be reported in accordance with section 2433 of title 10 United States Code .

When one or more problems with the software component of the Major Acquisition Defense Program, or any designated major subprogram under the program, has significantly contributed to the increase in program unit costs, the action taken and proposed to be taken to solve such problems must also be included in the Selected Acquisition Report (SAR). The only exception to that requirement occurs when a program acquisition unit cost increase or a procurement unit cost increase for a major defense acquisition program or designated major subprogram results in a termination or cancellation of the entire program or subprogram.

10.10.1.5.2.1. Significant Cost Growth Notification Requirements

The Program Manager will notify the Component Acquisition Executive (CAE) immediately, whenever there is a reasonable cause to believe that the current estimate of either the Program Acquisition Unit Cost (PAUC) or Average Procurement Unit Cost (APUC) (in base-year dollars) of a Major Defense Acquisition Program, or designated subprogram, has increased by at least 15 percent over the PAUC or APUC objective of the currently approved Acquisition Program Baseline (APB), respectively, or has increased by at least 30 percent over the PAUC or APUC of the original/revised original APB.

If the CAE determines that there is an increase in the current estimate of the PAUC or APUC objective of at least 15 percent over the currently approved APB, or an increase of at least 30 percent over the original APB, the CAE, based on the PMs notification, shall inform the cognizant Head of the DoD Component of this determination. If the cognizant Head of the DoD Component subsequently determines that there is, in fact, an increase in the current estimate of the PAUC or APUC of at least 15 percent over the currently approved APB, or an increase in the current estimate of the PAUC or APUC of at least 30 percent over the original APB, the Head of the DoD Component will notify Congress, in writing, of the determination of a significant cost breach. The notification will be made not later than 45 days after the end of the quarter, in the case of a quarterly report; or not later than 45 days after the date of the report, in the case of a report based on reasonable cause. In either case, notification will include the date that the Head of the DoD Component made the determination. In addition, the Head of the DoD Component will submit a Selected Acquisition Report (SAR) for either the fiscal year quarter ending on or after the determination date, or for the fiscal year quarter that immediately precedes the fiscal year quarter ending on or after the determination date.

This SAR shall contain the additional, breach-related information.

The cognizant Head of the DoD Component shall also inform the Under Secretary of Defense (Acquisition, Technology, and Logistics) of the significant cost breach determination not later than five working days prior to submitting the congressional notification.

10.10.1.5.2.2. Critical Cost Breach Certification Requirements

Per section 2433a of title 10 United States Code , the Program Manager shall notify the Department of Defense Component Acquisition Executive (CAE) immediately, whenever there is a reasonable cause to believe that the current estimate of either the Program Acquisition Unit Cost (PAUC) or Average Procurement Unit Cost (APUC) objective of a Major Defense Acquisition Program (MDAP),, or designated subprogram (in base-year dollars) has increased by at least 25 percent over the PAUC or APUC objective of the currently approved Acquisition Program Baseline (APB) estimate, or at least 50 percent over the PAUC or APUC objective of the original/revised original APB (aka Nunn-McCurdy breach).

If the CAE determines that there is an increase in the current estimate of the PAUC or APUC objective of at least 25 percent over the currently approved APB, or an increase in the current estimate of PAUC or APUC objective of at least 50 percent over the original APB, the CAE, based upon the PMs notification shall inform the cognizant Head of the DoD Component of this determination. If the cognizant Head of the DoD Component subsequently determines that there is, in fact, an increase in the current estimate of the PAUC or APUC of at least 25 percent over the currently approved APB, or an increase in the PAUC or APUC of at least 50 percent over the original APB, the Head of the DoD Component shall notify Congress, in writing, of the determination of a critical cost breach. The notification shall be not later than 45 days after the end of the quarter, in the case of a quarterly report; or not later than 45 days after the date of the report, in the case of a report based on reasonable cause. In either case, notification shall include the date that the Head of the DoD Component made the determination. In addition, the Head of the DoD Component shall submit a Selected Acquisition Report (SAR) for either the fiscal year quarter ending on or after the determination date, or for the fiscal year quarter that immediately precedes the fiscal year quarter ending on or after the determination date. This SAR shall contain the additional critical cost breach-related information.

The cognizant Head of the DoD Component shall also inform the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) of the critical cost breach determination not later than five working days prior to submitting the congressional notification.

Per section 2433a of title 10, United States Code the USD(AT&L), after consultation with the Joint Requirements Oversight Council regarding program requirements, shall determine the root cause or causes of the critical cost growth in accordance with

applicable statutory requirements and DoD policies, procedures, and guidance based upon the root cause analysis conducted by the Director, Performance Assessments and Root Cause Analyses (DPARCA); and in consultation with the Director, Cost Assessment and Program Evaluation (DCAPE), shall carry out an assessment of:

1. The projected cost of completing the program if current requirements are not modified;
2. The projected cost of completing the program based on reasonable modification of such requirements;
3. The rough order of magnitude of the costs of any reasonable alternative system or capability; and
4. The need to reduce funding for other programs due to the growth in cost of the program.

After conducting the reassessment, the USD(AT&L) shall terminate the program unless the USD(AT&L) submits a written certification to Congress before the end of the 60-day period beginning on the day the SAR containing the unit cost information is required to be submitted to Congress. The certification must state:

1. The continuation of the program is essential to the national security;
2. There are no alternatives to the program that will provide acceptable capability to meet the joint military requirement (as defined in section 181 of title 10, United States Code) at less cost.
3. The new estimates of the PAUC or APUC have been determined by the DCAPE, to be reasonable;
4. The program is a higher priority than programs whose funding must be reduced to accommodate the growth in cost of the program; and
5. The management structure for the program is adequate to manage and control PAUC or APUC.

The written certification shall be accompanied by a report presenting the root cause analysis and assessment and the basis for each determination made in accordance with the five certification criteria listed above together with supporting documentation.

If the USD(AT&L) elects not to terminate a MDAP that has experienced critical cost growth, the USD(AT&L) shall:

1. Restructure the program in a manner that addresses the root cause or causes of the critical cost growth, as identified by the actions described above, and ensure that the program has an appropriate management structure as set forth in the written certification;
2. Rescind the most recent milestone approval for the program or designated subprograms and withdraw any associated certification(s) pursuant to section 2366a or 2366b of title 10, United States Code;
3. Require a new milestone approval for the program or designated subprograms before taking any contract action to enter a new contract, exercise an option

under an existing contract, or otherwise extend the scope of an existing contract under the program, except to the extent determined necessary by the MDA, on a non-delegable basis, to ensure that the program can be restructured as intended by the Secretary of Defense without unnecessarily wasting resources.; and
4. Include in the report a description of all funding changes made as a result of the growth in cost of the program, including reductions made in funding for other programs to accommodate such cost growth. (The report specified here is the first SAR for the program submitted after the President submits a budget in the calendar year following the year in which the program was restructured.)

If, subsequent to a critical breach and based on a cost assessment and root cause analysis, the MDA determines that after eliminating the cost increase attributed to a quantity change the remaining increase to the PAUC is 5 percent or less to the current baseline and 10% or less to the original baseline, the following two requirements from section 2433a of title 10, United States Code may be waived:

1. Requirement to rescind the program's most recent milestone approval and associated MDA Milestone Certification Memorandum,
2. Requirement for a new milestone approval prior to contract actions.

This waiver is only applicable if the change in quantity was not made as a result of an increase in program cost, a delay in the program, or a problem meeting program requirements.

Additionally, for each MDAP that has exceeded the critical unit cost thresholds, but has not been terminated, the DPARCA shall conduct semi-annual reviews until 1 year after the date a new milestone approval is received. The DPARCA shall report the results of the semi-annual reviews to the USD(AT&L) and summarize the results in the Director's next annual report.

If an MDAP is terminated after experiencing a critical unit cost breach, the USD(AT&L) shall submit to Congress a written report with the following information:

1. An explanation of the reasons for terminating the program;
2. The alternatives considered to address any problems in the program; and
3. The course the Department of Defense plans to pursue to meet any continuing joint military requirements otherwise intended to be met by the program.

10.10.1.5.2.3. Restriction on Obligation of Funds

If the Head of the DoD Component makes a determination of either a Program Acquisition Unit Cost (PAUC) or Average Procurement Unit Cost (APUC) increase of at least 15 percent over the current Acquisition Program baseline (APB) or an increase of at least 30 percent over the original/revised original APB and a Selected Acquisition Report (SAR) containing the additional unit cost breach information is not submitted to Congress as required, or if the Head of the DoD Component makes a determination of

either a PAUC or APUC increase of at least 25 percent over the current APB or at least 50 percent over the original/revised APB and a SAR containing the additional unit cost breach information and a certification by the USD(AT&L) is not submitted to Congress as required, funds appropriated for Research, Development, Test & Evaluation, procurement, or military construction may not be obligated for a major contract under the program.

A critical cost breach to the PAUC or APUC that results from the termination or cancellation of an entire program will not require a critical cost breach certification by the USD(AT&L).

10.10.1.6. Reporting Breaches of Milestone A Cost Estimates and Initial Operational Capability (IOC) Objectives

Section 2366a of title 10, United States Code requires the Milestone Decision Authority (MDA) to certify that a cost estimate for the program has been submitted, with the concurrence of the Director of Cost and Program Evaluation, and that the level of resources required to develop and procure the program is consistent with the priority level assigned by the Joint Requirements Oversight Council (JROC).

Section 2366a also requires the Program Manager (PM) to notify the MDA if:

- The projected cost of the certified program, at any time before Milestone B, exceeds the cost estimate submitted at the time of certification by at least 25% or
- The time period required for delivery of an IOC exceeds the schedule objective established in accordance with section 181(b)(5) of title 10, United States Code by more than 25%.

The MDA, in consultation with the JROC, must then determine whether the level of resources required to develop and procure the program remains consistent with the priority assigned by the JROC. The MDA may withdraw the MS A certification or rescind the MS A approval if the MDA determines that such action is in the interest of national defense.

Not later than 30 days after the PM submits a notification to the MDA, the MDA must submit a report to the congressional defense committees that:

- Identifies the root cause(s) of the cost or schedule growth;
- Identifies appropriate acquisition performance measures for the remainder of the development of the program; and
- Includes one of the following:
    - A written certification (with a supporting explanation) stating that-
        - the program is essential to national security;
        - there are no alternatives to the program that will provide acceptable military capability at less cost;
        - new estimates of the development cost or schedule, as appropriate,

are reasonable; and
    - the management structure for the program is adequate to manage and control program development cost and schedule.
- A plan for terminating the development of the program or withdrawal of Milestone A approval, if the Milestone Decision Authority determines that such action is in the interest of national defense.

10.10.1.7. Reporting Status of Milestone A Cost Estimates and Initial Operational Capability (IOC) Objectives

For programs that are expected to be Major Defense Acquisition Programs, the Office of the Under Secretary of Defense for Acquisition Technology and Logistics (OUSD(AT&L) will ensure that the program cost estimate and the IOC objective are documented in the Milestone A Acquisition Decision Memorandum (ADM).

Program Managers are required to submit current program status with respect to the original cost estimate and IOC objective as captured in the MS A ADM on a quarterly basis via the Defense Acquisition Executive Summary tool in the Defense Acquisition Information Management Retrieval System. Reporting will begin in the first quarter following the Milestone A decision approval and will continue until Milestone B approval is granted for the program.

10.11. Major Automated Information System (MAIS) Statutory Reporting

10.11.1. Major Automated Information System (MAIS) Programs Required to Report

10.11.1.1. Major Automated Information System (MAIS) Programs versus Increments

10.11.1.2. Major Automated Information System (MAIS) Programs

10.11.1.3. Pre-Major Automated Information System (Pre-MAIS (now "Unbaselined MAIS"))Programs and Other Investments

10.11.1.4. Major Automated Information System (MAIS)/Major Defense Acquisition Program (MDAP) Section 817 Determination

10.11.1.5. Ending the Requirement to Report under Chapter 144A of title 10 United States Code; Close-out Reports

10.11.2. Major Automated Information System (MAIS) Annual Report (MAR)

10.11.2.1. Preparing the Major Automated Information System (MAIS) Annual Report (MAR)

10.11. Major Automated Information System (MAIS) Statutory Reporting

The FY07 National Defense Authorization Act (NDAA), Section 816, instituted a reporting regime requiring MAIS programs to submit annual and quarterly reports. This was codified in Chapter 144A of title 10, United States Code and has been amended several times.

Briefly, the statute defines dollar thresholds for Major Automated Information System (MAIS) programs and other investments required to report . A MAIS Annual Report (MAR) is due to Congress 45 days after submission of the President's Budget, and each quarter a MAIS Quarterly Report (MQR) is due to "a senior Department of Defense official responsible for a MAIS program," hereafter referred to as the Senior Official.

The Senior Official responsible for a program is:

- The Service Acquisition Executive (SAE) for a program acquired by a Military Department (Army, Navy, or Air Force).
- The Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) for a program acquired by a DoD Component.

The statute also describes reports that are due to the congressional defense committees if a Program Manager (PM) estimates a Significant or Critical Change and the Senior Official agrees. As shown in table 10.11.T1, below, Significant and Critical Changes can occur in performance, schedule, and/or cost.

Table 10.11.T1. Significant and Critical Changes

	Significant	Critical
Cost - total acquisition - total life-cycle	15-25% increase	25% increase
Schedule	>6 month - 1 year delay	1 year delay
		Failed to achieve FDD within 5 years after the MS A decision or the date when the preferred alternative was selected and approved by the MDA. (See 10.11.5.2)
Performance	Significant adverse change in expected performance.	Undermines the ability of the system to perform mission as originally intended (i.e., did not meet a KPP threshold)
Report to congressional defense committees	Notification due 45 days after the MQR was due in the office of Senior Official	Program Evaluation and Report due 60 days after the MQR was due in the office of Senior Official

If a Significant Change to a program is determined by the Senior Official, the requirement to send the congressional defense committees a Notification within 45 days is triggered. Determination of a Critical Change , however, will initiate the requirement to conduct an Evaluation of the program and send a Report (with certifications) to Congress within 60 days. If the Report is not submitted within the 60-day period, appropriated funds may not be obligated for any major contract under the program. This prohibition ends on the day on which the congressional defense committees receive a report in compliance with the statute.

For additional information please see the Chapter 144A Key Documents and References. A complete copy of this DAG implementation guidance is also available there.

10.11.1. Major Automated Information System (MAIS) Programs Required to Report

Chapter 144A of title 10 United States Code requires annual and quarterly reports for each MAIS program and each other major information technology investment program for which funds are requested by the President in the budget.

10.11.1.1. Major Automated Information System (MAIS) Programs versus Increments

In the Defense acquisition context the terms "Program" and "Increment" refer to the management structure of the acquisition effort. Information System (IS) acquisitions require a short cycle time, so the Increment has become the basic unit for management of an Information System (IS) acquisition.

Increment -the Increment is "a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained. Each Increment must have an Acquisition Program Baseline (APB) with its own set of threshold and objective values set by the user." (DODI 5000.02, Encl.2, 2.c.) In the context of an IS acquisition, this means that both threshold and objective values for cost, schedule, and performance parameters must be established for each Increment.

Program -the term "Program" in the IS context will refer to the summation of a succession of Increments, and is a consolidation of acquisition efforts that is useful for Planning, Programming, Budgeting, and Execution System purposes. An IS "Program" does not have its own APB, rather each "Program" Increment has its own APB and is a separate acquisition program (as defined in DoDD 5000.01).

For a more complete discussion of Programs and Increments, see the AIS Acquisition Terms of Reference and Definitions .

10.11.1.2. Major Automated Information System (MAIS) Programs

A MAIS Program is defined in Chapter 144A of title 10 United States Code as "a Department of Defense acquisition program for an Automated Information System (either as a product or a service) that is either:

- "Designated by the Milestone Decision Authority (MDA) as a MAIS; or
- Estimated to exceed [one of the MAIS dollar thresholds]."

The MAIS threshold definition is statutory (per title 10 U.S.C. Chapter 144A) and explained in Table 1 of DoD Instruction 5000.02 :

- $32 million in fiscal year (FY) 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred in any single fiscal year; or
- $126 million in FY 2000 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or
- $378 million in FY 2000 constant dollars for all expenditures, for all increments,

regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system.

As a footnote to Table 1, AIS is defined as "a system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. Excluded are computer resources, both hardware and software, that are:

- an integral part of a weapon or weapon system;
- used for highly sensitive classified programs (as determined by the Secretary of Defense);
- used for other highly sensitive information technology programs (as determined by the DoD Chief Information Officer); or
- determined by the USD(AT&L) or designee to be better overseen as a non-AIS program (e.g., a program with a low ratio of RDT&E funding to total program acquisition costs or that requires significant hardware development)."

10.11.1.3. Pre-Major Automated Information System (Pre-MAIS (now "Unbaselined MAIS")) Programs and Other Investments

Chapter 144A of title 10 United States Code extends coverage of the reporting requirements to pre-MAIS Programs and other investments in Automated Information System (AIS).

- A Pre-MAIS program is defined as "an investment that is designated by the Secretary of Defense, or a designee of the Secretary, as a pre-Major Automated Information System' or 'pre-MAIS' program." Pre-MAIS designations are made by the Under Secretary of Defense (Acquisition, Technology, and Logistics (USD(AT&L)). The Department will also consider that an "investment" exists at Milestone A or when the preferred alternative is approved by the Milestone Decision Authority. Despite historic and statutory references to "pre-MAIS," the acquisition community prefers the term "unbaselined MAIS" as it is more descriptive of the programs acquisition status. Chapter 144A requirements will apply, whether the statutory or preferred term is used. See the AIS Acquisition Terms of Reference and Definitions .
- The reporting requirements also apply to "any other investment in [AIS] products or services that is expected to exceed the [MAIS thresholds] but is not considered to be a [MAIS] program because a formal acquisition decision has not yet been made with respect to such investment."

10.11.1.4. Major Automated Information System (MAIS)/Major Defense Acquisition Program (MDAP) Section 817 Determination

Section 817 of the Fiscal Year 2010 National Defense Authorization Act amended

Section 2445d of title 10 U.S.C . giving the Secretary of Defense authority to designate a program that both meets the definition of a MAIS and meets or exceeds the cost threshold for an MDAP, to be treated only as a MAIS or only as an MDAP.

Section 817 provides that as a general rule:

- A program that requires the development of customized hardware shall be treated only as an MDAP under chapter 144 of title 10 United States Code , and
- A program that does not require the development of customized hardware shall be treated only as a MAIS program under chapter 144A of title 10 United States Code.

While these criteria will be employed as a general rule, other factors will also be considered in determining whether to designate a program a MAIS or an MDAP, and will be applied on a case-by-case basis.

10.11.1.5. Ending the Requirement to Report under Chapter 144A of title 10 United States Code ; Close-out Reports

Many reasons exist to suggest the need for a program to report under Chapter 144A should not arise or has come to an end. The Under Secretary of Defense (Acquisition, Technology, and Logistics) or his designee will make this determination based on consideration of the facts, including:

- The program does not or no longer meets the definitions presented above in 10.11.1.2 ;
- The program has been terminated*; or
- The program has achieved full deployment (FD)**.

For programs determined to no longer require Chapter 144A reporting, a "close-out" Major Automated Information System (MAIS) Annual Report must be completed and submitted to Congress during the next reporting cycle. Similarly, a "close-out" MAIS Quarterly Report must be completed and submitted to the Senior Official when it is next due. Close-out reports should articulate one of the three circumstances above and cite an existing authoritative document (signed by an appropriate authority) as support. If subsequent increments of a program survive, note their existence in the Program Description of close-out reports.

NOTES:

* Terminating an Increment does not cause a Critical Change to be determined. Programs being terminated, however, must comply with Section 806 of P.L. 109-163 (FY06 NDAA). This statute requires the Secretary of Defense to notify the congressional defense committees not less than 60 days before cancelling (or significantly reducing the scope of) a MAIS program that is already post-Milestone C or has been fielded.

** Full Deployment is achieved according to the terms of an Acquisition Decision Memorandum (ADM) which documents a Full Deployment Decision (FDD). The FDD ADM should:

- Define FD in sufficient detail so that it can be reasonably determined when FD has occurred.
- Define FD Objective and Threshold dates. Following the FDD ADM approval, the Program Manager should submit a new Original Estimate using the Defense Acquisition Management Information Retrieval tool updating ONLY the FD TBD date with the FD Objective date from the ADM. (See page 21 of the DAMIR MAR Users Guide for instructions to update the FD Date.)
- Identify the acquisition organization that is responsible to declare (in writing) when FD has occurred.

10.11.2. Major Automated Information System (MAIS) Annual Report (MAR)

Chapter 144A of title 10 United States Code requires the Secretary of Defense to "submit to Congress each calendar year, not later than 45 days after the President submits to Congress the budget justification documents regarding cost, schedule and performance for each [Program Required to Report] for which funds are requested by the President in the budget." DoD meets this requirement by preparing for each program a report called the MAIS Annual Report (MAR). The MAR should be unclassified. If the required information is classified, then the classified data is replaced with the word "CLASSIFIED."

10.11.2.1. Preparing the Major Automated Information System (MAIS) Annual Report (MAR)

The MAR is prepared using the Defense Acquisition Management Information Retrieval (DAMIR) tool. A separate MAR for each Increment is prepared by the Program Manager and consists of the following sections: Program Information, Points of Contact, Program Description, Business Case, Program Status, Schedule, Performance Characteristics, and Cost. Do not report Increments that have submitted a close-out MAR. The DAMIR MAR Users Guide explain how to prepare the report.

10.11.2.2. Submitting the Major Automated Information System (MAIS) Annual Report (MAR)

Program Managers should submit the MAR via the Defense Acquisition Management Information Retrieval (DAMIR) tool to the DoD Component Acquisition Executive (CAE) (or equivalent official). The CAE's designated representative will then release the unclassified reports through the established DAMIR hierarchy.

Components will submit Final Draft reports as detailed above for Office of Secretary of Defense (OSD)-level review and coordination by the second Friday of January each year. The Office of the Under Secretary of Defense (Acquisition, Technology, and

Logistics) (OUSD(AT&L)) will coordinate the OSD-level review and provide feedback to the Components through issue resolution teleconferences held during the second week of February.

Components will release a Final MAR not later than the last Friday in February. OUSD(AT&L) will prepare and coordinate transmittal letter and release (via DAMIR) the final MARs to Congress no later than 45 days after submission of the President's Budget (normally the first Monday in February). Table 10.11.2.2.T1 describes a typical reporting cycle.

Table 10.11.2.2.T1. Review Cycle Events and Typical Target Dates

Event	Responsible Party	Typical Target Date
Train the Component Trainers	OUSD(AT&L)	Nov 15
Task Components for MAR cycle	OUSD(AT&L)	Dec 10
Submit final Draft MARs	Components	Jan 15
Review and consolidate feedback to the OSD acquisition analyst	OSD staff	Feb 5
OSD/Component issue resolution teleconferences	OSD & Components	Feb 10
Release Final MARs to OSD	Components	Feb 25
Hold final OSD MAR Reviews	OUSD(AT&L)	Mar 2
Coordinate MAR package within OSD	OUSD(AT&L)	Mar 3-Mar 10
Staff MAR package to USD(AT&L) for signature	OUSD(AT&L)	Mar 12
Sign MAR transmittal letters	USD(AT&L)	Mar 18
Deliver MAR "transmittal" letters to Congress; release MARs via DAMIR	OUSD(AT&L)	Mar 20

10.11.3. Major Automated Information System (MAIS) Quarterly Report (MQR)

Chapter 144A of title 10 United States Code requires the Program Manager to submit a written MQR to the Senior Official that identifies any variance from the projected schedule, cost, or key performance parameters as baselined in the Major Automated Information System (MAIS) Annual Report (MAR). All Programs Required to Report , once having submitted a MAR, will submit MQRs even if they have not experienced any variance from their cost, schedule or performance baseline.

10.11.3.1. Reporting Cycle: Major Automated Information System (MAIS) Quarterly Report (MQR)

Although a separate report, the MQRs follow the Defense Acquisition Executive

Summary (DAES) submission cycle and bear the same date as the program's DAES. The Component Acquisition Executives representative should release the MQRs (via the Defense Acquisition Management Information Retrieval tool) to the Senior Official (and to the OSD Lead) on the last business day of every third month, maintaining the DAES group reporting rotation . The OSD Lead may review MQRs to assist Components in compliance with Chapter 144A of title 10 United States Code and this guidance.

10.11.3.2. Major Automated Information System (MAIS) Quarterly Report (MQR) Form and Contents

The Defense Acquisition Management Information Retrieval (DAMIR) tool will adapt the most recent MAR or MQR (if MQR is more recent than the MAR) to create each new MQR. Instructions for the MQR can be found in the DAMIR MQR Users Guide .

The Program Manager should update information that has changed and summarize any program variances not previously reported in an MQR in the Program Status section.

The "Current Estimate or Actual" columns for each of the cost, schedule, and performance factors should be updated to reflect the Current Estimate on the as-of-date of the MQR.

10.11.3.3. Major Automated Information System (MAIS) Program Manager's Current Estimate

The Program Manager's (PMs) Current Estimate is the latest estimate of program acquisition cost, schedule milestone dates, and performance characteristic values of the approved program (i.e., the approved program as reflected in the currently approved Acquisition Program Baseline, Acquisition Decision Memorandum, or in any other document containing a more current decision of the Milestone Decision Authority or other approval authority).

- For cost, the current estimate is normally the President's budget plus or minus fact of life changes.
- For schedule, the Current Estimate is normally the PMs best estimate of current schedule milestone dates.
- For performance, it is normally the PM's best estimate of current performance characteristic values.

10.11.3.4. Major Automated Information System (MAIS) Quarterly Report (MQR) Anticipation and Receipt

Program Managers (PMs) are responsible for reporting the execution status of their programs to their acquisition management chain: Program Executive Officer, Component Acquisition Executive, Milestone Decision Authority, and-for Chapter 144A Quarterly Reports purposes-the Senior Official. If a PM becomes aware the program will

experience a variance exceeding a Significant or Critical Change threshold, the PM should immediately notify his/her acquisition management chain, in advance of the due date for the next MQR. Since the MQR is the vehicle for official notification of Significant and Critical changes, the 45- or 60-day deadlines for reporting to Congress are established from the date the MQR is due to the office of the Senior Official, i.e., the last business day of the month the MQR is due.

- If determination of a Significant Change is contemplated, the deadline for Notification to Congress is the last business day before 45 days expire.
- If determination of a Critical Change is contemplated, the deadline for conducting a program evaluation and certifying a report of results to Congress is the last business day before 60 days expire.

10.11.3.5. Determinations by the Senior Official

The (staff office of a) Senior Official should 1) promptly review a Major Automated Information System (MAIS) Quarterly Report (MQR) to see whether it reflects a less than "significant" (or no) variance, a "Significant Change," or a "Critical Change" in cost, schedule or performance and, 2) each month promptly provide the MQR to the Senior Official. Senior Officials may choose to obtain independent opinions on the measurement of a variance and proper determination of a Change.

If none of the reported factors exhibit a variance exceeding a Significant Change threshold , nothing further needs to be done to satisfy the statute.

If a cost, schedule, or performance factor exhibit's a variance exceeding a Significant or Critical Change threshold , the Senior Official makes such determination, and proceeds to satisfy the statutory requirements. Model processes for Significant Changes and Critical Changes are suggested below.

10.11.4. Significant Changes

10.11.4.1. Significant Change Thresholds

10.11.4.2. Model Significant Change Process

10.11.4.3. Coordination and Transmittal of a Significant Change Notification to Congress

10.11.4. Significant Changes

If, based on the MAIS Quarterly Report (MQR) , the Senior Official makes a determination that a Significant Change has occurred, he or she must notify the congressional defense committees in writing of that determination not later than 45 days after the MQR was due.

10.11.4.1. Significant Change Thresholds

A Significant Change is defined as one in which one of the following has occurred:

- There has been a schedule change that will cause a delay of more than 6 months but less than a year in any program schedule milestone or significant event from the schedule submitted as the Original Estimate;
- The estimated total acquisition cost or total life-cycle cost for the program has increased by at least 15 percent, but less than 25 percent, over the Original Estimate, or
- There has been a significant, adverse change in the expected performance from the parameters submitted in the original MAR. The Department, however, has determined that a "significant, adverse change" is defined as a failure to meet a Key Performance Parameter (KPP) threshold value, which is the same definition chosen for a Critical Change in performance (addressed below). Therefore, all such failures will be determined to be Critical Changes .

10.11.4.2. Model Significant Change Process

When a Significant Change is determined, the Senior Official must notify the congressional defense committees in writing that he or she has made such Determination. The Notification should be in the form of a one-to-two page letter signed by the Senior Official and is due to the congressional defense committees not later than 45 days after the date the MAIS Quarterly Report (MQR) was due in the office of the Senior Official.

The Notification should acknowledge that a Significant Change, as defined by the statute, has occurred. Succinctly state the specific factor that has varied in excess of a threshold, the reasons for the variance, and indicate what actions (including reprogramming) the PM has taken or may take to bring the program back within the Original Estimate parameters or to avoid further deviation from the Original Estimate. If known, indicate the projected new cost or schedule.

If a Notification has been sent informing the congressional defense committees of a Significant Change in one element (for example, Milestone C date), and that elements variance has expanded (but not exceeded a Critical Change criteria) in a subsequent MQR, no additional Notification need be sent to the congressional defense committees. If, however, a subsequent MQR indicates that a different reporting element has an over-threshold variance, another Notification must be sent informing the congressional defense committees of this additional basis for a Determination of Significant Change. When one Significant Change is identified, a prudent Program Manager will examine the entire program for other Significant Changes and report them all in a single Notification letter. One schedule element slip, for example, is likely to cause subsequent elements to slip.

10.11.4.3. Coordination and Transmittal of a Significant Change Notification to Congress

Notifications are drafted by Program Managers and coordinated with their respective Program Executive Officers and Component Acquisition Executives (CAE) for signature by the Senior Official. The Notification must be coordinated with the Under Secretary of Defense (Acquisition, Technology, and Logistics), the Deputy Chief Management Officer, or the DoD Chief Information Officer, as appropriate before sending to Congress. Copies of Notifications should be sent to the cognizant Overarching Integrated Product Team (OIPT) Leader before transmittal to Congress. Example Significant Change Notifications are available.

10.11.5. Critical Changes

10.11.5.1. Critical Change Thresholds

10.11.5.2. Five-Year-to-Full Deployment Decision (FDD) Threshold

10.11.5.2.1. Failed to Achieve a Full Deployment Decision (FDD)

10.11.5.2.2. Five-Year Development Clock Start Date/Stop Date

10.11.5.2.3. Full Deployment Decision (FDD) Date

10.11.5.3. Program Evaluation to Inform a Critical Change Report

10.11.5.4. Report on Critical Program Changes

10.11.5.5. Model Critical Change Process

10.11.5.5.1. Critical Change Triage Team; Determination and Tasking

10.11.5.5.2. Critical Change Team (CCT) and Meetings

10.11.5.5.3. Critical Change Integrated Product Teams (IPT) Membership and Focus

10.11.5.5.4. Critical Change Process Calendar

10.11.5.5.5. Critical Change Report (CCR)

10.11.5.6. Coordination and Transmittal of a Critical Change Report (CCR) to the Congressional Defense Committees

10.11.5. Critical Changes

When the Senior Official anticipates or makes a determination that a Critical Change has occurred, the Senior Official should initiate a process to satisfy the statutory and regulatory requirements. This section describes those requirements and sets forth a model process.

10.11.5.1. Critical Change Thresholds

A Critical Change is defined as one in which any of the following has occurred:

- The system failed to achieve a full deployment decision (FDD) within 5 years after the Milestone A decision or if no Milestone A then the date when the preferred alternative was selected and approved by the Milestone Decision Authority (this threshold is more fully explained in section 10.11.5.2, below);
- There has been a schedule change that will cause a delay of one year or more in any program milestone or significant event from the schedule originally submitted to Congress in the Major Automated Information System (MAIS) Annual Report (MAR);
- The estimated total acquisition cost or total life-cycle cost for the program has increased by 25 percent or more over the Original Estimate submitted to Congress in the MAR; or
- There has been a change in the expected performance of the MAIS that will undermine the ability of the system to perform the functions anticipated at the time information on the program was originally submitted to Congress in the MAR. The Department has determined that a critical performance change is defined as a failure to meet a Key Performance Parameter threshold value.

10.11.5.2. Five-Year-to-Full Deployment Decision (FDD) Threshold

Major Automated Information System (MAIS) programs should be structured so that each Increment can achieve an FDD within five years from the Milestone A decision, or if there was no Milestone A decision, the date when the preferred alternative was selected and approved by the Milestone Decision Authority. The program structure and (upon sufficient maturity) the criteria that constitute a FDD, should be reflected in the Increments Acquisition Strategy and Acquisition Program Baseline.

10.11.5.2.1. Failed to Achieve a Full Deployment Decision (FDD)

The phrase "failed to achieve" is interpreted literally; i.e., the Increment must have actually exceeded (not expected to exceed) five years between start of the 5-year development clock and FDD. A breach of this threshold will therefore be reported in the Major Automated Information System (MAIS) Quarterly Report (MQR) next due after the 5-year point.

If, however, any other Critical Change is reported in advance of the 5-year point and it is

expected that FDD will not occur within the 5-year threshold, include an additional determination of the 5-year-to-FDD breach in the evaluation and report to Congress. When the 5-year point arrives, re-send the same report to Congress with a transmittal letter indicating that "the previously reported certifications were meant to apply now."

If there is no reason to determine and report any Critical Change in advance of failure to achieve FDD within 5 years, such determination, evaluation, report, and certification will be accomplished after the 5-year point is reached in accordance with the first paragraph of this section.

For Acquisition Category III programs that are graduating to MAIS status and have achieved an FDD (no matter how long it took), that event has overcome the 5-year-to-FDD breach criterion, and it is no longer applicable. Graduating programs carry their program history with them (including the date the 5-year development clock was started).

10.11.5.2.2. Five-Year Development Clock Start/Stop Dates

The 5-year development clock starts when the automated information system or information technology investment is granted Milestone A approval for the program, or if there was no Milestone A decision, the date when the preferred alternative is approved by the Milestone Decision Authority (excluding any time during which program activity is delayed as a result of a bid protest).

Because schedule events and thresholds are expressed in whole months, the additional time to be added as a consequence of bid protest is calculated by dividing the bid protest time lost in days by 30 and rounding up to the next month. For example, if a bid protest was filed on October 26, 2011 and resolved on December 20, 2011 (53 days), the 5-year development clock would be extended two months (53/30=1.76 and rounded up to 2 months).

10.11.5.2.3. Full Deployment Decision (FDD) Date

With respect to a MAIS program, the Full Deployment Decision is the final decision made by the Milestone Decision Authority (MDA) authorizing an Increment of the program to deploy software for operational use. Each Increment can have only one FDD. The 5-year development clock stops when the MDA signs the FDD Acquisition Decision Memorandum.

If the Increment will have multiple partial deployments, the MDA should specifically designate which partial deployment decision will serve as the FDD for the entire Increment. At the MDAs discretion and as specified in the Acquisition Strategy, a partial deployment would be appropriately designated as the FDD with an accumulation of successes related to the entire Increment, such as:

- Low percentage of total functionality remains to be developed;

- IOT&E indicates that the system is operationally effective, suitable, and survivable;
- High percentage of capability fielded;
- High percent of geographical fielding completed;
- High percentage of legacy system(s) replaced;
- Insignificant risk associated with remaining releases ; and
- Achievement of Initial Operational Capability.

If the MDA has not formally specified which partial deployment will serve as the FDD, by default, the last partial deployment will be the FDD.

10.11.5.3. Program Evaluation to Inform a Critical Change Report

Upon determination of a Critical Change, the statute directs an evaluation ("E") of the program, including "an assessment of-

- (E1) "the projected cost and schedule for completing the program if current requirements are not modified;
- (E2) "the projected cost and schedule for completing the program based on reasonable modification of such requirements; and
- (E3) "the rough order of magnitude of the cost and schedule for any reasonable alternative system or capability."

While not *per se* a part of the Critical Change Report that will be submitted to the congressional defense committees, these three "E" assessments will feed into the four certification ("C") areas of the Critical Change Report described below.

10.11.5.4. Report on Critical Program Changes

The statute further directs delivery of a report (i.e., Critical Change Report (CCR)) to the congressional defense committees, including: "a written certification (with supporting explanation) stating that-

- (C1) "the automated information system or information technology investment to be acquired under the program is essential to the national security or to the efficient management of the Department of Defense;
- (C2) "there is no alternative to the system or information technology investment which will provide equal or greater capability at less cost;
- (C3) "the new estimates of the costs, schedule, and performance parameters with respect to the program and system or information technology investment, as applicable, have been determined, with the concurrence of the Director of Cost Assessment and Program Evaluation, to be reasonable; and
- (C4) "the management structure for the program is adequate to manage and control program costs."

To avoid a prohibition on the obligation of funds for major contracts, the report must be

submitted to the congressional defense committees not later than 60 days after the date the Major Automated Information System (MAIS) Quarterly Report (MQR) was due to the staff office of the Senior Official.

10.11.5.5. Model Critical Change Process

10.11.5.5.1. Critical Change Triage Team; Determination and Tasking

In anticipation of, or upon receipt of a Major Automated Information System Quarterly Report (MQR) containing notice of a Critical Change, the staff office of the Senior Official should organize a Triage Meeting to:

- Review the nature and severity of the Change;
- Recommend a tailored Critical Change process to the Senior Official; and
- Outline the leadership structure and scope of the Critical Change Team (CCT) that will conduct the evaluation and prepare a Critical Change Report (CCR). See below for further advice on organizing the CCT and its several Integrated Product Teams (IPTs).

For Acquisition Category (ACAT) IAM programs, Triage Meeting attendees should be senior representatives from 1) the staff office of the Senior Official, 2) the office of the Joint Chiefs of Staff (J8,Force Structure Resources and Assessment), 3) the office of the Deputy Director, Program Evaluation (plus the office of the Deputy Director Cost Analysis if the Under Secretary (Acquisition, Technology and Logistics) is the Milestone Decision Authority), 4) the office of the Director, Acquisition Resources & Analysis, and 5) the OSD office with program oversight responsibility (Overarching Integrated Product Team, Investment Review Board, or equivalent).

For ACAT IAC programs, Triage Meeting attendees should be from analogous Component organizations.

The staff office will document the recommendations of the Triage Meeting in a draft Determination and Tasking memorandum to be signed by the Senior Official. The "Determination and Tasking" memorandum will:

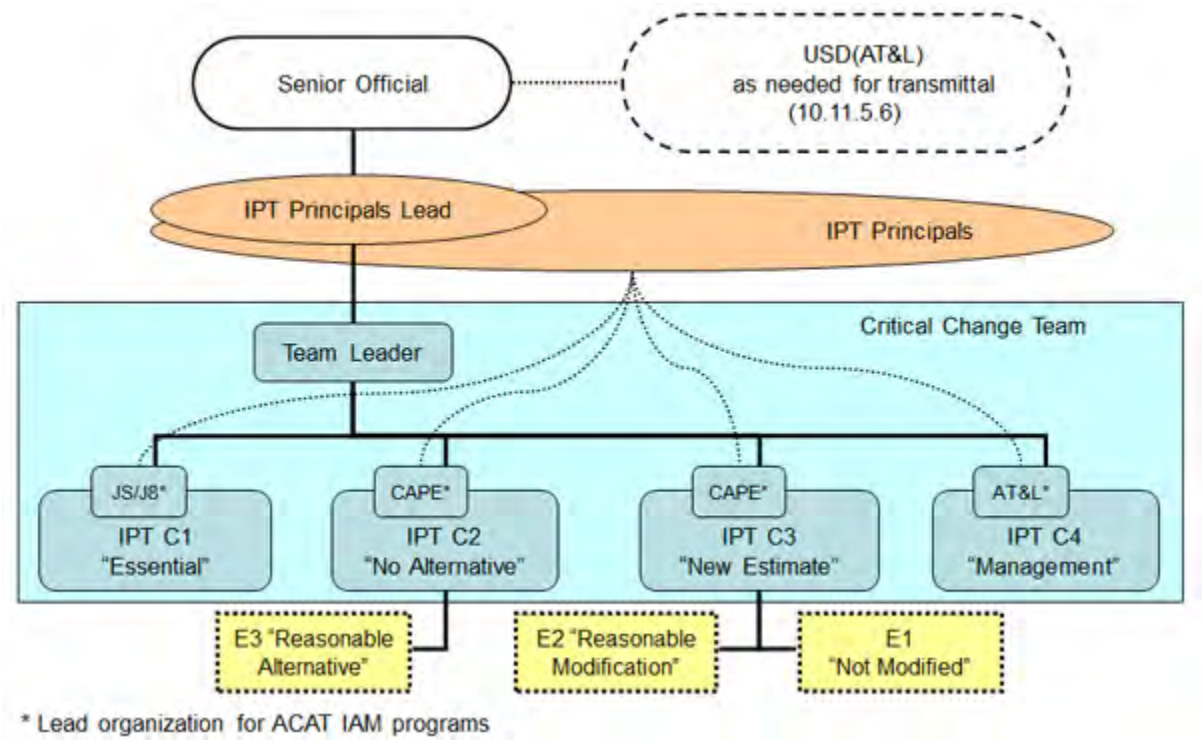
- State the Senior Official's determination and nature of the Critical Change;
- Direct a program evaluation be conducted;
- Direct a report of the results be prepared; and
- Designate leadership of a Critical Change Team to manage the process.

10.11.5.5.2. Critical Change Team (CCT) and Meetings

As part of the "Determination and Tasking" memorandum, the Senior Official should establish leadership for a CCT to conduct the program evaluation and produce the Critical Change Report. A Team Leader from an appropriate oversight or program integration office under the Senior Official will organize the CCT and integrate the

contributions of the several IPTs. The Team Leader should be an O-5/O-6 or equivalent civilian. If the magnitude of the program warrants it, a Flag/General Officer/Senior Executive Service-level "Integrated Product Team (IPT) Principals Lead" from the Senior Official's staff should be named to provide advice and direction to the CCT, as well as to chair meetings of a committee of "IPT Principals." Figure 10.11.5.5.2.F1. is a notional depiction of CCT Organization and Reporting Paths.

Figure 10.11.5.5.2.F1. Critical Change Team (CCT) Organization and Reporting Path



Ultimately, the Senior Official must be satisfied sufficiently with the evaluation and report to sign the certification statements required by the statute. When the Senior Official perceives the need to specify leadership or membership of individual IPTs, that specification should also be made as part of the "Determination and Tasking" memorandum. Otherwise, the IPT Principals Lead and Team Leader will select individual members and leadership of the IPTs that will focus on certifications C1-4. Membership should include all interested parties, and individuals must be empowered to represent their organizations. In all cases, IPT membership and leadership designations should consider joint/departmental interests as well as the circumstances of the Critical Change.

A kickoff meeting of the CCT should be held as soon as possible in anticipation of a Critical Change being determined. The IPT Principals Lead and CCT Leader should guide the organization of the CCT into IPTs and specify expected contributions and a detailed timeline. The CCT (or the Team Leader alone) should meet again with the IPT

Principals Lead as necessary, and at least once for a mid-process progress check. Eventually, the CCT should meet to pre-brief the IPT Principals Lead on the final Report. The final Report and briefing should then be presented to the IPT Principals for a final review of the Report before delivery to the Senior Official for certification (signature).

10.11.5.5.3. Critical Change Integrated Product Teams (IPT) Membership and Focus

The Critical Change process should be conducted by IPTs under the Critical Change Team (CCT), each focused on Certifications 1-4 . To preserve IPT and CCT independence to the maximum extent practicable, team membership should be independent of the Program Management Office (PMO). IPT membership should be selected to maximize the success of the group and avoid non-productive contributions. For Acquisition Category (ACAT) IAM programs, IPT membership is suggested below. For ACAT IAC programs, the IPT membership representatives should be from analogous Component organizations plus the appropriate OSD organizations.

- IPT C1 will document the explanation that permit's the Senior Official to certify "the automated information system or information technology investment to be acquired under the program is essential to the national security or to the efficient management of the Department of Defense." The IPT C1 should write a few paragraphs about the need for the program:
    - Include threat, mission, and current systems available to meet the threat or efficient management need.
    - Reference relevant strategy documents, Concept of Operations (CONOPS), roadmaps, requirements documents, threat assessments, Quadrennial Defense Review, etc.
    - Address the program and the capability to be acquired, as appropriate.
    - *IPT C1 members* : Component operations staff, Program Executive Officer (PEO) staff, Component Acquisition Executive (CAE) staff, user representatives, Program Manager (PM), Joint Chiefs of Staff (JCS)/J8, Office of the Secretary of Defense (OSD) (Principal Staff Assistant (PSA) and the Overarching Integrated Product Team (OIPT) acquisition analysts).
- IPT C2 will document the explanation that permit's the Senior Official to certify that "there is no alternative to the system or information technology investment which will provide equal or greater capability at less cost." This IPT should:
    - Reference any existing Analysis of Alternatives (AoA) and discuss any major deviations from past analysis. Do not re-accomplish the AoA.
    - Identify any alternative systems.
    - Include the assessment (E3) of the "rough order of magnitude of the cost and schedule for any reasonable alternative system or capability."
    - *IPT C2 members* : Component operations staff, user representatives, Component & program office cost estimators, PM, CAE and PEO staff; JCS/J8; OSD (PSA; Office of the Deputy Director, Program Evaluation;

and OIPT acquisition analyst).

- As indicated in Figure 10.11.5.5.2.F1 , above, IPT C3 is responsible for assessing E1 and E2, forming conclusions thereupon, and recording an explanatory statement that permit's the Senior Official to certify "the new estimates of costs, schedule, and performance parameters with respect to the program and system or information technology investment, as applicable, have been determined, with the concurrence of the Director of Cost Assessment and Program Evaluation (D, CAPE), to be reasonable." This IPT should:
    - Identify changes that have occurred to the program's requirements.
    - Summarize acquisition and total life-cycle cost growth from the Original Estimate. Display changes in constant (BY) and current (TY) dollars.
    - Include rationale for growth such as technical uncertainties/corrections or changes in inflation, requirements, escalation outlay, quantity, schedule, budget, or estimating errors.
    - Include the assessment (E1) about the "projected cost and schedule for completing the program if current requirements are not modified."
    - Include the assessment (E2) about "projected cost and schedule for completing the program based on reasonable modification of ... requirements."
    - Update the cost estimate and milestone schedule
    - Develop a draft Acquisition Program Baseline for management approval concurrent with the Critical Change Report. The Original Estimate status is explained in 10.11.7.1.
    - IMPORTANT: In addition to concurrence, an independent cost estimate by D, CAPE) may also be required. See 10.11.7.2 and 10.5.1. Independent Cost Estimates for further explanation.
    - *IPT C3 members:* Component operations staff, user representatives, Component & program office cost estimators, PM, CAE and PEO staff; JCS/J8; OSD (PSA; Office of the Deputy Director, Cost Assessment; OIPT acquisition analyst).
- IPT C4 will document the explanation that permit's the Senior Official to certify "the management structure for the program is adequate to manage and control program costs." The IPT C4 should:
    - Review PMO and contractor management structures.
    - Conduct site visit's if the IPT Principal Lead determines they would be useful.
    - Re-examine recent program oversight reviews and recommendations to appraise the degree and success of implementation.
    - Develop a draft Acquisition Decision Memorandum for the MDA to direct corrective actions.
    - *IPT C4 members* : CAE and PEO staff; PM; OSD (Office of the Assistant Secretary of Defense (Research and Engineering) (ASD(R&E)); Offices of the Deputy ASD (Developmental Test & Evaluation) and the Deputy ASD (Systems Engineering), Office of the Director, Defense Procurement and Acquisition Policy, Office of the DoD Chief Information Officer; and the

OIPT acquisition analyst).

Table **10.11.5.5.3.T1** summarizes recommended IPT membership.

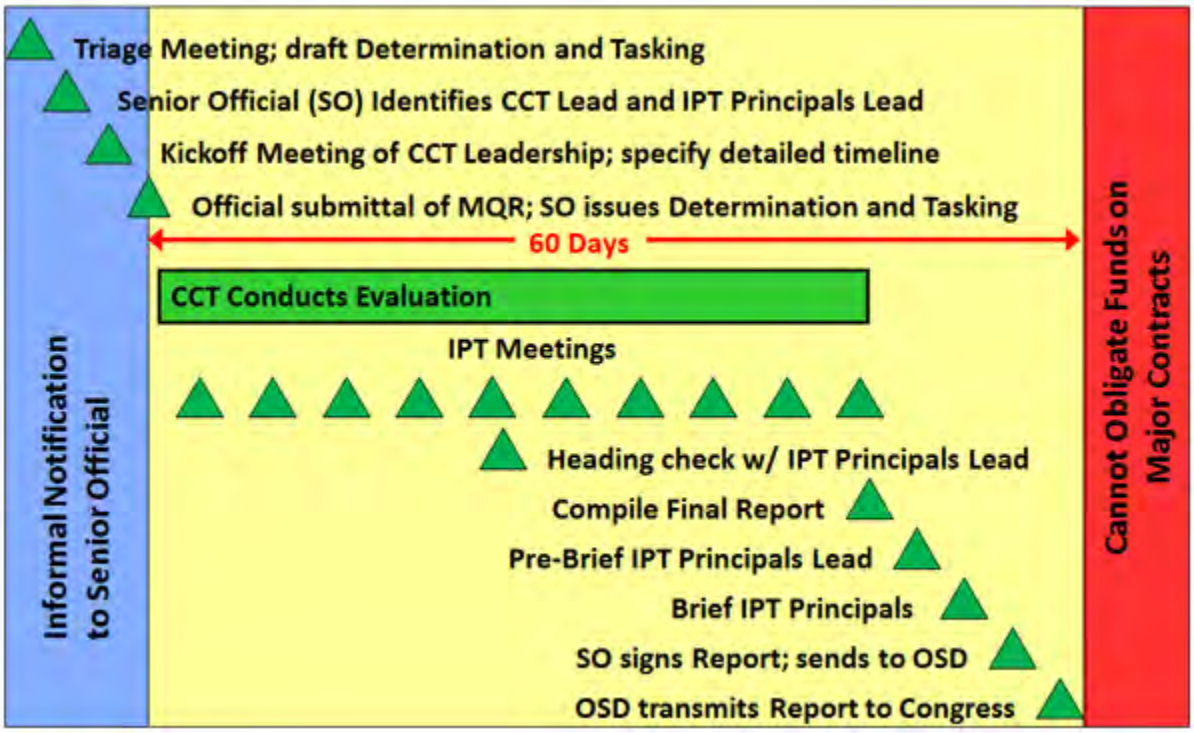
Table 10.11.5.5.3.T1. Summary of Recommended IPT Membership

IPT	C1	C2	C3	C4
Organization	**essential**	**no alternative**	**new estimate**	**management**
PMO/PM (as required)	X	X	X	X
PMO Cost/Finance		X	X	
PEO Staff		X	X	X
CAE Staff	X	X	X	X
Component Operations Staff	X	X	X	
User Representatives	X	X	X	
JCS/J8	X	X	X	
OSD Acquisition Analyst	X	X	X	X
DASD(SE)				X
DASD(DT&E)				X
AT&L(DPAP)				X
OSD CAPE		X	X	
OSD PSA	X	X	X	X
DoD CIO				X

10.11.5.5.4. Critical Change Process Calendar

Figure 10.11.5.5.4.F1 **.** portrays a typical Critical Change process calendar and shows the general flow of events described in 10.11.5.5.

Figure 10.11.5.5.4.F1. Critical Change Process Calendar



10.11.5.5.5. Critical Change Report (CCR)

The Critical Change Report is envisioned to be a document of about six pages: a two-page letter offering a succinct introduction/background on the program and the events that led to the Critical Change that contains the required certifications and one page each for the explanations provided by the Integrated Product Teams (IPTs) C1-4. The IPT C1-4 sections include an outline of corrective actions that will be taken to add discipline to program execution and avoid repeated deviation from the new Original Estimate. Example CCRs are available.

In most cases, an Acquisition Decision Memorandum and Acquisition Program Baseline will also be required to direct the actions cited in the CCR.

In case of an audit, it is important for the Component to keep all records used to prepare the CCR.

10.11.5.6. Coordination and Transmittal of a Critical Change Report (CCR) to the Congressional Defense Committees

In accordance with section 2445c(d)(1)(B) of title 10, United States Code , CCRs must be sent "through the Secretary of Defense, to the congressional defense committees." In cases where the Senior Official is an individual within OSD, this will be inherent in the

CCR coordination and signature process.

In cases where the Senior Official is not an individual within OSD, the CCR shall be signed by the Senior Official and provided to the cognizant OSD official for transmittal to Congress. The signed CCR should be provided to the appropriate OSD official with draft Transmittal Letters addressed to the congressional defense committees no later than 5 working days before expiration of the 60-day period.

10.11.6. Restrictions on Obligation of Funds

If the Senior Official determines a Critical Change has been reported by a program and a Critical Change Report (CCR) is not submitted to the congressional defense committees within the 60-day period, "Appropriated funds may not be obligated for any major contract under the program." For Chapter 144A purposes, the term "major contract" is defined as any contract under the program that is not a firm-fixed price contract whose target cost exceeds $17M (FY00 constant dollars); or if no contract exceeds $17M (FY00 constant dollars), then the largest contract under the program.

Program Managers should not obligate funds for a major contract during the period in which the CCR is being prepared.

The prohibition on the obligation of funds will cease to apply on the date on which the congressional defense committees have received a report in compliance with Chapter 144A requirements.

10.11.7. Revision of the Original Estimate

According to Chapter 144A of title 10 United States Code , a Critical Change is the only opportunity to update the Original Estimate contained in the Major Automated Information System (MAIS) Annual Report (MAR): "an adjustment or revision of the Original Estimate or information originally submitted on a program may be treated as the Original Estimate or information initially submitted on the program if the adjustment or revision is the result of a Critical Change."

10.11.7.1. Status of the Critical Change Report (CCR) Estimate

The new estimates of cost, schedule, and performance parameters included in a CCR will be the basis for a revised Original Estimate in the Major Automated Information System (MAIS) Annual Report (MAR) and the MAIS Quarterly Report (MQR), and inform the continuing management of the program. An Acquisition Decision Memorandum and an Acquisition Program Baseline (APB) should therefore be coordinated concurrently with the CCR to direct the actions responsive to the CCR. Failing to get concurrent signatures, the Program Manager (PM) should make approval of an updated APB a high priority.

Once the CCR has been sent to Congress and before the next MQR is prepared, the Program Manager should submit the new cost, schedule, and performance parameters as an updated MAR Original Estimate using the Defense Acquisition Management Information Retrieval (DAMIR) tool (see the DAMIR MAR Users Guide , and call the DAMIR Hot Line for assistance). Subsequent MQRs will commence reporting variances from the revised Original Estimate .

10.11.7.2. Independent Cost Estimates

The Weapon Systems Acquisition Reform Act of 2009 (P.L. 111-23, May 22, 2009), codified at section 2334(a)(6)) of title 10 United States Code , requires the Director, Cost Assessment and Program Evaluation (D, CAPE) to conduct an Independent Cost Estimate (ICE) in the case of a Major Automated Information System (MAIS) Critical Change if the Milestone Decision Authority (MDA) is the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L); and at any other time considered appropriate by the Director or upon the request of the USD(AT&L).

Additionally, DTM 11-009 , Acquisition Policy for Defense Business Systems (DBS), June 23, 2011, requires the D, CAPE to conduct an ICE for all DBS MAIS reporting a Critical Change if the MDA is the USD(AT&L), the Deputy Chief Management Officer, or the Department of Defense Chief Information Officer. If the MDA is delegated after incurrence of a Critical Change, an ICE is still required.

If a D, CAPE ICE was conducted, great weight should be given to the resulting estimate derived from that effort as it is likely to possess the accuracy desired for publication in the Acquisition Program Baseline.

10.11.7.3. Base Year Conversion

The Base Year of an Original Estimate (as reported in the Major Automated Information System (MAIS) Annual Report (MAR) and MAIS Quarterly Report) may be updated without going through a Critical Change process, provided that the proper conversion factors have been applied. Such a conversion should be footnoted in those reports through submittal of the next MAR. The conversion calculations should be retained as a

Memorandum for the Record in the program files.

10.11.8. Sources for Additional Information

Chapter 144A Key Documents and References includes:

- Defense Acquisition Guidebook 10.11 - MAIS Statutory Reporting
- DAMIR MAR Users Guide
- DAMIR MQR Users Guide
- Section 811 FY07 NDAA - Time-Certain Development for Defense Business Systems
- Automated Information System Acquisition Terms of Reference and Definitions
- Chapter 144A of title 10 United States Code (annotated)
- MAIS Annual Report Program Analysts and Principal Staff Representatives
- Chapter 144A Overview Briefing

10.12. Defense Acquisition Executive Summary (DAES) Process

The purpose of the DAES is to provide a venue to identify and address, as early as possible, potential and actual program issues which may impact the Department of Defenses (DoD's) on-time and on-schedule delivery of promised capabilities to the

warfighter. The DAES is not just a report; it is a process that includes;

1. Submission of program status and assessment information by the Program Manager of each Major Defense Acquisition Program (MDAP) and Major Automated Information System (MAIS) for which the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is the Milestone Decision Authority;
2. Independent assessments of each program by Office of the Secretary of Defense (OSD) and Joint Staff stakeholders; and
3. A monthly DAES meeting.

The goal of the DAES process is to facilitate communication between, and provide feedback to, key stakeholders in OSD, the Joint Staff, the Components, and Program Offices. It is important to note that the DAES is an internal management system meant to fulfill the needs of senior Department of Defense executives and is NOT for general public consumption. Unlike the Selected Acquisition Report information, DAES information is considered to be For Official Use Only and is not releasable outside the department without prior approval from the Director, Acquisition and Resource Analyses.

The DAES process enables the USD(AT&L) to fulfill statutory requirements to manage and oversee MDAPs and MAIS programs. Additionally, it establishes a mechanism for the Department to meet the Unit Cost Reporting requirement of section 2433, Chapter 144 of title 10, United States Code . Access to the data reported through the DAES also enables the Director of Performance Assessments and Root Cause Analyses to fulfill statutory requirements to perform program assessments as directed by the Weapon Systems Acquisition Reform Act of 2009 (Section 103 Public Law 111-23).

10.12.1. Defense Acquisition Executive Summary (DAES) Reporting Requirements

The DAES process for a program begins when the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) designates the program as a DAES reporting program and the Office of the USD(AT&L), specifically the Office of the Director, Acquisition Resources and Analyses (ARA), assigns it to a quarterly reporting group (A, B, or C). Most DAES reporting programs are ACAT ID or IC programs and full DAES reporting usually begins at program initiation (typically Milestone B) and after the program has submitted its initial Selected Acquisition Report (SAR).

With the exception of contract/earned value information, DAES information is only required to be submitted on a quarterly basis. Contract/earned value information is required to be submitted on a monthly basis. Whether or not it has changed from the previous submission, all required information must be submitted at a minimum each quarter (or month for contract/earned value information). The month in which a program is required to submit is determined by its DAES Group. Table **10.12.1.T1** below shows the yearly calendar for all three groups. It is important to note that the DAES process overlaps; each DAES Group is at a different stage of the process during any given

month. For example, the Group A DAES submitted by the PM at the end of January is assessed by OSD in February and the corresponding DAES meeting is held in March.

Table 10.12.1.T1. DAES Group Schedules

Month	PM Prepares and Submits DAES (NLT Last Working Day of Month)	Submissions Available to OSD (First Working Day of Month)	OSD Assessments Due (8th Working Day of Month)	DAES Meeting (3rd Week of Month)
Jan	**Group A**	**Group C**	**Group C**	**Group B**
Feb	**Group B**	**Group A**	**Group A**	**Group C**
Mar	**Group C**	**Group B**	**Group B**	**Group A**
Apr	**Group A**	**Group C**	**Group C**	**Group B**
May	**Group B**	**Group A**	**Group A**	**Group C**
Jun	**Group C**	**Group B**	**Group B**	**Group A**
Jul	**Group A**	**Group C**	**Group C**	**Group B**
Aug	**Group B**	**Group A**	**Group A**	**Group C**
Sep	**Group C**	**Group B**	**Group B**	**Group A**
Oct	**Group A**	**Group C**	**Group C**	**Group B**
Nov	**Group B**	**Group A**	**Group A**	**Group C**
Dec	**Group C**	**Group B**	**Group B**	**Group A**

10.12.1.1. Duration of Defense Acquisition Executive Summary (DAES) Reporting

Once DAES reporting is initiated, it continues until the program is 90% or more delivered through the production phase (or 90% expended, if RDT&E only), at which time a program will begin submitting only a Unit Cost Report (UCR) DAES pursuant to section 2433 of title 10, United States Code that is supplemented by Sustainment information.

DAES reporting may be terminated for a program when it is 90% delivered or expended and the final SAR has been submitted. The official list of active DAES reporting programs is maintained by the Office of the Director, ARA and is available via the Defense Acquisition Management Information Retrieval (DAMIR) system.

10.12.1.2. Defense Acquisition Executive Summary (DAES) Submission Process

The DoD Components submit the DAES information to DAMIR in accordance with the prescribed monthly or quarterly submission cycle. DAES submissions are due to OSD on the last working day of the month. The required information consists of both the

electronic DAES information and supplemental Microsoft Office Power Point charts.

DAES information must be submitted to the Defense Acquisition Management Information Retrieval (DAMIR) system in the prescribed format. Most program offices will enter the DAES information into one of the Service acquisition information management systems (i.e., Army AIM, Air Force SMART, or Navy Dashboard) and the Services will electronically submit the information to the DAMIR system via web services. Alternatively, programs without the capability to submit electronically via web services may obtain permission from the Office of the Director, Acquisition Resources and Analyses and their Component leadership to enter the data directly into the DAMIR system.

The supplemental Power Point charts are sent to the Component who then e-mails them to DAMIR@osd.mil . The DAMIR team loads the charts into the DAMIR Acquisition Documents where they are visible to any DAMIR user with DAES access to the program. As the DAMIR system is the mechanism that OSD uses to view and assess the programs, it is highly recommended that each program office access DAMIR and validate that all information and supplemental charts were correctly submitted.

10.12.1.3. Defense Acquisition Executive Summary (DAES) Content

The content of a DAES submission is dependent on where a program is in the Acquisition lifecycle. See Table **10.12.1.3 .T1** below for a summary of the required information. Detailed instructions on what is required in each section can be found in the Defense Acquisition Management Information Retrieval system.

Table 10.12.1.3 .T1. DAES/Web Services Information Requirements

Information	Program Initiation-75%	> 75%	Minimum Update Frequency
Program Information	-	-	Quarterly
Points of Contact	-	-	Quarterly
APB Dates	Calculated		Quarterly
Mission & Description	-	-	Quarterly
Executive Summary	-		Quarterly
Threshold Breaches	Calculated		Quarterly
PM Assessments	-		Quarterly
Schedule	-		Quarterly
Performance	-		Quarterly
Track to Budget	-		Quarterly
Cost & Funding	-	-	Quarterly
Low Rate Initial Production	-		Quarterly
Foreign Military Sales	-		Quarterly
Nuclear Costs	-		Quarterly

Information	Program Initiation-75%	> 75%	Minimum Update Frequency
Unit Cost	Calculated		Quarterly
Contracts/Earned Value	-		Monthly
Deliveries & Expenditures	-		Quarterly
Operating & Support Costs	-	-	Quarterly
Sustainment	-	-	Quarterly
Risk Summary Chart (Power Point)	-		Quarterly
Issue Summary Chart (Power Point)	-		Quarterly

10.12.1.4. Consistency of Defense Acquisition Executive Summary (DAES) Data

The DAES information submitted should be the Program Managers assessment of the program and be consistent with the Acquisition Program Baseline (APB) , President's Budget (PB), Acquisition Decision Memorandums (ADMs) and other official program guidance. The Program Manager is responsible for both ensuring the accuracy, completeness and consistency of the information, and for elevating risks and other issues that may require managerial attention.

10.12.1.5. Office of the Secretary of Defense (OSD) Defense Acquisition Executive Summary (DAES) Assessment Process

Once the DAES information is submitted to the Defense Acquisition Management Information Retrieval (DAMIR) system by the Department of Defense Components, OSD and Joint Staff stakeholders have 8 working days to perform an assessment of the status of each program in the current DAES group that is less than 75% complete. The purpose of the OSD assessment process is to ensure routine surveillance of Major Defense Acquisition Programs by the OSD and Joint Staff stakeholders and to identify risks and issues that require managerial attention.

The OSD and Joint Staff stakeholders collectively evaluate each program in 10 different categories. A green/yellow/red rating and an associated narrative is provided for each category rated by an individual stakeholder. The categories evaluated by OSD are identical to the categories evaluated by the Program Offices. The OSD assessments provide an independent assessment of program execution status and are used when selecting programs to be briefed at the DAES meeting. Detailed instructions on completing a DAES assessment can be found in the DAMIR Acquisition Documents.

Table 10.12.1.5.T1 below shows which OSD and Joint Staff stakeholders have primary responsibility for each indicator; however, any stakeholder may evaluate any category.

Table 10.12.1.5.T1 List of Assessment Indicators

Assessment Indicator	Rating Organization(s)
Cost	ARA/AM, CAPE, DCMA, OIPT Lead
Schedule	OIPT Lead
Performance	OIPT Lead, ASD(R&E)/SE, Joint Staff
Funding	ARA/RA, USD(C)
Test	OT&E, ASD(R&E)/DT&E
Sustainment	L&MR, P&R
Management	OIPT Lead
Contracts	DPAP, IC
Interoperability	OIPT Lead
Production	MIBP
International	International Cooperation

10.12.1.6. Defense Acquisition Executive Summary (DAES) Data Quality Assessment

In addition to the program assessment process performed by the Office of the Secretary of Defense (OSD) and Joint Staff stakeholders, the Office of the Director, ARA/Acquisition Visibility (AV) concurrently performs a data quality assessment of the submitted information. All information is reviewed for availability, currency, and consistency. Non-compliance with reporting requirements is reported to the Components and requires the immediate correction and re-submittal of information.

10.12.1.7. Defense Acquisition Executive Summary (DAES) Senior Meeting Forum

The Principal Deputy Under Secretary of Defense (Acquisition, Technology, and Logistics) (PDUSD(AT&L)) conducts a monthly DAES meeting. The purpose of the meeting is to provide a senior forum in which to surface problems requiring managerial attention with the intent of achieving early and effective resolution.

It is typically a two-hour meeting scheduled for the third week of the month. Attendance is tightly controlled.

10.12.1.7.1 Defense Acquisition Executive Summary (DAES) Agenda Selection

Once the Office of the Secretary of Defense (OSD) assessments have been submitted, the DAES meeting agenda selection process begins. The Director, Acquisition Resources and Analyses (ARA) chairs a DAES Program Selection meeting on approximately the 15 th working day of the month at which the Overarching Integrated Product Team Leaders and the Director, Program Assessment and Root Cause Analysis are responsible for recommending programs and/or issues for review at the

monthly DAES meetings.

The criteria for nomination vary from month to month, but nominations normally fall within one of the following categories:

- Program Briefs. This is the most typical agenda item. Programs may be selected due to specific issues that requires management attention or as a good news story. Program assessments are just one factor used to determine if a program should be recommended, as all knowledge of the program is considered when making the selection. Program Briefs are typically presented by the Program Manager.
- Single Issue Program Updates. These are condensed briefings that normally focus on a previously identified issue where a short status update is required. Single Issue Program Updates are typically given by the OSD staff.
- Program Executive Officer (PEO) Portfolio Briefs. A PEO portfolio brief may be recommended in conjunction with a specific Program Brief or independent of a specific Program Brief. Briefings requested independent of a specific program brief are typically due to a systemic issue affecting multiple programs within the portfolio. PEO Portfolio Briefs are typically presented by the PEO.

Typically, 3 or 4 programs or issues are selected for the agenda each month. Normally, programs that are within 90 days (before or after) of a Defense Acquisition Board review are excluded from consideration. Once the agenda selection is finalized, the Office of the Director, ARA publishes the agenda and schedule.

10.12.1.7.2. Defense Acquisition Executive Summary (DAES) Briefings, Minutes, and Action Items

Templates for the Program Briefings can be found in the Acquisition Documents section of the Defense Acquisition Management Information Retrieval system. Primary focus areas of the briefings should be: contract and Acquisition Program Baseline compliance status, closure plans for known issues, risk management/mitigation of potential issues, and Better Buying Power initiatives (to include should cost).

The Program Briefing charts are due to the Office of the Director, Acquisition Resources and Analyses (ARA) no later than 6 working days prior to the scheduled date of the DAES meeting.

In addition to the selected program or issue briefings, the Office of the Director, ARA provides summaries of the Program Manager assessments and the OSD and Joint Staff assessments for each selected program as well as an update on any outstanding actions from previous DAES meetings. A data quality assessment update is also provided by the Office of the Director, ARA/Acquisition Visibility. Other systemic issues are briefed as required or directed by the Principal Deputy Under Secretary of Defense (Acquisition, Technology, and Logistics) (PDUSD(AT&L)).

Within 5 working days of the DAES meeting, the Office of the Director, ARA submits the DAES meeting minutes, including any action items, to the PDUSD(AT&L) for approval. Once approved, the meeting minutes are posted in the DAMIR Acquisition Documents. The Office of the Director, ARA is responsible for tracking DAES action items to completion.

10.13. Acquisition Visibility

In 2007, the Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) started an initiative to achieve Acquisition Visibility (AV) within the Department of Defense (DoD). AV is defined as having timely access to accurate, authoritative, and reliable information supporting acquisition oversight, accountability, and decision making throughout the Department for effective and efficient delivery of warfighter capabilities. AV began as a concept in early 2008 with a demonstration of data governance and Service Oriented Architecture to support major weapons system decision-making.

Five years later, the technology framework and governance process has solidified, providing the Defense Acquisition Community with a capability that supports management of Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. It is a capability that:

- Captures acquisition data from the Military Departments and the Office of the Secretary of Defense (OSD);
- Federates that data through a single interface; and
- Publishes this information through web-services where a customer can access the appropriate information for his or her reporting or tracking requirements.

Currently, over 180 data elements are used to provide acquisition system information that is compartmentalized into seven major categories: earned value management, unit cost, budget, milestones, sustainment, science and technology, and program administration. AV is now entering into a phased-production environment and working to increase the number of data elements (totaling approximately 500) available to the AV capability which will bring additional, relevant data to our decision makers.

AV continues to mature in providing a range of value-added data services supporting acquisition management and oversight. Objectives are to:

- Expand the use and functionality of AV Capabilities;
- Automate data quality validation and verification processes;
- Align technically to the strategic goals of the DoD's Chief Information Officer;
- Provide additional program coverage;
- Provide an acquisition documentation repository; and
- Encompass a range of relevant data sets to support acquisition management and oversight.

Questions regarding the AV project should be directed to the Office of Enterprise Integration and OSD Studies (within the Office of the Director, Acquisition Resources and Analysis).

10.13.1. Defense Acquisition Management Information Retrieval (DAMIR)

The Defense Acquisition Management Information Retrieval (DAMIR) system creates a net-centric environment to provide data transparency of acquisition management information to the Department of Defense. DAMIR provides:

- Full web-services data exchange with Components' acquisition information systems for Defense Acquisition Executive Summary (DAES) information and Program/Budget Review (P/BR) (formerly known as the Program Objective Memorandum (POM)) information;
- web applications that allow Components to input Selected Acquisition Report (SAR), Acquisition Program Baseline (APB), Major Automated Information System (MAIS) Annual Report (MAR), and the DAES data, making DAMIR the authoritative source for the SAR, APB, and MAR information;
- Analytical tools that enable users to customize the way they search, view, and display previously unavailable combinations of information electronically; and
- Workflow and collaboration capabilities.

Based upon an Office of the Secretary of Defense enterprise decision, use of the DAMIR system is mandatory for all Major Defense Acquisition Programs (MDAPs) and all MAIS programs and must be employed to satisfy statutory requirements for SAR and MAR submissions and the APB. Non-MDAP and non-MAIS programs may also use the system.

The Director, Acquisition Resources and Analysis, has responsibility for the development, upgrade, and maintenance of the DAMIR system. The DAMIR system includes instructions for preparing the APB, the SAR, the MAR, the DAES, the Unit Cost Report, and the P/BR submission (referred to in the DAMIR system as POM), including administrative procedures. User help can be obtained through the following sources:

- DAMIR public web site (www.acq.osd.mil/damir)
- DAMIR hotline (703-679-5345)

DAMIR mailboxes (damir@caci.com for technical and functional support or damir@osd.mil for account administration support)

10.13.1.1. Defense Acquisition Management Information Retrieval (DAMIR) Acquisition Program Baselines (APBs)

The DAMIR system is the authoritative source for all APBs. APBs for Acquisition Category (ACAT) I and IA programs must be created and released using the DAMIR system. The DAMIR system provides the data entry capability and required workflow to create and edit an APB. An APB is approved within the DAMIR system when a formal signature page with the Milestone Decision Authority's signature is acquired--at this point, the APB can no longer be edited. The APB Objectives and Thresholds will also be visible within both the Selected Acquisition Report and Defense Acquisition Summary (DAES) views in the DAMIR Purview Program View module. The full Web Services data exchange with the Components acquisition information systems: Army (Acquisition Information Management), Navy (Dashboard), and Air Force (System Metric and Reporting Tool) also allows the Components to pull the official APBs into their respective systems to use in their respective DAES processes.

10.13.1.2. Defense Acquisition Management Information Retrieval (DAMIR) Selected Acquisition Reports (SARs)

The DAMIR system is the authoritative source for SARs and provides the data entry capability and required workflow to create and edit a SAR. The computational model capability is also integrated into the DAMIR SAR module. DAMIR provides extensive data checks, ensuring that a SAR is not released to Congress with critical errors. [**NOTE:** Acquisition Program Baseline (APB) values are pulled from the APB module and cannot be edited within the SAR.] All Major Defense Acquisition Programs are required to use DAMIR to prepare the annual and quarterly SARs. Hard copy SARs are no longer submitted to Congress. Instead, Congress is granted access to the SAR information through DAMIR. The only exception is when the SAR contains classified

information. In those few cases, a hard-copy classified annex is submitted.

10.13.1.3. Defense Acquisition Management Information Retrieval (DAMIR) Major Automated Information System (MAIS) Annual Reports (MARs)

The DAMIR system is the authoritative source for MARs and provides the data entry capability and required workflow to create and edit a MAR. All MAIS programs are required to use the DAMIR system to prepare the annual MARs. The DAMIR MAR Module supports both Baselined and Unbaselined MAIS programs. The DAMIR system provides extensive data checks, ensuring that a MAR is not released to Congress with critical errors. Historical MARs (December 2008 December 2010) will be stored in PDF format in DAMIR *Acquisition Documents* .

For Baselined MARs, a MAR Original Estimate (OE) module is provided; the MAR OE will be automatically pulled into the MAR by the DAMIR system. The MAR OE can be initialized from the APB. Hard copy MARs are no longer submitted to Congress. Instead, Congress is granted access to the MAR information through the DAMIR system.

10.13.1.4. Defense Acquisition Management Information Retrieval (DAMIR) Defense Acquisition Executive Summary (DAES)

To improve information sharing and to reduce duplicate data entry, DAES information is now obtained either via Web Services data exchange between the Components' acquisition information systems and the DAMIR system or directly via the DAMIR *Create or Edit DAES Report* module. Major Automated Information System programs that are not Component-specific must enter all DAES information directly into the DAMIR system. (The action in the data exchange between the DAMIR system and the Component systems is referred to as a push; DAES data is pushed to the DAMIR system via Web Services on a monthly/quarterly basis.) DAES information is required to be submitted for all Acquisition Category (ACAT) I and IA programs using one of the previously mentioned collection methods.

Acquisition Program Baseline (APB) values displayed in the DAES/Web Services view are pulled directly from the APB module and cannot be updated via web services. In addition to the Currently Approved APB Objectives and Thresholds, for reference only, the DAMIR DAES submission will also show the Initial Phase Objectives and Thresholds, if applicable.

Office of the Secretary of Defense (OSD) Assessments against the quarterly pushed Program Managers Assessments are created in the DAMIR *DAES Review* module. Each organization has the ability to rate a program on any of the eleven indicators. OSD Assessments are visible in the DAMIR system the month after the Program Managers assessments are submitted.

Two unclassified supplemental Microsoft Word Power Point briefing slides (Issues

Summary and Risk Summary.) must be submitted with the quarterly DAES submission. For those programs selected to be on the monthly DAES Meeting Agenda, an additional eleven slides must also be submitted. The list of thirteen (total) required slides is:

1. Program Information
2. Overview
3. Issues/Help Needed
4. Schedule
5. Cost and Quantity
6. Quad Chart
7. Earned Value
8. Risk Summary
9. Interrelationships, dependencies, and Synchronization with Complementary Systems
10. Sustainment
11. Better Buying Power
12. International Program Aspects
13. O&M and O&S Crosswalk Chart

When received, these slides are loaded into the DAMIR *Acquisition Document* module by the DAMIR administrative support staff. Access to DAES information is based on approved permissions.

10.13.1.5. Defense Acquisition Management Information Retrieval (DAMIR) Ad hoc Reports

The DAMIR *Ad hoc Report* s module provides a capability for cross-program analysis. Access to completed reports is permission based, but all users have access to SARs and SAR Ad hoc reports.

Users may request a report, or a query, of the DAMIR system database by sending an e-mail message to damir@osd.mil . Results from report requests will be added to the long-standing Ad hoc report list; results from queries are a one-time data dump into an excel spreadsheet and will not be turned into an ad hoc report unless specifically requested.

10.13.1.6 Defense Acquisition Management Information Retrieval (DAMIR) Portfolio View

The DAMIR *Portfolio View* module provides a cross-program analytical capability much like that of the DAMIR *Ad hoc Reports* module with the addition of graphical representations of the data. The DAMIR system software presents both dashboard and detailed views of Selected Acquisition Report data or Defense Acquisition Executive Summary data in the form of tables, charts, and graphs. The data presented in these views is based on portfolios of identified programs. The DAMIR system supports several standard portfolios that are accessible to all users. The standard portfolios allow the

user to view data for all programs or for only those programs related to a specific Component. Users are also able to create personal portfolios that reference only specific programs that they identify. Any of these portfolios may then be used to create the portfolio views relevant to these programs. The DAMIR *Portfolio View* module also allows the user to customize their dashboard views uniquely, so that the user is presented with only those charts and graphs which are most useful to their inquiry. The ability to see draft and unofficial information is permission-based.

10.13.1.7. Integrated Program/Budget Review Data Submissions

During the first phase in the annual budget cycle, the Office of the Director, Cost Assessment and Program Evaluation (D, CAPE) and the Office of the Under Secretary of Defense (Comptroller) (USD(C)) are responsible for conducting an annual Integrated Program/Budget Review (P/BR) on all Department of Defense (DoD) resources and require an annual Integrated Program/Budget data submission from all DoD Components.

The Components are also required to submit supplemental Program/Budget Review (P/BR) data on their Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. This supplemental submission of MDAP and MAIS data supports the efforts of the MDAP transparency study initially directed in the Fiscal Year 2011 Integrated Program Review Resource Management Directive 700 study and provides the details necessary to assess the status of programs.

Data shall be submitted for all current MDAPs and MAIS programs, as well as acquisition program concepts and Unbaselined MAIS programs that will achieve Milestone B prior to the end of the calendar year, or have been certified under the provisions of section 2366a of title 10 United States Code . The MDAP and MAIS program data shall include all acquisition costs (RDT&E, Procurement, MILCON, Acquisition O&M, Working Capital Funds, or Other Financing with an explanation) and MDAP quantities (RDT&E and Procurement) for the full acquisition cycle of each MDAP and each MAIS program (by fiscal year and funding appropriation). For MAIS programs, the total life-cycle cost is the development cost plus ten years of Operation and Support (O&S) costs following Full Deployment declaration. For MDAP programs, the full acquisition lifecycle and associated funding is defined by the D, CAPE and USD(C) annual Integrated Program/Budget Submission Guidance.

All MDAPs and MAIS programs shall submit annual P/BR data that has been coordinated with and approved by the appropriate Component Acquisition Executive (CAE) into their Components acquisition information system. For efficient information sharing, the CAE systems shall publish P/BR data to Acquisition Visibility (AV) using the Defense Acquisition Management Information Retrieval (DAMIR) system Web Services. Components without access to one of the Component acquisition information systems shall use the DAMIR *Create or Edit a Budget Report* module. Notwithstanding the method of transmission, exposure, or publication, the CAE-approved P/BR data shall be

available for consumption by AV and AV subscribers as determined by annual guidance.

All MDAPs shall submit P/BR data at the sub-program level and all MAIS programs shall submit at the increment level as appropriate, consistent with the Track-to-Budget rules established for the data submission to the Program Resources Collection Process (PRCP), per the program/budget transparency requirements of the Fiscal Year Integrated Program/Budget Submission Guidance.

MDAPs and MAIS programs whose schedules have changed due to funding and quantity changes in the P/BR submission shall report estimated program schedule changes. A limited number of large MDAP and MAIS programs may be required to provide P/BR revision data periodically during the Integrated P/BR. For programs so designated, revisions driven by the MDAP Issue Review Team or by any other direction shall cover the same data included with the original transmission and will be maintained by the responsible Component.

Components shall also review their acquisition program budgets, and ensure RDT&E Program Element funding is reflected in the RDT&E budget activity that aligns with the program's acquisition phase as defined in DoD Instruction 5000.02.

10.14. Special Interest Programs

10.14.1. Major Defense Acquisition Program (MDAP) or Special Interest Programs

10.14.2. Major Automated Information System (MAIS) or Special Interest Programs

10.14. Special Interest Programs

A program, or a technology project that will result in a program, has special interest if it has one or more of the following factors: technological complexity; Congressional interest; a large commitment of resources; the program is critical to achievement of a capability or set of capabilities; the program is part of a system of systems; or the program is a joint program. Generally, the level of funding, desired oversight and reporting will determine the Milestone Decision Authority and whether or not the program is designated a "Special Interest" program.

Programs that already meet the dollar thresholds for a Major Defense Acquisition Program (MDAP) may not be designated Special Interest programs.

10.14.1. Major Defense Acquisition Program (MDAP) or Special Interest Programs

If a program meets one of the MDAP dollar thresholds (per section 2430 of title 10, United States Code), then the program is automatically an MDAP. If the program is below the dollar threshold for designation as an MDAP, the Defense Acquisition

Executive (DAE) may still choose to designate the program an MDAP if he or she deems oversight with statutory reporting is needed. An MDAP is designated ACAT I and it's oversight comes from the DAE. The DAE can either retain MDA or delegate it to a Component Head or Component Acquisition Executive (CAE). If the DAE retains MDA, the program is an ACAT ID program. If the DAE delegates MDA to the Component Head or CAE, then the program is an ACAT IC program. As an MDAP, the program must meet all statutory reporting requirements for MDAP programs.

If the DAE desires oversight of a program that falls below MDAP dollar thresholds, and deems that statutory reporting associated with MDAPs is not needed, the program is designated a Special Interest Program. If the DAE retains MDA, the program is an ACAT ID Special Interest program. If the DAE delegates MDA to the Component Head or CAE, then the program is an ACAT IC Special Interest program. The CAE may also designate programs that are ACAT II or below as CAE Special Interest Programs.

For such Special Interest programs, the reporting requirements are tailored to meet the specific oversight needs and must be captured in an Acquisition Decision Memorandum.

Table 10.14.1.T1 MDAP & Special Interest Designations & Decision Authorities

MDAP and Special Interest Designations & Decision Authorities			
Designation	**MDA**	**Funding Level**	**Information & Reporting**
ACAT ID MDAP	DAE	MDAP	MDAP
ACAT IC MDAP	CAE	MDAP	MDAP
ACAT ID Special Interest	DAE	Less than MDAP	Less or equal to MDAP
ACAT IC Special Interest	CAE	Less than MDAP	Less or equal to MDAP

10.14.2. Major Automated Information System (MAIS) or Special Interest Programs

If an Automated Information System (AIS) program meets one of the dollar thresholds for it to be designated a MAIS, then the program is automatically a MAIS program. If an Acquisition Information System (AIS) program falls below the MAIS dollar thresholds, the Defense Acquisition Executive (DAE) may still designate the program a MAIS program if he or she deems that oversight with statutory reporting is needed. A MAIS program is designated ACAT IA and the Milestone Decision Authority (MDA) is the Defense Acquisition Executive (DAE) or the person within OSD to whom the DAE delegates MDA. If the MDA remains within OSD (with the DAE or delegated MDA within OSD), the program is an ACAT IAM program. If MDA is delegated to the Component Head or CAE, then the program is an ACAT IAC program. A MAIS program must meet

all statutory reporting requirements for MAIS programs.

If the DAE desires oversight of an AIS program, but deems that the statutory reporting associated with MAIS programs is not needed, the program is designated a "Special Interest" program. If MDA remains within OSD (DAE or DAE delegated MDA within OSD), the program is an ACAT IAM Special Interest program. If MDA is delegated by the DAE to the Component Head or CAE, then the program is an ACAT IAC Special Interest program.

For such Special Interest programs, the reporting requirements are tailored to meet the specific oversight needs and must be captured in an Acquisition Decision Memorandum.

Table 10.14.2.T1 MAIS & Special Interest Designations & Decision Authorities

MAIS and Special Interest Designations and Decision Authorities			
Designation	MDA	Funding Level	Information & Reporting
ACAT IA MAIS	DAE or OSD	MAIS	MAIS
ACAT IAC MAIS	CAE	MAIS	MAIS
ACAT IAM Special Interest	DAE or OSD	Less than MAIS	Less or equal to MAIS
ACAT IAC Special Interest	CAE	Less than MAIS	Less or equal to MAIS

10.15. Relationship of Affordability and Should-Cost

For product development programs, some understandable confusion exists as to how to implement both affordability as a requirement and should-cost, particularly early in a programs life cycle before Engineering and Manufacturing Development and Production. The two are compatible, but must be balanced differently across the product life cycle. The emphasis, prior to Milestone B approval for a program, should be on

defining and achieving affordability targets. Past that point, the emphasis shifts to defining and achieving should-cost estimates.

10.15.1. Affordability as a Requirement

Affordability as a requirement directs that we establish quantified goals for unit production cost and sustainment coasts for our products, driven by what the Department or Component can afford to pay. These goals should be set early and used to drive design trades and choices about affordable priorities.

The Milestone Decision Authority (MDA) considers affordability at all major decision points of an acquisition program. In part, this consideration ensures that sufficient resources (funding and manpower) are programmed and budgeted to execute the program acquisition strategy. The MDA also examines the realism of projected funding over the programming period and beyond, given likely DoD Component resource constraints.

10.15.1.1. Affordability Analysis

Affordability Analysis is based upon the budgets we expect to have for the product over its life cycle and provides a design constraint on the product we will build, procure, and sustain. When the Department, i.e., the Milestone Decision Authority (MDA), establishes the affordability requirement, it represents a metric that captures the products expected capability against its expected (affordable) life cycle cost. From this point on, any future unit or sustainment cost increase above those levels, whatever the cause, must come back to the MDA and to the user to determine what requirements can be dropped to stay within the affordability requirement, or-if the program must be terminated. For further discussion of affordability and affordability assessments, see 3.2 .

10.15.2. Should-Cost

Should-cost asks us consciously to do something different. It asks us to continuously fight to lower all of our costs, wherever that makes sense. Should-cost is a tool to manage all costs throughout the lifecycle, and it operates in parallel with the effort to constrain our requirements appetites in order to control the final product unit and sustainment costs. Should-cost is focused on controlling the cost of the actual work that we are doing and expect to do. In particular, should-cost estimates inform our negotiations with industry over contract costs and incentives. The should-cost approach challenges us to do our best to find specific ways to beat the Independent Cost Estimate (ICE) or Program Estimate (which should already reflect the affordability requirements) and other cost projections funded in our budgets (i.e., will-cost), when we find sensible opportunities to do so. For example, should-cost does not mean trading away the long-term value of sound design practices and disciplined engineering management for short-term gain.

Should-cost can be applied to anything that we do and to any source of costs, including

costs for services and internal government costs as well as contracted product costs. Should-cost targets are often stretch goals we expect our leaders to do their best to reach; we expect them to be based on real opportunities, but to be challenging to execute. Unlike affordability requirements, we do not expect them to always be achieved, but we do expect strong efforts to do so.

Should-cost and affordability can come into conflict early in programs, particularly before Milestone B, when an affordability requirement may have been defined based on expected budgets, but it is too early to define should-cost estimates for future production or sustainment of products because we have not yet defined the design. This is also the time when spending money on efforts to reduce future costs can have the biggest payoff. As a result, during the early stages of product development, the priority should be toward establishing affordability constraints and working to provide the enablers to achieve them in the ultimate design. In the early phases of programs, should-cost can still be constructively used to control program overhead and unproductive expenses and to generally reduce contracted development costs, but it should not keep us from making sound investments in product affordability. Prior to the pre-EMD Review or MS B, the ICE or Program Estimate for production and sustainment has not been finalized and any should-cost estimates for future production lots and sustainment would be premature. At that point, however, particularly if we are ready to ask for bids and negotiate low rate initial production prices, we need a should-cost estimate to inform negotiations. Once the requirements, design, and affordability goals are established and an CE or Program Estimate exists, then it is time to challenge the assumptions embedded in those analyses, formulate should-cost estimates for production and sustainment, and work to achieve those estimates.

10.15.2.1. Annual Should-Cost Progress Reporting

On April 22, 2011, the Under Secretary of Defense (Acquisition, Technology and Logistics) directed the Component Acquisition Executives to deliver an annual progress report on their Should-Cost implementation .

The annual report must list all Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs for which should-cost estimates have been established. It should describe the challenges and successes in implementing these initiatives for each program from the perspectives of the respective Program Executive Officers and Program Managers, especially with regard to the programs the Services selected as models for Should-Cost implementation. The report should also describe the incentive plans the Service/Component has developed for Program Managers to reinforce and reward commitment to the Will-Cost and Should-Cost Management process.

Additionally, each Component should submit a Should-Cost datasheet for each MDAP and MAIS program that has established a Should-Cost estimate. The datasheet template is to be used as a guide and may be tailored to better present relevant

information.

Questions regarding the annual Should-Cost Report may be directed to the Deputy Director, Resource Analysis in the Office of the Director, Acquisition Resources and Analysis.

10.15.2.2. Should-Cost Information for Defense Acquisition Board (DAB) Preparation

Information regarding the programs should-cost efforts must be included in material prepared for presentation to the Overarching Integrated Product Team (OIPT), the DAB Planning Meeting, the DAB Readiness Meeting, and the DAB Review. See the current Should-Cost Template for guidance.

10.16. Acquisition Program Transition Workshops (APTW)

General . Acquisition Program Transition Workshops (APTWs) are intended to provide timely and tailored assistance to Acquisition Category (ACAT) ID, ACAT IAM, and select special interest government program managers in aligning the government/contractor team at critical points in the programs schedule. APTWs are neither reviews nor assessments. They are to be conducted for the program manager on a non-judgmental basis with any findings, conclusions and recommendations provided to only the government and industry program managers. The APTW should enhance both the government and industry program managers capability to successfully anticipate and resolve commonplace challenges as well as unanticipated issues that may arise throughout program execution. Flowing from this effort, the Defense Acquisition University maintains a lessons-learned program for dissemination among all program teams to foster better program performance and increase the chance for successful program outcomes. As part of a governance effort, the offices of the Deputy Assistant Secretary of Defense (DASD) (Strategic & Tactical Systems), the DASD (Space & Intelligence), the DASD (Command, Control, Communications & Cyber), the Deputy Chief Management Officer, and the Service Military Deputies will collaborate on common threads and trends from completed APTWs, and adjust workshop content as required.

10.16.1. Acquisition Program Transition Workshop (APTW) Purpose and Objectives

The basic purpose, common goals, and common deliverables for the APTW process

are listed below.

Basic Purpose. To achieve early alignment of government & industry teams, particularly at the Integrated Product Team level and with a product orientation.

Common Goals.

- Common Interpretation of Contract Requirements/Provisions
- Understanding/Alignment of Government & Industry Processes
- Understanding/Agreement on Program Risk Elements
- Understanding/Agreement on Integrated Product Team (IPT) Structure, Concept of Operations, Authority

Common Deliverables.

- Integrated Baseline Review (IBR) Roadmap/Preliminary or Critical Design Review Roadmap (Major Goals)
- Agreement on Program Management Review Scope & Processes
- Joint Understanding of Program Scope & Configuration Management
- Resolution of Issues/Interpretation of Differences
- Commitment to Timely Communications and Transparency
- Actions Needing Further Consideration/Resolution

10.16.2. Acquisition Program Transition Workshop (APTW) Execution

It is strongly recommended that Program Managers of all Acquisition Category (ACAT) ID, ACAT IAM ,and special interest programs conduct an APTW with their Industry PM counterparts within the first few weeks following contract award or re-baseline action (such as those associated with Post Nunn-McCurdy certifications). Requests for workshops from other programs will be entertained as resources allow.

Program Managers should contact the Defense Acquisition University in a timely manner to facilitate the following planning and execution processes.

Draft Request for Proposal (RFP). As a DoDI 5000.02 defined Milestone or a major transition/restart is approached, information regarding APTWs should be included in the RFP and Statement of Work. Acquisition Category (ACAT) ID and ACAT IAM Program Managers should address APTWs in their Draft RFP briefings to possible respondents.

Pre-Contract Award. The period prior to source selection and contract award is a particularly useful time for the government Program Manager to engage in APTW government team training and/or process development for contract execution.

Post Contract Award. In the first few weeks following contract award, program managers should coordinate with the industry program manager counterpart on actions

that will result in a joint APTW within five weeks following contract award.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 11 -- Program Management Activities

11.0. Overview

11.0.1. Purpose

The purpose of this chapter is to describe and explain some of the activities and decisions available to and required of the program manager as he or she manages and executes the program.

11.0.2 Contents

Chapter 11 covers the following topics:

- Knowledge-Based Acquisition
- Technical Representatives at Contractor Facilities
- Contractor Councils
- Government Property in the Possession of Contractors
- Modeling and Simulation (M&S) Support to the Entire Product

Acquisition Additional information regarding Program Management can be found at the DAU Acquisition Community Connection website , the Program Management Community of Practice.

11.1. Joint Programs

There are two aspects of "jointness" to consider when discussing joint program management: the jointness of the capability and the jointness of the development and production of the system.

11.1.1. Identifying Joint Capabilities

As part of the Joint Capabilities Integration and Development System (JCIDS) , the Joint Staff J-8, with the assistance of the DoD Components, evaluates all JCIDS documents, regardless of Acquisition Category or previous delegation decisions to determine whether the proposal has joint force implications. The Joint Staff documents, CJCS Instruction 3170.01 and the JCIDS Manual , provide full detail and direction on this topic.

11.1.2. Joint Acquisition Management

Acquisitions that contribute to joint capabilities may be managed as joint acquisition programs. A "joint acquisition" is any acquisition system, subsystem, component, or technology program with a strategy that includes funding by more than one DoD Component during any phase of a systems life cycle. DoD Instruction 5000.02, Enclosure 10, paragraph 4 addresses DoD Component fiscal responsibilities associated with participation in programs under joint acquisition management.

11.1.2.1. Designation

Considering the recommendation of the Joint Staff and the Heads of the DoD Components, the Milestone Decision Authority decides whether to place the program under joint acquisition management. The Milestone Decision Authority should make this decision and, if appropriate, designate the Lead Executive DoD Component, as early as possible in the acquisition process.

The DoD Components should periodically review their programs to determine the potential for joint cooperation. The DoD Components should structure program strategies to encourage and to provide an opportunity for multi-Component participation.

11.1.2.2. Execution

The designated Lead Executive DoD Component for a joint acquisition should act on behalf of all DoD Components involved in the acquisition.

A Memorandum of Agreement should specify the relationship and respective responsibilities of the Lead Executive DoD Component and the other participating components. The Memorandum of Agreement should address system capabilities and the development of capabilities documents, funding, manpower, and the approval process for other program documentation.

The following additional considerations have proven effective in managing joint programs:

- The assignment of a Lead Executive DoD Component should consider the demonstrated best business practices of the DoD Components, including plans for effective, economical, and efficient management of the joint program; and the demonstrated willingness of the DoD Component to fund the core program, essential to meeting joint program needs.
- The Milestone Decision Authority and DoD Components should consolidate and co-locate the supporting efforts of the joint program at the Lead Executive DoD Component's program office, to the maximum extent practicable.
- The Component Acquisition Executive of the Lead Executive DoD Component should optimally use the acquisition organizations, test organizations, and other facilities of all Military Departments.
- The designated Lead Executive DoD Component selects the qualified program manager for the designated program under joint acquisition. The single program manager should then be fully responsible and accountable for the cost, schedule, and performance of the development system.
- If the joint program results from a consolidation of several different DoD Component programs, each with a separate program manager, the selected joint program manager should have the necessary responsibility and authority to effectively manage the overall system development and integration.
- A designated program under joint acquisition should have one quality assurance

program, one program change control program, one integrated test program, and one set of documentation and reports (specifically: one set of capabilities documents, (with Service unique capability requirements identified), one Information Support Plan , one Test and Evaluation Master Plan , one Acquisition Program Baseline , etc.).

- The Milestone Decision Authority should designate the lead Operational Test Agency to coordinate all operational test and evaluation. The lead Operational Test Agency should produce a single operational effectiveness and suitability report for the program.
- Documentation for decision points and periodic reporting should flow only through the Lead Executive DoD Component acquisition chain, supported by the participating components.
- The program should use inter-DoD Component logistics support to the maximum extent practicable, consistent with effective support to the operational forces and efficient use of DoD resources.
- Unless statute, the Milestone Decision Authority, or a memorandum of agreement signed by all DoD Components directs otherwise, the Lead Executive DoD Component should budget for and manage the common Research, Development, Test, and Evaluation funds for the assigned joint programs.
- Individual DoD Components should budget for their unique requirements.

11.2. International Programs

11.2.1. International Cooperative Programs

11.2.1.1. International Considerations and Program Strategy

11.2. International Programs

11.2.1. International Cooperative Programs

An international cooperative program is any acquisition program or technology project that includes participation by one or more foreign nations, through an international agreement, during any phase of a systems life cycle. The key objectives of international cooperative programs are to reduce weapons system acquisition costs through cooperative development, production, and support; and to enhance interoperability with coalition partners.

11.2.1.1. International Considerations and Program Strategy

Title 10 U.S.C. 2350a(e) as amended by Section 1251 of the National Defense Authorization Act for Fiscal Year 2008 requires an analysis of potential opportunities for international cooperation for all Acquisition Category I programs before the first milestone or decision point. DoD Directive 5000.01, Enclosure 1 , and DoD Instruction 5000.02, Enclosure 10, paragraph 5 , specify the requirements for international cooperative program management; amplifying guidance and information appears in this

Guidebook. DoD Directive 5000.01 requires International Armaments Cooperation; requires interoperability with U.S. coalition partners; and establishes the preference for a cooperative development program with one or more Allied nations over a new, joint, or DoD Component-unique development program.

During the development of the Technology Development Strategy (TDS) for Milestone A or the initial Acquisition Strategy for Milestone B for a new program, the potential for international cooperative research, development, production, and logistic support should be addressed, and thereafter, the potential for international cooperation should be considered in every phase of the acquisition process. DoD Components should periodically review their programs to determine the potential for international cooperation. Milestone Decision Authorities may recommend forming international cooperative programs based on the TDS or Acquisition Strategy considerations; DoD Component Heads may also recommend forming international cooperative programs. The Milestone Decision Authority should make the decision to establish an international cooperative program as early as possible in the Defense Acquisition Management System.

The Milestone Decision Authority, with the advice and counsel of the DoD Components and the Joint Requirements Oversight Council, makes the decision to pursue an international cooperative program. The decision process should consider the following:

- Demonstrated best business practices, including a plan for effective, economical, and efficient management of the international cooperative program;
- Demonstrated DoD Component willingness to fully fund their share of international cooperative program needs;
- The long-term interoperability and political-military benefit's that may accrue from international cooperation; and
- The international program's management structure as documented in the international agreement. The designated program manager (U.S. or foreign) is fully responsible and accountable for the cost, schedule, and performance of the resulting system.

The DoD Component remains responsible for preparation and approval of most statutory, regulatory, and contracting reports and milestone requirements, as listed in DoD Instruction 5000.02, Enclosure 4 . Documentation for decision reviews and periodic reports flow through the DoD Component acquisition chain, supported by the participating nation(s).

International cooperation can add stability to the program. DoD Instruction 5000.02 prevents DoD Components from terminating or substantially reducing participation in international cooperative programs under signed international agreements without Milestone Decision Authority notification, and in some cases, Milestone Decision Authority approval.

Additional information may be found in the Director, International Cooperation,

International Cooperation in Acquisition, Technology and Logistics Handbook .

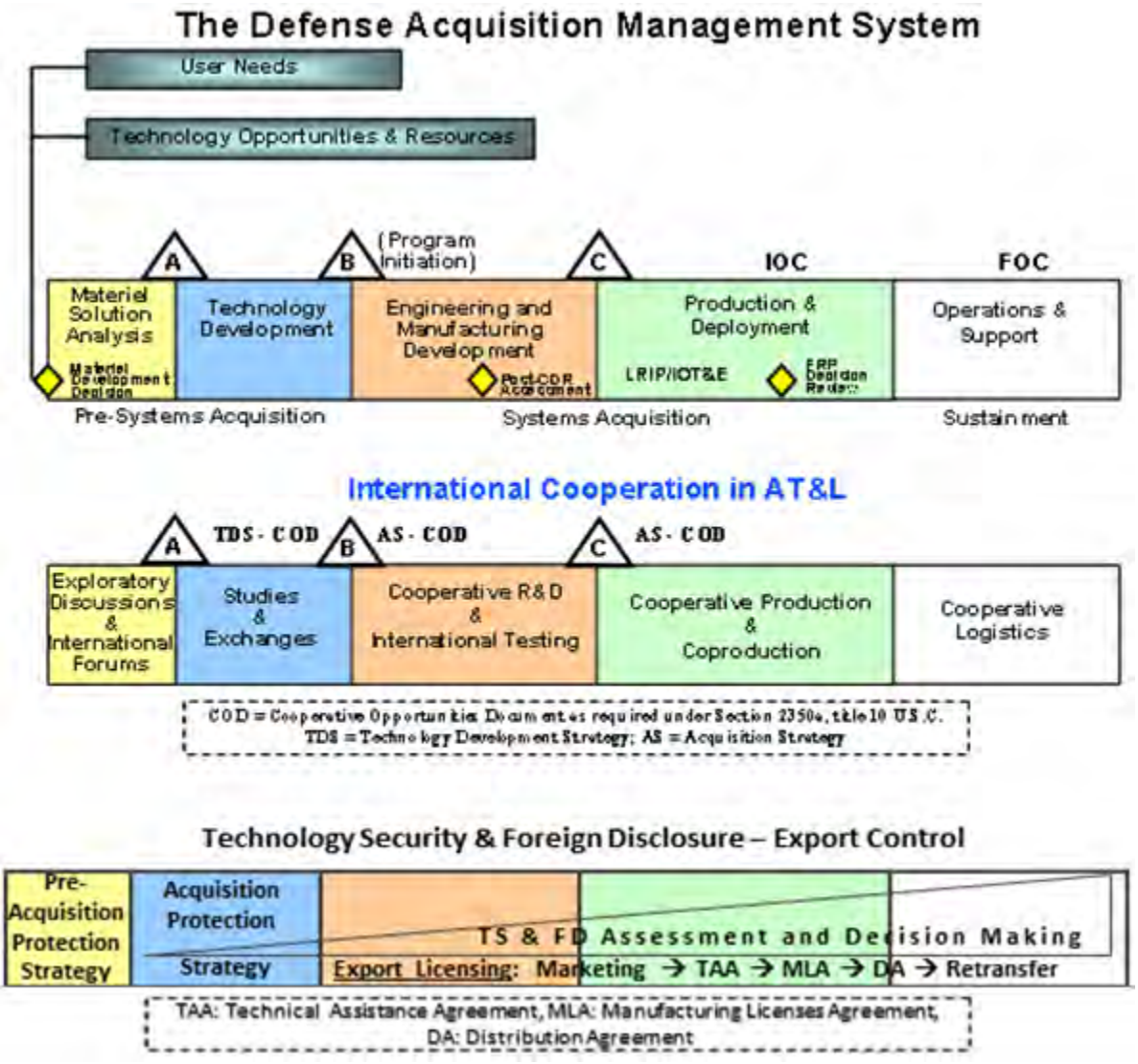
11.2.1.2. International Considerations within the Defense Acquisition Management System

11.2.1.2. International Considerations within the Defense Acquisition Management System

Establishing and maintaining cooperative relationships with friends and Allies are critical to achieving interoperability of equipment and services to be used by the U.S. Armed Forces and our coalition partners; to achieving access to technology from sources worldwide; to achieving economies of scale with our investment resources; and to expanding our influence in critical areas of the world (USD(AT&L) Memorandum, Support for International Armaments Cooperation Activities, January 23, 2006)

International programs may be established at any point in the defense acquisition management system when justified as a prudent business judgment. Figure 11.2.1.2.F1 depicts the key considerations for each phase to include consideration of program protection concerns, which are part of the overshadowing technology security and foreign disclosure process, further discussed in 11.2.1.3.

Figure 11.2.1.2.F1. Key International Cooperative Considerations During Acquisition.



Determination of User Needs & Exploring Technology Opportunities (Early Technology Projects). The efforts needed to identify cooperative development opportunities before entering into a formal acquisition program are often challenging, but such activities capitalize on high payoffs in cost savings and interoperability when successful. Formulation of cooperative development programs involves resolution of issues in the areas of requirements harmonization, cost sharing, work sharing, intellectual property rights, technology transfer, including technology security and foreign disclosure (TS&FD) considerations, and many others. While multinational force compatibility may increase system acquisition cost, it can provide more cost-effective defense for the whole force through increased interoperability and reduced life-cycle

costs. Cooperative opportunities identification and formulation should be pursued during the earliest stages of the pre-systems acquisition research and development process to maximize the chance for success. DoD Instruction 5000.02, Enclosure 3, paragraph 2 , identifies technology projects and initiatives.

Using the Joint Capabilities Integration and Development System process, representatives from multiple DoD communities formulate broad, time-phased, operational goals, and describe requisite capabilities in the Initial Capabilities Document. They examine multiple concepts and materiel approaches to optimize the way the Department of Defense provides these capabilities. This examination includes robust analyses that consider affordability, technology maturity, and responsiveness.

Several important mechanisms available to provide insight into the needs of potential foreign partners are exploratory discussions, international forums, studies, and the exchanges of information and personnel:

Exploratory Discussions. Before entering into an international project, many forms of dialogue can take place with potential partners. These informal discussions are usually called exploratory discussions or technical discussions--they are NOT called "negotiations," which requires a legal authority and formal permission from the Office of the Secretary of Defense. Exploratory discussions are characterized by the avoidance of any binding commitments on the part of the U.S. Government, and the absence of any draft, international agreements. Other than the two exclusions above, the parties may discuss most other topics, provided release authority has been obtained for any information provided by DoD representatives or defense contractors.

International Forums. There are many international forums dedicated to discussing mutual armaments needs and early technology projects. These forums include the Conference of National Armaments Directors (CNAD) , whose U.S. representative is the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)). The CNAD's subsidiaries are the "Main Armaments Groups," particularly the NATO Army Armaments Group, NATO Navy Armaments Group , and the NATO Air Force Armaments Group . The NATO Science and Technology Organization conducts and promotes cooperative research and information exchange in NATO. The Technical Cooperation Program with Australia, Canada, New Zealand, and the United Kingdom is another multilateral forum dedicated to cooperation in conventional military technology development. In addition there are about 30 bilateral forums, such as the U.S.-Japan Systems and Technology Forum and the U.S./Canadian Armaments Cooperation Management Committee, that have a similar purpose. Also see International Cooperation in Acquisition, Technology and Logistics Handbook, Chapter 11.

Studies. It is normal for the DoD and potential partners to conduct studies before entering into a cooperative acquisition project. These studies can be conducted years before the project starts, and are often called feasibility studies, or pre-feasibility studies. Industry, government agencies, or a combination of both generally conduct the feasibility studies, with the objective of providing a technical appraisal of the feasibility of

developing and producing equipment. These studies can develop input for the Analysis of Alternatives required by DoD before the start of a new acquisition program.

International Exchanges of Information and Personnel. A common source for cooperative program opportunity identification is the Defense Research, Development, Test and Evaluation Information Exchange Program (IEP) , which provides a standardized way of conducting bilateral science and technology information exchange (formerly called data exchange). The IEP has proven extremely useful as a means of cooperative opportunities formulation. Another source for identifying cooperative opportunities is the Defense Personnel Exchange Program , especially the Engineers and Scientists Exchange Program (ESEP).

Pre-Systems Acquisition. Decisions made during the Materiel Solution Analysis and Technology Development phases of Pre-Systems Acquisition generally define the nature of the entire program. Once the program enters the Engineering and Manufacturing Development phase, it is difficult to adopt major changes without significant schedule or cost adjustments. Consequently, the decision to include international partners needs to be addressed as early as possible, preferably during development of the Initial Capabilities Document, but no later than during the Materiel Solution Analysis phase.

To meet the requirements of Title 10 U.S.C. 2350a(e) , the Technology Development Strategy (TDS) prepared for Milestone A or the Acquisition Strategy for Milestones B and C must follow the mandatory TDS and Acquisition Strategy (AS) outline addressed and provided in DAG Chapter 2.8 . The outline addresses milestone document preparation, including a section for international involvement.

International involvement must be addressed in the TDS and AS as follows:

International Involvement

- Indicate any limitations on foreign contractors being allowed to participate at the prime contractor level.
- International Cooperation.
    - Summarize any plans for cooperative development with foreign governments or cognizant organizations. List the memorandums of agreement (MOAs) in place and identify the contracting activities.
    - Summarize plans to increase the opportunity for coalition interoperability as part of the developing DoD program.
    - Employ the AT&L-developed Technology Development Strategy/Acquisition Strategy template to provide a coalition interoperability section in the Acquisition Strategy. Using the template will satisfy the cooperative opportunities document requirement of 10 USC 2350a.
- Foreign Military Sales. Specify the potential or plans for Foreign Military and/or Direct Commercial Sale and the impact upon program cost due to program

protection and exportability features.

These considerations are based on 10 U.S.C. 2350a requirements. They encourage the consideration of alternative forms of international cooperation. Even if cooperative development is impractical, cooperative production, foreign military sales, licensed production, component/subcomponent co-development, or incorporation of subsystems from allied or friendly foreign sources should be considered where appropriate.

DoD Components should fully investigate potential cooperative opportunities as part of the Technology Development Strategy and Acquisition Strategy development. Program proponents should consult with the appropriate international programs organization to obtain assistance in addressing international considerations during Technology Development Strategy or Acquisition Strategy development for programs in all acquisition categories.

The Defense Exportability Features (DEF) Pilot Program. DEF was established in the fiscal year 2011 National Defense Authorization Act to develop and incorporate technology protection features into a system or subsystem during its research and development phase. By doing this, exportable versions of a system or subsystem could be sold earlier in the Production and Development phase, thereby (1) enabling capability to be available to allies and friendly companies more rapidly and (2) lowering the unit cost of DoD procurements. Prior to the Engineering and Manufacturing Development Phase, programs should investigate the necessity and feasibility (from cost, engineering, and exportability perspectives) of the design and development of differential capability and enhanced protection of exportable versions of the system or subsystem.

Acquisition programs candidates may be considered for the DEF pilot program via nominations from the DoD components. AT&L / International Cooperation (IC) is available for consultation regarding potential DEF candidate nominations. After a favorable preliminary assessment of exportability and differential capability / program protection needs, AT&L / IC will approve DEF candidates. Specific differential capability / program protection requirements will be determined by DoD technology security, foreign disclosure, anti-tamper processes. With sufficient industry and government support, a feasibility study will be conducted to determine the cost to implement the differential features and the associated design specifications. If a DEF candidate is pre-Milestone A, the feasibility study should be incorporated into the appropriate technology development requests for proposal (RFPs) and contracts. Otherwise, the feasibility study should be contracted through the prime contractor if funding is available. If government and industry agree that the differential capability / protection determined by the feasibility study should be implemented, and funding arrangements are agreed upon, the required design specifications should be incorporated into the engineering and manufacturing development RFP and/or contract, depending on when the feasibility study was completed.

Engineering and Manufacturing Development. After program initiation, during Engineering and Manufacturing Development, key elements of the system design are defined, and system/subsystem development begins. Major changes often present schedule delays that program managers are unwilling to accept; however, there have been numerous examples of successful subsystem cooperative development partnerships that have been formed during the Engineering and Manufacturing Development Phase. Once a program has reached this phase, absent cooperation in earlier stages, there will be only limited opportunity to bring other nations on as full cooperative development partners. Consequently, if the opportunity for cooperation in subsystem development arises prior to or during Engineering and Manufacturing Development, consult with the appropriate international programs organization to obtain further assistance.

Foreign Comparative Testing. A viable alternative to development is the acquisition of commercial items. While individual acquisition programs can conduct evaluations with their own resources, the Foreign Comparative Testing Program offers a structured and funded means for program offices to evaluate the suitability of a foreign developed item for purchase in lieu of developing a similar U.S. item.

International Test Operations Procedures. The International Test Operations Procedures (ITOP) program provides for international agreements that document state-of-the-art test techniques for technical testing of military material and allows the exchange of test data to avoid redundant testing when foreign equipment is purchased. Currently there are over 130 ITOPs with Germany, France, and the UK covering a variety of test types and/or equipment class. Through ITOPs, the U.S. has access to latest test technology and procedures of our allies, which could possibly be utilized by DoD program managers. The ITOP program is managed at OSD by the Office of the Director, Operational Test and Evaluation. See the International Cooperation in Acquisition, and Logistics Handbook Chapter 6 Section 6.4.3.

Production and Deployment Phase. There are three basic mechanisms for transfer of U.S. produced defense articles and associated production capability to other nations: sales, co-production and cooperative production. Sales under the Foreign Military Sales Program foreign co-production of a U.S. developed system, fall under the purview of the Defense Security Cooperation Agency (DSCA) . The Department of State is responsible for transfer of defense articles and associated production capability under export licenses. Both DSCA and the Defense Technology Security Administration coordinate closely with the responsible DoD Component regarding the development and implementation of DoD co-production policy in their respective areas of responsibility. USD(AT&L) is responsible for oversight of the third basic mechanism, cooperative production. Cooperative production is a joint or concurrent international production arrangement arising from a cooperative development project. Examples of this type of production program are the Rolling Airframe Missile and the Multi-Functional Information Distribution System . Cooperative production falls under the authority of the

Arms Export Control Act Section 2751 .

Operations & Support Phase. Cooperative logistics refers to cooperation between the U.S. and allied or friendly nations or international organizations in the logistical support of defense systems and equipment. Cooperative logistics is part of the acquisition process, but as a substantial part of military operations, much of the implementation process involves Security Assistance processes and procedures.

Cooperative logistics support includes:

- Logistics Cooperation international agreements (IAs), used to improve sharing of logistics support information and standards, and to monitor accomplishment of specific cooperative logistics programs;
- Acquisition and Cross-Servicing Agreements;
- Host Nation Support;
- Cooperative Logistics Supply Support Arrangements;
- Cooperative Military Airlift Agreements;
- War Reserve Stocks for Allies;
- Agreements for acceptance and use of real property or services;
- Standardization of procedures under American/British/Canadian/Australian/New Zealand auspices;
- International Standardization Agreements developed in conjunction with member nations of the North Atlantic Treaty Organization and other allies and coalition partners, as described in DoD 4120.24-M, "Defense Standardization Program (DSP) Policies and Procedures" and as listed in the Acquisition Streamlining and Standardization Information System (ASSIST) database (login required);
- Consideration of the interoperability implications of these agreements when constructing Work Breakdown Structures; and
- Planning support provided by the Program Manager's e-Tool Kit .

Each participant or party involved in cooperative logistics agreements should benefit from the agreement. Benefits could be tangible, such as the U.S. receiving support for its naval vessels when in a foreign port; or intangible, such as the foreign nation receiving the implied benefit of a visible, U.S. naval presence in the region. Other cases are more obviously quid-pro-quo: cross-servicing agreements , for example. In a cross-servicing agreement, each party receives the equivalent of the materiel or services provided to the other party. Besides the obvious material benefit's, such agreements have the collateral effects of opening dialog and creating relationships between the parties. Such dialog and relationships may serve to strengthen political bonds. While not a program manager responsibility, DoD acquisition personnel should be aware of the international consequences of their activities and appropriately support such efforts. See the International Cooperation in Acquisition, and Logistics Handbook Chapter 5.

11.2.1.3. International Aspects of Program Protection

Program protection considerations play a major role in international programs for obvious reasons. The program manager should consider technology security and foreign disclosure (TS&FD) factors in a program with international aspects. The TS&FD Office (TSFDO), located at the Defense Technology Security Administration in concert with DoD Component. Program managers should contact their DoD Component TS&FD organization early enough in the process to ensure that TS&FD factors that may affect international program aspects are taken into consideration.

Early consideration of TS&FD requirements as well as export control planning in international programs will enable the program to achieve maximum benefit from international participation while avoiding negative impacts on cost, schedule and performance goals. The program manager should consider technology release in the initial planning of a program with international aspects through a review of existing TS&FD guidance and development of elements of their Program Protection Plan .The Deputy Secretary of Defense established a TS&FD Review Group in July 2010 to investigate options for harmonizing and streamlining existing DoD TS&FD processes. The Arms Transfer and Technology Release Senior Steering Group, established in 2008, sponsored the effort. As of July 2011, a Directive-Type Memorandum is in coordination to initiate detailed design efforts for DoD TS&FD process consolidation with the thirteen existing DoD and interagency TS&FD processes. As noted above, a new TSFDO was established to improve the TS&FD system operations on a DoD-wide basis. To do this, TSFDO screens, prepares, and tracks DoD High Level Decisions (HLDs) to ensure all HLDs are identified in a timely fashion and appropriately routed to and addressed by all relevant DoD TS&FD processes and subject matter experts. Program Managers should work with their DoD Component TS&FD organizations and the TSFDO if they encounter challenges in identifying or processing HLDs related to the international aspects of their programs.

DoD Instruction 5000.02, Enclosure 10, paragraph 5 , and the tables of enclosure 4 establish international cooperative program protection policy requirements. Chapter 13.2 of this Guidebook provides additional insights into this policy.

11.2.1.3.1. Classification Guide

In addition to the Program Protection Plan required by all programs containing Critical Program Information, and the Technology Assessment/Control Plan , DoDM 5200.01 requires international programs to develop a classification guide for all programs containing classified information of either party. The classification guide, as prescribed in DoD Directive 5230.11 , identifies the items or information to be protected in the program, and indicates the specific classification to be assigned to each item.

11.2.1.3.2. Program Security Instruction (PSI)

A PSI details security arrangements for the program and harmonizes the requirements of the participants' national laws and regulations. Using the Under Secretary of Defense for Acquisition, Technology and Logistics international agreements streamlined procedures authorized by DoD Instruction 5000.02, Enclosure 10, paragraph 5 , the International Agreements Generator will lead the program manager through the considerations for, and the development of, a PSI. Additional information about the PSI is found in the International Cooperation in Acquisition, Technology and Logistics Handbook Chapter 7, Section 7.6..

If all security arrangements to be used in an international program are in accordance with an existing industrial security arrangement between the participants, a separate PSI is not required.

11.2.1.3.3. Delegation of Disclosure Authority Letter (DDL)

Per DoD Instruction 5000.02, a written authorization to disclose any classified or controlled unclassified information must be obtained prior to entering discussions with potential foreign partners. The authorization for release of classified information (developed or used during any part of the life cycle of the program) to any potential or actual foreign participants in the program will be in the form of a Delegation of Disclosure Authority Letter (DDL) , as prescribed in DoD Directive 5230.11 , or other written authorization issued by the DoD Component Foreign Disclosure Office. The authorization for release of classified or controlled unclassified information must comply with DoD Component policies for release of such information.

11.2.1.3.4. Technology Release Roadmap (TRR)

Prior to the Engineering and Manufacturing Development phase of an acquisition program with substantial international involvement by foreign industry, the program manager should prepare an export control TRR as part of their Technology Assessment/Control Plan (TA/CP) . This TRR will provide a projection of when export licenses will be required in support of the acquisition process, and when critical milestones regarding national disclosure policy implementation will need to be addressed. The TRR must be consistent with the program's TA/CP, Security

Classification Guide (SCG) , and other disclosure guidance.

The TRR accomplishes the following:

- Provides early DoD Component planning for the program's proposed technology releases to foreign industry consistent with the National Disclosure Policy.
- Provides early planning for higher-level (i.e., above DoD Component-level) special technical reviews and approvals (i.e. Low Observable/Counter Low Observable, anti-tamper, cryptography) needed in support of proposed technology releases to foreign industry.
- Establishes a detailed export license approval planning process for U.S.-foreign industry cooperation to meet critical program and contract timelines.

The TRR includes three sections: 1) A timeline mapping key projected export licenses against the program acquisition schedule; 2) A definition of the technologies involved in each export license; and 3) A list of U.S. contractors (exporters) as well as foreign contractors (end users) for each license.

11.2.2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))-Related International Agreement Procedures

An International Agreement (IA) is any agreement concluded with one or more foreign governments including their agencies, instrumentalities, or political subdivisions, or with an international organization. The IA delineates respective responsibilities and is binding under international law. IAs are required by U.S. law for all international cooperative projects.

Per DoD Instruction 5000.02 , all AT&L-related international agreements may use the USD(AT&L)-issued streamlined procedures found in this Guidebook and in the International Cooperation in Acquisition, Technology and Logistics Handbook , rather than following the lengthy documentation requirements mandated by DoD Directive 5530.3 , "International Agreements."

11.2.2.1. Preparation and Documentation

The following considerations apply to the preparation of and documentation associated with Acquisition, Technology and Logistics-related international agreements:

- Program managers or project leaders consult with the DoD Component's international programs organization, as well as foreign disclosure, legal, and comptroller personnel, to develop international agreements.
- The DoD Components develop international agreements in accordance with the provisions of the most recent version of DoD International Agreement Generator computer software.
- Prior to initiating formal international agreement negotiations, the DoD Components prepare a Request for Authority to Develop and Negotiate (RAD) that consists of a cover document requesting such authority and a Summary Statement of Intent (SSOI) that describes the DoD Component's proposed approach to negotiations. DoD Components that have not been delegated authority to negotiate (currently the three Military Departments and the Missile Defense Agency have such authority) normally are required to provide a copy of the draft international agreement prior to RAD approval.
- Prior to signing an international agreement, the DoD Components prepare a Request for Final Approval (RFA) that consists of a cover document requesting such authority, a revised SSOI that describes the outcome of negotiations, and the full text of the international agreement to be signed on behalf of the Department of Defense.
- The DoD Components should use the Streamlining I Coordination Process for both the RAD and the RFA. They should apply to Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation to be delegated authority to use Streamlining II procedures for processing International Agreements. If Streamlining II authority is or has been delegated, the DoD Component should use the streamlined process. (To date, the Office of the USD(AT&L)/International Cooperation has only delegated Streamlining II authority to the Department of the Navy.)

11.2.2.2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) Oversight

OUSD(AT&L)/International Cooperation provides the following international agreement oversight support:

- Approves and makes available the following agreement process guidance:

    - Request for Authority to Develop (RAD);
    - Request for Final Approval (RFA);
    - Summary Statement of Intent (SSOI);
    - Arms Export Control Act Section 27 Project Certification format requirements; and
    - DoD International Agreement Generator computer software.
- Approves the following agreement process actions:
    - RADs and RFAs for Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA);
    - Project Agreements and Arrangements;
    - Arms Export Control Act Section 65 Loan Agreements;
    - End-User Certificate (EUC) Waivers ;
    - Foreign Military Sales or Direct Commercial Sales of Major Defense Equipment with Letters of Request (LOR) Advisories and Requests for Major Defense Equipment (MDE) Prior to Satisfactory Completion of Operational Test and Evaluation (OT&E) formerly called Yockey Waivers ; and
    - DoD Component requests for DoD International Agreement Generator text deviations or waivers requested in RAD and RFA submissions.
- Delegates PA negotiation authority under the Streamlining I Coordination (Approval) Process to specifically designated DoD Components.
- Certifies DoD Component international agreement processes to the Streamlining II standards prior to delegation of RAD/RFA authority to a DoD Component.
- Decertifies a DoD Component international agreement process in the event minimum quality standards are not maintained.
- Resolves RAD/RFA coordination process disputes.
- Oversees the DEF pilot program to include technology protection features during research and development of defense systems under 10 USC 2358.
- Supports satisfaction of the following statutory requirements:
    - Obtains USD(AT&L) determination under 10 U.S.C. 2350a paragraph (b) for all international agreements that rely upon this statute as their legal authority;
    - Notifies Congress of all Arms Export Control Act Section 27 (see 22 U.S.C. Section 2767 , "Authority of President to enter into cooperative projects with friendly foreign countries") international agreements a minimum of 30 calendar days prior to authorizing agreement signature; and
    - Conducts interagency coordination with the Department of State, Department of Commerce, and the Department of the Treasury (see 22 U.S.C. 2767 and DoD Directive 5530.3).

11.2.2.3. Coordination Processes

There are two accredited international agreement coordination processes: Streamlining I and Streamlining II .

11.2.2.3.1. International Agreement Streamlining I Process

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation (IC) uses the following Streamlining I process unless it has delegated coordination authority to the DoD Component:

- **Request for Authority to Develop and Negotiate (RAD) Memorandum of Understanding (MOUs) and Memorandum of Agreements (MOAs)** . The DoD Component prepares the RAD and obtains OUSD(AT&L)/IC approval prior to initiating MOU or MOA negotiations. If applicable, the DoD Component develops and submits Coalition Warfare Program (CWP) funding requests associated with the RAD, in accordance with the CWP Management Plan. OUSD(AT&L)/IC conducts DoD and interagency coordination, as appropriate, using a standard review period of 21 working days, which may expedited at OUSD(AT&L)/IC's discretion.
- **RAD Program Authorizations (PAs) and Section 65 Loan Agreements** . Unless OUSD(AT&L)/IC delegates PA negotiation authority, the DoD Component prepares a RAD and obtains OUSD(AT&L)/IC approval prior to initiating PA or Section 65 Loan Agreement negotiations. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, using a standard review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion.
- **Negotiation** . Generally, within 9 months of receipt of RAD authority, the DoD Component negotiates the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.
- **Request for Final Approval to Conclude (RFA) MOUs and MOAs** . The DoD Component prepares the RFA and obtains OUSD(AT&L)/IC approval prior to signing the MOU or MOA. RFAs for agreements relying upon Arms Export Control Act (AECA) Section 27 as the legal authority for the international agreement will also include a Project Certification. OUSD(AT&L)/IC conducts interagency coordination, as appropriate, based upon a standard review period of 21 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.
- **RFA PAs and Section 65 Loan Agreements** . The DoD Component submits RFAs notifying OUSD(AT&L)/IC of its intention to sign PAs and Section 65 Loan Agreements prior to concluding such agreements. AT&L/IC conducts interagency coordination, as appropriate, based upon a review period of 15 working days, which may be expedited at OUSD(AT&L)/IC's discretion. OUSD(AT&L)/IC provides Congress with any required AECA Section 27 notifications.

11.2.2.3.2. International Agreement Streamlining II Process

Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))/International Cooperation (IC) may delegate approval authority for the Request for Authority to Develop and Negotiate/Request for Final Approval (RAD/RFA) for all international agreements associated with programs with a total program value of

less than $25M (in FY01 constant dollars) and for Acquisition Category II and Acquisition Category III programs to the DoD Component Acquisition Executive. The DoD Component Acquisition Executive may subsequently re-delegate RAD/RFA authority for programs with a total program value of less than $10M (in FY01 constant dollars) and Acquisition Category III programs to the Head of the DoD Component's international programs organization. The following procedures will apply:

- The DoD Components will obtain the concurrence of their legal, financial management, and foreign disclosure organizations prior to approving RADs/RFAs.
- The DoD Components will forward coordination disputes to OUSD(AT&L)/IC for resolution.
- The DoD Components will send Notices of Intent to Negotiate (NINs) or Notices of Intent to Conclude (NICs) to OUSD(AT&L)/IC for all approved RADs and RFAs. NINs will include the DoD Component's approval document and program Summary Statement of Intent. NICs will also include the final international agreement text to be signed, plus an Arms Export Control Act Section 27 Project Certification, if required. The DoD Components will not sign international agreements until a 15-working-day period (for PAs and Loans) or 21-working-day period (for Memoranda of Understanding) after AT&L/IC receipt of the NIC has elapsed and any required 10 U.S.C. 2350a approval or AECA Section 27 Congressional notification process has been completed.
- OUSD(AT&L/IC) may, at its discretion, decide to waive these rules on a case-by-case basis and require that certain agreements receive specific OUSD(AT&L/IC) approval before conclusion.
- OUSD(AT&L)/IC will use NINs, NICs and other relevant information to verify DoD Component international agreement process quality.
- Generally, within 9 months of receipt of RAD authority, DoD Component personnel will negotiate the international agreement in accordance with the provisions of the most recent version of DoD International Agreement Generator.

11.2.2.3.3. Coordination of Requests for Authority to Develop and Negotiate (RADs), Requests for Final Approval (RFAs), Notices of Intent to Negotiate (NINs), and Notices of Intent to Conclude (NICs) Relating to Nuclear, Chemical, and Biological (NCB) Fields

The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics/International Cooperation coordinates all international agreements (including Memoranda of Understanding, Project Arrangements, other similar agreements) and Information Exchange Program annexes (See IC in AT&L Handbook, Chapter 13.) relating to NCB warfare technologies (including defenses against such technologies) with the Assistant to the Secretary of Defense (Nuclear and Chemical and Biological Defense Programs) prior to approving the agreement. DoD policy requires this coordination for NCB-related RADs for project arrangements under Streamlining I authority, and for NINs and NICs under Streamlining II authority.

11.2.3. Acquisition and Cross-Servicing Agreements (ACSAs)

ACSAs are bilateral international agreements that allow for the provision of cooperative logistics support under the authority granted in 10 U.S.C. Sections 2341-2350 . They are governed by DoD Directive 2010.9 , "Acquisition and Cross-Servicing Agreements" and implemented by CJCS Instruction 2120.01B , "Acquisition and Cross-Servicing Agreements." ACSAs are intended to provide an alternative acquisition option for logistics support in support of exercises or exigencies.

11.2.3.1. Types of Acquisition and Cross-Servicing Agreements (ACSAs) Authorities

Title 10 of the United States Code provides two legal authorities for foreign logistic support, supplies, and services: an Acquisition-only Authority, and a Cross-Servicing Authority, which includes an acquisition authority and a transfer authority.

Acquisition-Only Authority . 10 U.S.C. Section 2341 , "Authority to acquire logistic support, supplies, and services for elements of the armed forces deployed outside the United States," authorizes elements of the U.S. Armed Forces, when deployed outside the United States, to acquire logistic support, supplies, and services from eligible foreign entities on a reimbursable basis. The authority is not reciprocal and does not require the existence of a cross-servicing agreement or implementing arrangement. This is a very limited authority that has been mainly supplanted by the use of broader authorities in ACSAs. Acquisition-only authority may be used with the governments of NATO members, NATO and its subsidiary bodies, the United Nations Organization, any regional organization of which the United States is a member, and any other countries which meet one or more of the following criteria:

- Has a defense alliance with the United States;
- Permit’s the stationing of members of the U.S. armed forces in such country or the home porting of naval vessels of the United States in such country;
- Has agreed to preposition materiel of the United States in such country; or
- Serves as the host country to military exercises which include elements of the

U.S. armed forces or permit's other military operations by the U.S. armed forces in such country.

Cross-Servicing Authority . 10 U.S.C. 2342 , "Cross-servicing agreements," authorizes the Department of Defense, upon coordination with the Secretary of State, to conclude reciprocal agreements with foreign countries and regional and international organizations for the provision of logistics, support, supplies and services. A current listing of these agreements and countries and organizations eligible to negotiate them is maintained by the Director for Logistics, The Joint Staff (J-4). DoD Directive 2010.9 provides the official process for nominating countries for eligibility for such agreements as well as for concluding them.

11.2.3.2. Permitted and Prohibited Uses of Acquisition and Cross-Servicing Agreements (ACSAs)

ACSA is for the transfer of logistics, support, supplies, and services only. Per Section 4.5 of DoD Directive 2010.9 , items that may not be acquired or transferred under ACSA authority include weapons systems; the initial quantities of replacement and spare parts for major end items of equipment covered by tables of organization and equipment, tables of allowances and distribution, or equivalent documents; and major end items of equipment. Specific items that may not be acquired or transferred under ACSA authority include guided missiles; naval mines and torpedoes; nuclear ammunition and included items such as warheads, warhead sections, projectiles, and demolition munitions; guidance kit's for bombs or other ammunition; and chemical ammunition (other than riot control agents). General purpose vehicles and other items of non-lethal military equipment not designated as Significant Military Equipment on the United States Munitions List promulgated pursuant to 22 U.S.C. 2778 , may be leased or loaned for temporary use. Specific questions on the applicability of certain items should be referred to the Combatant Command's legal office for review and approval.

11.2.3.3. Repayment of Acquisition and Cross-Servicing Agreement (ACSA) Obligations

In addition to the use of cash and subject to the agreement of the parties, ACSA obligations may be reconciled by either Replacement-in-Kind or Equal Value Exchange. ACSA obligations not repaid by Replacement-in-Kind or Equal Value Exchange automatically convert to cash obligations after one year.

Replacement in Kind (RIK) . RIK allows the party receiving supplies or services under the ACSA to reconcile their obligation via the provision or supplies and services of an identical or substantially identical nature to the ones received. As an example, a country may provide extra water to the United States during a training exercise with the proviso that the United States will provide the same amount of water during a future exercise.

Equal Value Exchange (EVE) . EVE enables the party receiving supplies or services under the ACSA to reconcile their obligation via the provision of supplies or services

that are considered to by both parties to be of an equal value to those received. As an example, a country may provide extra water to the United States during a training exercise in exchange for the United States providing extra ammunition.

11.2.3.4. Acquisition and Cross-Servicing Agreement (ACSA) Implementation

DoD Directive 2010.9 and CJCS Instruction 2120.01B provide management guidance on initiating ACSA orders, receiving support, reconciling bills, and maintaining records. As this is a Combatant Command-managed program, organizations interested in acquiring logistics, support, supplies and services should work through the applicable logistics branch to receive further guidance on this topic.

11.2.4. Summary of International Cooperation Guidance and Resources

11.2.4. Summary of International Cooperation Guidance and Resources

International cooperation offers the opportunity to achieve cost savings from the earliest phases of Pre-Systems Acquisition throughout the life cycle, while enhancing interoperability with coalition partners. All DoD acquisition personnel, in consultation with the appropriate international programs organizations, should strive to identify and pursue international cooperative programs in accordance with DoD 5000 policy . Specific topics are found in the International Cooperation in Acquisition, Technology and Logistics Handbook at the OSD/International Cooperation website .

11.3. Integrated Program Management

11.3. Integrated Program Management

The program manager should obtain integrated cost and schedule performance data at an appropriate level of summarization to monitor program execution. The program manager should require contractors and government activities to use internal management control systems that accomplish the following:

- Relate time-phased budgets to specific tasks identified in the statement of work;
- Produce data that indicate work progress;
- Properly relate cost, schedule, and technical accomplishment; and
- Produce data that is valid, timely, and auditable.

Unless waived by the Milestone Decision Authority, the program manager should require that the management control systems used to plan and control contract performance comply with American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748 (see DoD Instruction 5000.02) in accordance with paragraph 11.3.1.1.. The program manager should not impose a specific system or method of management control or require a contractor to change its system, provided it complies with ANSI/EIA-748.

11.3.1. Earned Value Management (EVM)

EVM is a key integrating process in the management and oversight of acquisition programs, to include information technology projects. It is a management approach that has evolved from combining both government management requirements and industry best practices to ensure the total integration of cost, schedule, and work scope aspects of the program.

Unless waived by the Milestone Decision Authority, EVM applies to contracts as described in the subsections below. The program manager's approach to satisfying the EVM requirement for applicable contracts should be documented in the program acquisition strategy. This strategy then should be reflected in the contract language and CDRLs provided to the contractor for a given contract while not violating the basic tenets of sound EVM implementation.

The Office of Performance Assessment and Root Cause Analysis (PARCA) is responsible for developing, publishing, and maintaining DoD policy and guidance on EVM. For more information on EVM, refer to the OSD PARCA EVM web site or the EVM Community of Practice web site on the Acquisition Community Connection knowledge sharing system.

11.3.1.1. Earned Value Management (EVM) Applicability

The requirement for EVM applies to cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements that meet the dollar thresholds prescribed in DoD Instruction 5000.02 and DFARS Subpart 234.2 . The application thresholds (total contract value including planned options in then-year dollars) are summarized below:

- $20 million but less than $50 million EVM implementation compliant with ANSI/EIA-748 is required. No formal Earned Value Management System (EVMS) validation is required.
- $50 million or greater EVM implementation compliant with the guidelines in ANSI/EIA-748 is required. An EVMS that has been formally validated and accepted by Defense Contract Management Agency (DCMA) (per paragraph 11.3.1.5) in coordination with, the cognizant contracting officer is required.

The program manager will implement EVM on applicable contracts within acquisition,

upgrade, modification, or materiel maintenance programs, including highly sensitive classified programs, major construction programs, and automated information systems. EVM should also be implemented on applicable contracts wherein the following circumstances exist: (1) the prime contractor or one or more subcontractors is a non-U.S. source; (2) contract work is to be performed in government facilities, or (3) the contract is awarded to a specialized organization such as the Defense Advanced Research Projects Agency (DARPA) . In addition, EVM should be implemented on applicable contracts designated as major capital acquisitions in accordance with Office of Management and Budget Circular A-11, Part 7 , and the Capital Programming Guide .

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements valued at less than $20 million (total contract value including planned options). The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. The program manager is required to conduct a cost-benefit analysis before deciding to implement EVM on these contracts. The purpose of the cost-benefit analysis is to explain the rationale for the decision to require cost/schedule visibility into the contract and to substantiate that the benefit's to the government outweigh the associated costs. If the value of a contract is expected to grow to $20 million or more, the program manager should impose an EVM requirement on the contract.

The application of EVM is not required on contracts, subcontracts, intra-government work agreements, and other agreements less than 12 months in duration, including options. The decision to implement EVM on these contracts is a risk-based decision at the discretion of the program manager. If the duration of a contract is expected to grow to reach or exceed 12 months, the program manager should impose an EVM requirement on the contract.

The application of EVM on Firm-Fixed Price (FFP) contracts, subcontracts, intra-government work agreements, and other agreements is discouraged regardless of dollar value. If knowledge by both parties requires access to cost/schedule data, the first action is to re-examine the contract type (e.g., is a fixed price incentive contract more appropriate). However, in cases where cost/schedule visibility is required, such as for development or integration efforts valued at or greater than $20 million, the program manager is required to obtain a waiver for individual contracts from the MDA. In these cases, the program manager is required to conduct a business case analysis that includes rationale for why a cost or fixed price incentive contract was not the proper contracting vehicle. When possible, the business case analysis should be included in the acquisition approach section of the program acquisition strategy.

If a contract type is mixed, the EVM policy should be applied separately to the different parts (contract types).

For Indefinite Delivery/Indefinite Quantity (ID/IQ) or task order types of contracts, the application of EVM based on dollar threshold is assessed at the computed total contract

value and not by each separate order. To determine EVM applicability, anticipated cost or incentive orders should be summed to reach the computed total contract value. FFP orders are generally not included in that summation.

11.3.1.2. Earned Value Management (EVM) Requirements

The DoD program manager should use Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.234-7001 and 252.234-7002 to place the Earned Value Management System (EVMS) requirement in solicitations and contracts.

The contract should not, either at the time of award or in subsequent modifications, specify requirements in special provisions and/or statements of work that are not consistent with the EVM policy and EVMS guidelines (required by imposition of DFARS 252.234-7002), or which may conflict with offeror's or contractors approved EVM system descriptions. Consult DCMA for guidance on compliance of the contractor's EVMS.

11.3.1.3. Integrated Baseline Reviews (IBRs)

An IBR is a joint assessment of the Performance Measurement Baseline (PMB) conducted by the government program manager and the contractor. The IBR is not a one-time event. It is a process, and the plan should be continually evaluated as changes to the baseline are made (modifications, restructuring, etc.). IBRs should be used as necessary throughout the life of a project to facilitate and maintain mutual understanding of:

- The scope of the PMB consistent with authorizing documents;
- Management control processes;
- Risks in the PMB associated with cost, schedules, and resources; and
- Corrective actions where necessary.

IBRs should be scheduled as early as practicable and the timing of the IBRs should take into consideration the contract period of performance. The process will be conducted not later than 180 calendar days (6 months) after a significant program event or contract change including, but not limited to: (1) contract award, (2) the exercise of large contract options, and (3) the incorporation of major modifications. IBRs are also performed at the discretion of the program manager at any time, even without the occurrence of a major event in the life of a program.

Events that may trigger an IBR include completion of the preliminary design review, completion of the critical design review, a significant shift in the content and/or time phasing of the PMB, or when a major milestone such as the start of the production option of a development contract is reached. Continuous assessment of the PMB will help identify when a new IBR should be conducted with the clause at DFARS 252.234-7002 and DoD Instruction 5000.02 require IBRs on all contracts that require the implementation of Earned Value Management The IBR is not dependent on the

contractor's Earned Value Management System being formally validated as complying with the guidelines in ANSI/EIA-748 . Subcontracts, intra-government work agreements, and other agreements also require IBRs as applicable. The scope of the IBRs should be tailored to the nature of the work effort.

The policy allows for the use of IBRs prior to contract award in situations where they may be appropriate and beneficial. If a program manager elects to conduct a pre-award IBR on a DoD contract, that requirement should be included in the statement of work.

See the NDIA Guide to the Integrated Baseline Review Process(April 2003 version) for additional guidance on IBRs.

11.3.1.4. Contract Performance Management Reporting

11.3.1.4.1. Integrated Program Management Report (IPMR), Formats 1-7

11.3.1.4.2. Integrated Program Management Report (IPMR) Format 6, Integrated Master Schedule (IMS)

11.3.1.4. Contract Performance Management Reporting

The Integrated Program Management Report (IPMR) applies to all contracts that meet the Earned Value Management (EVM) applicability requirements in DoD Instruction 5000.02 . The IPMR combines the CPR (DI-MGMT-81466) and the IMS (DI-MGMT-81650) into a single Data Item Description (DID), DI-MGMT-81861. This new DID was effective as of July 1, 2012. However, for those existing contracts with separate Contract Data Requirements Lists (CDRLs) for the CPR and the IMS, those two DIDs and their content are still contractually applicable. On contracts valued at or greater than $20 million but less than $50 million, it is recommended that IPMR reporting be appropriately tailored. Refer to the IPMR DID Implementation Guide for tailoring guidance. See PARCA EVM Website for the latest version of the guide.

A common, product-oriented Work Breakdown Structure (WBS) that follows the DoD Work Breakdown Structure Standard (MIL-STD-881C) (current version at time of award) is required for the IPMR and the Contractor Cost Data Report (CCDR). Except for high-cost or high-risk elements, the required level of reporting detail should not normally exceed level three of the contract WBS.

The IPMR for all Acquisition Category (ACAT) I programs must be submitted directly to the EVM Central Repository (CR) by the reporting contractors. The EVM CR, which is managed by the PARCA Deputy Director for EVM, is the sole addressee on the Contract Data Requirements Lists for these reports. See the EVM CR Manual for additional guidance on the CR requirements.

All formats shall be submitted electronically in accordance with the DoD-approved

Extensible Markup Language (XML) schemas located in the EVM CR .

11.3.1.4.1. Integrated Program Management Report (IPMR), Formats 1-7

The IPMR provides performance data which is used to identify problems early in the contract and forecast future contract performance. The IPMR should be the primary means of documenting the ongoing communication between the contractor and the program manager to report to date cost and schedule metric trends and to permit assessment of their effect on future performance.

The program manager obtains an IPMR on all cost or incentive contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $20 million. The IPMR is not typically required for cost or incentive contracts valued at less than $20 million, contracts less than 12 months in duration, or Firm-Fixed Price contracts for production efforts.

Data Item Description (DID) DI-MGMT-81861 (current version at time of award URL: https://assist.dla.mil/quicksearch/basic_profile.cfm?ident_number=278901) is used to obtain the IPMR. The contracting officer and contractor should negotiate reporting provisions in the contract, including frequency and selection of formats, level of detail, submission dates, variance thresholds and analysis, and the Work Breakdown Structure to be used. The program manager should tailor the IPMR, via the contractual CDRL, to the minimum data necessary for effective management control on contracts valued at less than $50 million. In exceptional cases, the contractor may determine that the performance measurement baseline (PMB) or existing contract schedule cannot be achieved and no longer represents a reasonable basis for management control. With government approval, the contractor may implement an Over Target Baseline (OTB) or Over Target Schedule (OTS). For cost-reimbursement contracts, the contract budget base excludes changes for cost growth increases, other than for authorized changes to the contract scope. The OTB/OTS creates additional budget to complete in-scope work, but it does not increase the negotiated contract cost.

11.3.1.4.2. Integrated Program Management Report (IPMR) Format 6, Integrated Master Schedule (IMS)

The IMS is an integrated and networked multi-layered schedule of program tasks required to complete the work effort captured in a related Integrated Master Plan (IMP). The IMS is traceable not only to the IMP but also the contract Work Breakdown Structure, and the statement of work. The IMS is used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components.

Data Item Description DI-MGMT-81861 (current version at time of award) Format 6 is used to obtain the IMS. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail, submission dates, and frequency of the schedule risk analysis. The program manager should tailor the IMS to the minimum

data necessary for effective management control on contracts valued at less than $50 million.

11.3.1.5. Earned Value Management System (EVMS) Compliance, Validation, and Surveillance

11.3.1.5.1. Earned Value Management System (EVMS) Compliance and Validation

11.3.1.5.2. Earned Value Management System (EVMS) Surveillance

11.3.2. Contract Funds Status Report (CFSR)

11.3.1.5. Earned Value Management System (EVMS) Compliance, Validation, and Surveillance

The Defense Contract Management Agency (DCMA) has responsibility for EVMS compliance, validation, and surveillance for the Department of Defense, except for those DoD Components that are also part of the Intelligence Community (IC) and are excluded from the requirement to delegate EVMS authorities to DCMA.

11.3.1.5.1. Earned Value Management System (EVMS) Compliance and Validation

DCMA, or the applicable Intelligence Community Component, will perform EVMS compliance and/or validation reviews, as necessary, at each contractor awarded a contract requiring EVM compliance or validation. The contractor demonstrates EVMS compliance through the use of management processes and program reporting that are consistent with the guidelines in ANSI/EIA-748. The requirement for EVMS validation is mandated only for those contracts, subcontracts, intra-government work agreements, and other agreements valued at or greater than $50 million.

Validation is achieved by conducting a formal review of the processes defined and used by the contractor to manage major acquisitions that assesses the capability of the contractor's proposed system to comply with the EVMS guidelines in ANSI/EIA-748. It determines that the contractor is using the system as one of its primary program management processes; that the contractor has properly implemented the system on the contract; and that the contractor is using the data from its system in reports to the government. See the DCMA EVMS Compliance Review Instruction for additional guidance on EVMS compliance and validation.

11.3.1.5.2. Earned Value Management System (EVMS) Surveillance

Surveillance is required for all contract efforts that require the implementation of an EVMS, regardless of whether a formal system validation is required. For the life of the contract, surveillance will be conducted on a recurring basis and should evaluate both the continuing capability of the contractor's EVMS and the validity of the internal and external performance information generated by the system. The results of surveillance

efforts should be documented and identified deficiencies should be monitored and corrected. The responsibility and requirement for government surveillance of contracts should be based on the effectiveness of the contractor's implementation of internal management controls. See the Defense Contract Management Agency (DCMA)'s surveillance process for additional guidance on surveillance activity where applicable.

The Navy Supervisors of Shipbuilding have the authority to conduct EVMS surveillance activities, issue Advance Agreements, approve EVM processes, and the responsibility to coordinate with DCMA for the contracts under their cognizance. EVM system validation reviews and reviews for cause are the responsibility of DCMA in coordination with the contracting officer.

11.3.2. Contract Funds Status Report (CFSR)

The CFSR described in this section applies to many defense contracts. It helps to ensure effective program management and supplies funding data about defense contracts to program managers for:

- Updating and forecasting contract funds requirements;
- Planning and decision making on funding changes in contracts;
- Developing funds requirements and budget estimates in support of approved programs;
- Determining funds in excess of contract needs available for deobligation;
- Obtaining rough estimates of termination costs; and
- Determining if sufficient funds are available by fiscal year to execute the contract.

The program manager will obtain a CFSR (DD Form 1586) on contracts over 6 months in duration. The CFSR has no specific application thresholds; however, the program manager should carefully evaluate application to contracts valued at less than $1.5 million (in then-year dollars).

DID DI-MGMT-81468 (current version at time of award) is used to obtain the CFSR. The contracting officer and contractor should negotiate reporting provisions in the contract, including level of detail and reporting frequency. The program manager should require only the minimum data necessary for effective management control. The CFSR should not be applied to Firm-Fixed Price contracts unless unusual circumstances dictate specific funding visibility.

The CFSR for all Acquisition Category I programs is submitted directly to the Earned Value Management Central Repository (CR) by the reporting contractors. The CR will be the sole addressee on the CDRL for this report. See the EVM CR Manual for additional guidance on the CR requirements.

The use of a standard electronic data exchange format is required for all reports unless disclosure of this information would compromise national security. All data will be in a readable digital format (e.g., PDF files are not acceptable). The Extensible Markup

Language standard (Project Schedule Cost Performance Management message) is the preferred format. The American National Standards Institute X12 standard (839 transaction set) is also acceptable. On-line access to the data may be provided to augment formal submission.

11.3.3. Quality Management

According to American National Standards Institute (ANSI), International Organization for Standardization (ISO), and American Society for Quality (ASQ), international standard ANSI/ISO/ASQ Q9000-2005 (ISO 9000), Quality Management Systems-Fundamentals and Vocabulary:

- Quality is the degree to which a set of inherent characteristics fulfills requirements. It may apply to a product or process. Inherent characteristics may be physical, sensory, behavioral, temporal, ergonomic, functional, etc.
- Quality management represents the organized activities to direct and control an organization with regard to quality.
- Quality assurance is the part of quality management focused on providing confidence that quality requirements will be fulfilled.

Effective quality management activities are important for reducing process-related risks to programs. Such risks include:

- Ill-defined or omitted requirements;
- A breakdown in requirements flow down;
- Uneconomically producible designs as a result of inappropriate application of technical processes;
- Inadequate procedures to implement contract requirements;
- Suppliers with inadequate capabilities;
- Decreasing leverage with sub tiers as a result of ineffective supplier management;
- Dissatisfied customer's as a result of ineffective customer engagement; and/or

- Undetected product defects resulting from unidentified verification technologies or failure to implement existing ones.

If not managed and mitigated, these risks may start a chain of events leading to undesirable outcomes such as:

- Product defects discovered in production or testing that may require expensive and time-consuming rework
- Products that may not meet customer needs
- Product deficiencies discovered in the field that may lead to degraded mission effectiveness, early wear out or mishaps
- Cost overruns or delays for current contracts and
- Cost escalation for future contracts
- Parts shortages at the wholesale and retail levels

The later these risks are identified, the greater the cost of corrective action and the greater the delays in schedule. Early identification, management, and mitigation of important process-based risks to a program lead to less expensive and less disruptive corrective actions that break the chain of undesirable outcomes.

While the DoD program manager should encourage and support the contractor's efforts to assure quality, ultimately, the prime contractor is responsible. Therefore, from a DoD perspective, a key program success factor is selecting contractors that can demonstrate effective quality management. This subject is discussed in section 11.3.3.1 .

The contract should provide incentive to the contractor to deliver products or services that provide value beyond the basic requirement. Without additional incentives, the systems engineering process will normally lead to decisions that satisfy requirements at the lowest cost. It may however be possible to incentivize the contractor to (1) exceed a basic requirement such as mean time between failures or (2) generate a higher level for an important derived requirement (e.g., one that affects operational flexibility, maintainability, supportability, etc.). Section 11.3.3.2 discusses this topic.

Applying best practices as described in Sections 11.3.3.1 and 11.3.3.2 may not be sufficient to manage and mitigate the process-based risks list above. Section 11.3.3.3 discusses how encouraging a quality focus can also contribute.

Government Contract Quality Assurance (GCQA) determines if contractual requirements have been met prior to acceptance of supplies and services. GCQA is conducted by the program manager and Defense Contract Management Agency (DCMA) as identified in contract administration delegations to DCMA by the Contracting Officer. Section 11.3.3.3 discusses some best practices for setting quality assessment and oversight requirements for the GCQA function, tailored to the expected risks.

11.3.3.1. Differentiating Among Offeror's on the Basis of Quality

A contractor's quality management system is used to direct and control the organization with regard to quality. Quality management is an enterprise level process, driven by senior leadership involvement, to support the delivery of high quality products and services by ensuring that all aspects of quality are considered and acted upon by every element of the organization. The fundamental goal is to provide objective insight to assure that: customer requirements are thoroughly analyzed and understood; processes are defined and capable; and the resulting product meets the customer's needs. It interacts with systems engineering technical processes and technical management processes by focusing on both the quality of the system and the quality of the processes being used to create the system. Quality management provides objective insight into processes and work products for all stakeholders including program team members, management, suppliers, customer's, and users involved with the development, manufacture, operation, and support of a system.

The quality management process begins early in the life cycle and continues throughout. The principal elements of the quality management process include:

- Objectively evaluating performed processes, work products, product/process design and services against the applicable process descriptions, standards, procedures, policies, and documented expectations;
- Understanding the full scope of customer requirements, assessing risks associated with meeting those requirements, and verifying that they are satisfied;
- Identifying and documenting noncompliance issues, especially those affecting cost, schedule, productivity, and performance;
- Using tools and techniques in a disciplined manner to determine root causes of noncompliance issues;
- Addressing noncompliance issues by initiating and tracking corrective and preventative actions to assure the root cause(s) of the defect/deficiency has been identified and removed; and
- Providing feedback to program managers, their staff, and corporate managers to identify lessons learned, improve process robustness for future projects, and evaluate trends.

While the quality management focus is on the key aspects of the product realization process (e.g., requirements, design, make/buy decisions, supplier management, production), it also encompasses supporting processes such as contracting and training. Both value-added activities and continuous process improvement should be stressed and encouraged.

Further information about quality management may be found in ISO 10005 Quality Management - Guidelines for Quality Plans (available for purchase), AQAP-2000 NATO Policy on an Integrated Systems Approach to Quality through the Life Cycle, AQAP-2009 NATO Guidance on the Use of the AQAP 2000 Series, and at Process and Product Quality Assurance in the CMMI for Development (CMMI-DEV) v1. 2 or the

CMMI for Acquisition (CMMI-ACQ) v1.2.

Program managers should allow contractors to define and use their preferred quality management system as long as it meets the needs of the program. International quality standard ISO 9001-2008, Quality Management Systems - Requirements, AQAP-2110, NATO Quality Assurance Requirements for Design, Development and Production, and AS 9100C:2009, Aviation, Space and Defense Quality Control Management System Standard, define process-based quality management systems and are acceptable for use on contracts per FAR 46.202-4, Higher-Level Contract Quality Requirements . AQAP-2110 and AS 9100 contain additional requirements beyond ISO 9001. AS 9100 is applicable to most complex DoD systems. The AQAP 2000 series should be considered for complex DOD systems, when the supply chain or the end products have NATO or international implications. Program managers should consider the use of additional requirements (such as those contained in the Missile Defense Agency Assurance Provisions) beyond ISO 9001 as appropriate.

Other sector specific quality management systems acceptable under FAR 46.202-4 include:

- TL 9000, Quality System Requirements for the telecommunications industry
- ISO/IEC 90003:2008 , Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software (available for purchase)
- QS-9000 or ISO/TS 16949:2009 (available for purchase), ISO 9000 harmonized standards for automotive suppliers of production materials and service parts in North America

To improve a contractor's quality management system, standards bodies encourage registration based upon an impartial third party evaluation. The Department of Defense does not require registration of a contractor's quality management system because registration does not guarantee product or service quality. Reasons why the Department of Defense does not require registration include the following:

- Registrars (auditors) do not look at the product;
- There have been instances where a registered contractor delivered a deficient product;
- Many companies pursue registration of their quality management system as a goal in itself or as a marketing tool; and
- Some registrars are less demanding.

Compliance to a standard such as ISO 9001 (available for purchase), AQAP-2000, AQAP-2009 , or AS 9100, does not, in itself, guarantee product or service quality. These standards are management system standards that identify requirements for processes within an organization, describe expected tasks and outcomes, and explain how the processes and tasks integrate to produce required inputs and outputs. Standards are meant to enable the organization to develop a set of processes that, if done by qualified persons using appropriate tools and methods with appropriate

leadership involvement, will enable a capability for delivering high quality products or services.

Product or service quality is achieved through the implementation of a strategic plan to integrate all business and technical functions that result in the consistent application of proven, capable processes within an organization. Managers must ensure that all management systems are working toward the same goals and are not creating conflicting or dysfunctional behavior. Implementing a standard is of little use if the financial system rewards individuals for delivering non-conforming products/services. Because everything a contractor does should be related to the quality of its products or services, a contractor's quality management system should be the basis for integrating all other management systems within an enterprise. Therefore, include quality management as a selection factor and look for the following elements of a quality management system in proposals:

- Effective policies and procedures that encourage the use of the system;
- Organizations with defined authorities and responsibilities;
- Objectives to drive people, processes, and the system;
- Method to analyze and resolve quality problems;
- Metrics that reflect desired outcomes;
- Interacting processes to transform inputs into outputs; and
- Records as evidence of what happened.

Furthermore, to the extent that they are available, metrics that show the effectiveness of the contractor's quality management system and processes over time should also be used to differentiate among offeror’s.

The following subsections describe several broad areas that have had a significant impact on quality. Topics include Customer Satisfaction , Supply Chain Quality Management , Top Management Involvement , and Continual Improvement of Performance . They provide additional guidance on items the program office and the contracting office should ask for in Requests for Proposals and evaluators should look for in proposals to make a better assessment of a contractor's quality. These items may be used to differentiate among offeror’s. Depending on the specific situation, there may also be other areas (e.g., competent personnel for special processes) where information should be sought.

11.3.3.1.1 Customer Satisfaction

Customer satisfaction, when quantified, is a valuable enterprise-level outcome metric. The Department of Defense has recognized the importance of customer-satisfaction performance measures. Since the passage of the Federal Acquisition Streamlining Act of 1994, all Federal Departments and Agencies have initiated procedures to record contractor performance on in-process contracts and to use past contractor performance information in source selection.

Too often in the past, the Department of Defense relied heavily upon detailed technical and management proposals and contractor experience to compare the relative strengths and weaknesses of offers. This practice often allowed offeror's that could write outstanding proposals, but had less than stellar performance, to "win" contracts even when other competing offeror's had significantly better performance records and, therefore, represented a higher probability of meeting the requirements of the contract. Emphasizing past performance in source selection, can help ensure that the winning teams (prime contractors and major subcontractors) are likely to meet performance expectations. When evaluating past performance data, consideration should be given to the relevancy, complexity and ultimate mission success of the contract.

Beyond the Department's past performance information, a Request for Proposals may ask for further evidence of customer satisfaction such as data tabulated from customer surveys or from complaints and equally important, how changes were made because of the results.

Supplier assessment programs may also be helpful in understanding how well a company is able to satisfy its customer's. Suppliers have demonstrated some degree of customer satisfaction when they are accredited by a group of companies, in a particular sector, that joined together to agree on criteria and a process for assessing, exchanging and publishing supplier data to facilitate business relationships. For example, Nadcap is a worldwide cooperative program of major companies designed to manage a cost effective consensus approach to special processes and products and provide continual improvement within the aerospace industry; the Coordinating Agency for Supplier Evaluations (C.A.S.E.) exchanges and publishes non-prejudicial supplier data to help make informed supplier selections. Reports from consumer organizations or the media may also be useful.

11.3.3.1.2 Supply Chain Quality Management

Because quality deficiencies for non-commercial-off-the-shelf (COTS) products often occur in the lower tiers, prime contractors should have insight at least two levels down their supply chain. Prime contractors, in addition to having approved vendor (i.e., subcontractor) lists, should ask their subcontractors' about planned suppliers. These subcontractors should also have insight two levels down their supply chain and flow the same requirement down to their suppliers, etc. For COTS products, all contractors should use approved sources.

It is important for DoD program managers to inform their prime contractors of their interest in quality throughout the supply chain. Therefore, through requests for proposals and corresponding proposal evaluation factors, the program office and the contracting office should request and evaluate evidence of effective supply chain management. The evidence should reflect the following characteristics:

- Relationships with suppliers that promote and facilitate communication to improve the effectiveness and efficiency of processes that add value;

- The use of supplier development programs focused on continuous improvement;
- Strategic partnerships with suppliers, over the product life cycle, that are based on a clear understanding of the partners' and customer's' needs and expectations in order to improve the joint value proposition of all stakeholders;
- Processes that effectively and efficiently monitor, evaluate, verify, and improve the suppliers' ability to provide the required products with a focus on defect prevention rather than defect detection;
- Right of access for both the prime contractor and the Government to supplier facilities and documentation where applicable; and
- Requirements for the supplier to flow down analogous quality management system provisions to its subcontractors.

Because quality deficiencies often occur in the lower tiers, prime contractors, in addition to having approved vendor (i.e., subcontractor) lists, should ask their subcontractors' about planned suppliers. These subcontractors should flow the same requirement down to their suppliers, etc. For critical and complex commercial-off-the-shelf (COTS) products, the prime and its subcontractors should use their own internal processes and controls to ensure that the COTS product meets it's critical attributes.

11.3.3.1.3 Top Management Involvement

Quality will permeate all levels of a company only if top management provides the leadership necessary to drive and reinforce that behavior. Requests for Proposals should also ask for evidence of top management support for quality. The following list identifies important factors in evaluating the effectiveness of top management support:

- Establishing a corporate strategic vision, objectives, policies and procedures that reflect a commitment to quality both in-house and in suppliers' facilities;
- Communicating, at every opportunity, organizational direction and values regarding quality;
- Providing structures and resources to support full implementation of a quality management system;
- Soliciting quantitative and qualitative feedback on the effectiveness and efficiency of quality management and taking actions based on that feedback, even when change may be difficult;
- Establishing a quality policy, at the highest level in the company, that commit's to continuously improving processes and exceeding customer expectations;
- Reviewing the quality management system periodically with particular attention paid to achieving goals and objectives throughout the organization, customer satisfaction, and the exchange of ideas for continuous improvement;
- Setting ambitious quality objectives and promulgating them through quality policy;
- Demonstrating importance put on quality functions by providing for independent reporting channels; and
- Establishing management accountability with emphasis on quality results and

customer satisfaction.

11.3.3.1.4 Continual Improvement of Performance

An offeror with effective quality management will seek continual improvement of its processes, product designs, and thereby products by improving its overall performance, efficiency, and effectiveness. Such behavior increases the likelihood of increasing customer satisfaction and enhancing an organization's competitive posture.

More specifically, all processes have defined inputs and outputs as well as the required activities, actions and resources. Therefore, process improvement encompasses both:

1. Improving conformance to the defined process and
2. Improving the defined process itself to add value and eliminate waste.

Such process improvement invariably leads to (work and end) product improvement and consequently increased customer satisfaction.

When asking for evidence of a strong commitment to continual improvement in a request for proposal, the following list provides considerations for evaluating a response.

- How conditions are created to promote innovation,
- How open two-way communications are encouraged,
- How corrective actions are treated as an improvement tool,
- How change is approached on a systematic, consistent basis, to include follow-through implementation, verification and documentation,
- How people are provided with the authority, technical support and necessary resources for change,
- How continuous improvement process tools are deployed company-wide,
- How self-assessments, benchmarking, competitor analysis, and other metrics are used to evaluate process performance and drive improvement, and
- How capability and maturity models or reviews support an effective continual improvement process and provide both insights to the improvement process itself and objective evidence of success.

11.3.3.2 Incentivizing Higher Quality in Contracts

Contract incentives can be structured to ensure quality by contributing to the contractor's value proposition. Factors that are typically important aspects of a contractor's value proposition include:

- Customer satisfaction;
- Planning stability;
- Good financial performance; and

- Improved cash flow.

Listed below are examples of contract incentives that can be made available to the prime contractor and the prime contractor can in turn make available to subcontractors under the appropriate conditions:

- Increased fee;
- Extended contract length;
- Follow-on contracts awarded;
- Accelerated progress payments;
- Shared savings; and
- Opportunities for return on investments (some of which may increase the contractor's competitiveness on other contracts).

The following are some potential ways to use these contract incentives to improve quality, and at the same time, improve other product characteristics that are of value to DoD. Their applicability depends on the specific situation.

- Warranties. The program manager could treat the warranty as a fixed price option per item. If there are no failures, the contractor keeps the money that DoD paid for the warranty. To reduce the price of the warranty, the program manager could consider a situation where DoD pays to repair the first failure and the contractor warranties the next "n" failures. Typically the warranty should exclude combat damage, abuse, misuse, and other factors out of the contractors' control.
- Award Fee for Product Support Contracts. The program manager could make the fee a function of operational availability.
- Award Fee for Product Development Contracts. The program manager could make the fee a function of successful operational test and evaluation.
- Progress Payments. The program manager could make payments contingent on successful corrective actions taken to alleviate quality deficiencies. The program manager could also establish an agreement with the contractor to repay the fee with interest if future measurements do not meet the conditions necessary for the entire amount of the fee to be awarded.
- Share of Savings. The contract could encourage the contractor to invest in facilities, non-recurring engineering, technology insertion, etc. that will result in improved performance and reduced costs. The program manager could then use the value engineering clause to repay the investment and give the contractor a share in the savings generated.

In building such relationships, the program manager should avoid actions that encourage risky behavior by the contractor. For example, by insisting on reducing cost, accelerating the schedule, improving performance beyond demonstrated technology limit’s, etc. the contractor may be forced to forgo quality-related processes. This may not only defeat the purpose of contractual incentives but also negate the other quality activities discussed in this section.

11.3.3.3 Encouraging a Quality Focus

11.3.3.3 Encouraging a Quality Focus

Applying best practices as described in sections 11.3.3.1 and 11.3.3.2 may not be sufficient to manage and mitigate process-based risks that may start a chain of events leading to undesirable outcomes. DoD should also stress the importance of effective quality management to industry. By encouraging a quality focus, DoD can help avoid mismatches among value, beliefs, and behaviors. DoD should therefore encourage and participate with industry to apply effective practices in the following areas.

At Program Startup

- The process for establishing the product or project quality budget,
- Where quality responsibility is placed in the program,
- How quality skills have been assigned to the project,
- The process for analyzing quality requirements and mitigating associated risks, and
- The quality strategy's consistency with industry best practices.

Throughout the Life Cycle

- How management uses quality data,
- The contractor's approach for continuous process improvement,
- The contractor's approach for preventive and corrective action, and
- The contractor's approach for achieving customer satisfaction.

Evaluation considerations for each of the above areas are shown below:

- The process for establishing the product or project quality budget,
- Project quality administration, product verification, quality engineering (hardware and software), quality planning, and supplier quality,
- Specific quality deliverables,
- Capital, equipment, and software verification needs,
- How the estimates are modified when there are changes to the strategy and/or scope of the program, and
- Measurement technology needs.

Where quality responsibility is placed in the program:

- Role in the general risk identification, classification, and mitigation process,
- Involvement in the design change control and release process,
- Role in processing waivers, deviations and engineering change proposals,
- Representation on Integrated Process Teams and boards (e.g., change control board, risk) for all product and process development activities,
- Involvement in test plans, material reviews, design reviews, build/buy/support to

packages,
- Participation in the integration of inspection points into processing and test documentation, and
- Role in the supplier management, development, incentivization, and control process.

How quality skills have been assigned to the project

- The process to identify the need for quality management, quality engineering (hardware and software), quality planning, supplier quality, and product verification skills across the life cycle,
- The process to identify quality skills and any associated certifications and qualifications, and
- The process for addressing quality staffing ratios and skill shortfalls.

The process for analyzing quality requirements and mitigating associated risks:

- The process for identifying and achieving quality tasks in support of contract deliverables,
- How a post award contract analysis for Quality's tasks was performed / has been updated,
- An evaluation of how the Quality plan matches the program requirements and their integration across program sites, IPTs, partners and suppliers, and
- How quality activities factored into the Integrated Master Plan and Integrated Master Schedule.

The quality strategy's consistency with industry best practices:

- The use of lessons learned,
- How similar programs' quality past performance have been reviewed,
- How the quality plan addresses program unique processes,
- How plans include verification approaches, nonconformance handling, operator verification manufacturing self-examination, nondestructive inspection, manufacturing systems, measurement approach, special measuring and test equipment,
- Adequacy of the quality plan to address all other program plans (manufacturing, systems engineering, subcontract management, delivery, etc.),
- Periodic review and update, and
- Early involvement in the program.

How management uses quality data

- Audit needs and addressing audit findings,
- The process for analyzing and performing trend analysis of internal/external audit findings, and
- How quality is defined, measured, analyzed, controlled, and used to drive

management decisions and actions on the program
    - The process for developing and identifying requirements for quality metrics and measurement systems
    - The system for monitoring supplier performance, including their product development activities
    - The process for review and update

The contractor's approach for continuous process improvement:

- Baldridge business model,
- CMMI,
- Lean,
- Six sigma,
- ISO recertification, and
- Actions taken to address feedback from assessments performed.

The contractor's approach for preventive and corrective action:

- The process for addressing test and inspection findings and discrepancies,
- The process for addressing supplier non-conformances,
- Establishment and maintenance of a closed loop corrective action system that includes the reporting, root cause analysis, and implementation of actions necessary to correct and preclude recurrence of problems, failures, quality issues, defects/non-conformances, and
- The process for using lessons learned to drive continuous improvement.

The contractor's approach for achieving customer satisfaction:

- The process to collect, monitor, and analyze information for measuring customer satisfaction,
- The process to rapidly mitigate customer concerns,
- The process to communicate with customer's at all levels, and
- The process / organizational structure for reacting to customer inquiries and needs.

The program managers and responsible technical authority will utilize DoD preferred method of acceptance as reflected in MIL-STD-1916 , *DoD Preferred Method of Acceptance* , (login, then URL: https://assist.daps.dla.mil/online/parms/mainframe.cfm?ident_number=120287), to allow contractors the maximum degree of flexibility to meet product or service requirements. The preferred method is acceptance by contractor-proposed provisions based on prevention-based strategies and process controls. The theme is partnering between Government and contractor to develop an optimal acceptance method for products and services that is consistent with the contract requirements for submission of all conforming products or services.

Prior to achieving effective prevention-based strategies and process controls, MIL-STD-1916 provides standardized acceptance sampling systems which are consistent with the contract requirements for submission of all conforming products or services. These sampling systems allow program managers to influence continuous improvement through corrective action while still allowing maximum degree of flexibility to contractors.

International quality standard ISO 21247, *Combined Accept-Zero Sampling Systems and Process Control Procedures for Product Acceptance* , (available for purchase) is an acceptable alternative to MIL-STD-1916.

11.3.3.4. Government Contract Quality Assurance (GCQA)

11.3.3.4.1. Formulating the Government Contract Quality Assurance Approach

11.3.3.4.2. Government Contract Quality Assurance (GCQA) Inspections

11.3.3.4.3. Government Contract Quality Assurance (GCQA) for Critical Safety Items (CSIs)

11.3.3.4. Government Contract Quality Assurance (GCQA)

GCQA is a joint responsibility between the program office and Defense Contract Management Agency (DCMA). Interdisciplinary skills (such as quality assurance, industrial specialist, engineering, and software) are needed.

The program manager should establish open and effective communication with DCMA. DCMA uses Contract Data Package Recommendation/Deficiency Reports (DD Form 1716) for the following:

- To improve contract data packages;
- When essential information is required as a basis for inspection/acceptance or shipment is incorrect, incomplete, unclear or unavailable; or
- When there is a conflict, ambiguity, noncompliance or other problem area between the contractor and Government concerning contractual requirements.

The DD Form 1716 is an important avenue of communication for DCMA to resolve contractual issues with the Procuring Activity and to understand and meet expectations and needs of their customer's.

For item-managed contracts, Defense Logistics Agency ICPs issue Quality Assurance Letters of Instruction to DCMA to provide additional contractor past performance history and to request tailored or specialized surveillances during contract performance.

11.3.3.4.1. Formulating the Government Contract Quality Assurance Approach

For defense acquisition programs, the program manager should conduct a customer

outcome strategy meeting (i.e., a post award conference) soon after the Systems Development and Demonstration contract award. At this meeting, the participants should:

- Identify desired customer/user expectations and outcomes,
- Determine the program risks that may negatively impact those outcomes,
- Analyze those risks to assess the potential consequences, and
- Define performance measures associated with the desired outcomes.

The program manager should ensure that some of these performance measures relate to key processes in the acquisition framework. For example, the performance measures should be linked to the entrance and exit criteria of the systems engineering technical reviews and the Milestone programmatic reviews during both the Systems Development and Demonstration Phase and the Production and Deployment Phase of the acquisition management framework.

The program manager should form a GCQA team and allow it the flexibility to formulate a risk-based quality assurance surveillance strategy designed to ensure that customer outcomes are achieved. The surveillance strategy should focus on the effectiveness of the contractor's product realization process which includes:

- Planning of Product Realization;
- Customer-Related Processes;
- Design and Development;
- Purchasing and Supplier Management;
- Production and Service Provision;
- Control of Monitoring and Measuring Devices; and
- Inspection, Test, Verification and Validation.

The surveillance strategy should also cover the contractor's continual improvement process. To be effective, this process should be data driven and the data should (1) be used to address both actual and predicted problems, and (2) should be revised to remain connected to process changes. In addition, include both periodic audits of the contractor's quality management system as well as product examinations in the surveillance strategy. Both independence and the use of criteria in conducting audit’s and surveillance are critical to providing objective, meaningful insight.

As performance data are collected, the GCQA team should adapt the surveillance strategy based on risks identified and the need for special surveillance of critical safety items, critical characteristics or processes, mission critical items, key characteristics, etc. When planned results are not achieved, the program manager should ensure that preventive and corrective actions are developed and implemented. The GCQA team should extend the surveillance to verify that such actions accomplished their objectives.

11.3.3.4.2. Government Contract Quality Assurance (GCQA) Inspections

For item-managed contracts, detailed guidance on when to require GCQA at source or destination is contained in the Federal Acquisition Regulation (FAR), Part 46 .

Per FAR Parts 46.402 and 46.404, the program manager shall use destination inspection for contracts or purchase orders under $250,000 for the reprocurement of items with no significant technical requirements, no critical characteristics, no special features, and no specific acquisition concerns, and where there is confidence in the contractor. Such inspections are limited to kind, count and condition. This may involve preservation, packaging, and marking (if applicable). Put FAR 52.246-1 on the contract. Use FAR 52.246-2 without FAR 52.246-11 only in those rare circumstances where there is reason to believe that there may be a problem.

Typically, source inspection is appropriate for complex / critical items where:

- The verification of technical characteristics requires in-process controls;
- Product quality cannot be adequately determined through basic end item product examination; or
- The contractor is experiencing or exhibiting difficulty controlling product characteristics.

The program manager should put both FAR 52.246-2 and FAR 52.246-11 (or FAR 52.246-8 for research and development programs) on the contract. FAR 52.246-2 allows Government access to the facility and requires the contractor to develop and maintain an inspection system. FAR 52.246-11 requires the contractor to implement a higher level quality management system. The responsible technical authority should prepare a Quality Assurance Letter of Instruction through the contracting officer to ensure that appropriate product specifications, drawings, and inspection and test instructions, including critical characteristics, are available and/or identified for use by the Defense Contract Management Agency. GCQA at the source encompasses one or more of the following based on defined risk:

- *Product Examinations:* Examinations of product characteristics to ensure they meet contract requirements. Depending on the identified risks, the Government CQA surveillance strategy might include various product examination techniques, such as inspecting, testing, witnessing, verifying by use of objective evidence, and analyzing Government or contractor performance data.
- *Process Reviews:* Reviews to determine the suitability, adequacy, and effectiveness of the process to achieve product outputs that meet contract requirements.
- *System Assessments/Audit's:* Systematic, independent assessments and audits of the various elements of the contractual quality management system impacting process or product quality.
- *Management and program reviews and meetings:* Maintains open channels of

communication.

11.3.3.4.3. Government Contract Quality Assurance (GCQA) for Critical Safety Items (CSIs)

Special attention must be paid to CSIs regardless of whether they are item-managed or program-managed. Defense Federal Acquisition Regulation Supplement (DFARS) 246.103 states that the activity responsible for technical requirements may prepare instructions covering the type and extent of Government inspections for acquisitions that have critical applications (e.g., safety) or have unusual requirements. Section 4.3.18.6 discusses CSIs as a systems engineering design consideration. It provides a definition and links to some additional reference material.

The contracting officer should clearly mark the front page of the solicitation/contract with the words "Critical Safety Item." This raises the alertness level and makes everyone aware that CSIs are involved in the contract. When CSIs are determined after contract award, the responsible technical authority should use the words "Critical Safety Items" in the subject line of a Quality Assurance Letter of Instruction (QALI). All critical and major characteristics, the extent of inspection required, and the associated acceptance criteria should be described either in the contract or in the QALI. In addition, the technical authority should provide criteria for special inspections, process verification, or similar requirements. Acceptance criteria should also include additional instructions for situations where a CSI is purchased from a distributor, a CSI is purchased on a commercial contract, or CSI critical characteristics cannot be fully examined at a prime contractor's facility. To assure the communications loop is closed with Defense Contract Management Agency (DCMA), the QALI should request acknowledgement and DCMA acceptance of duties included within. The form should be returned to the responsible technical authority that transmitted the QALI.

Public Law 108-136, "National Defense Authorization Act for FY04," Section 802, Quality Control in the Procurement of Aviation Critical Safety Items and Related Services, " requires that the head of the design control activity for aviation critical safety items establish processes to identify and manage the procurement, modification, repair, and overhaul of aviation critical safety items." DoD procedures for managing aviation CSIs are contained in Joint Service instruction, " Management of Aviation Critical Safety Items ," and the Joint Aeronautical Logistics Commanders' Aviation Critical Safety Items (CSIs) Handbook . Additionally, per DFARS 246.407, the head of the design control activity is the approval authority for acceptance of any nonconforming aviation critical safety items or nonconforming modification, repair, or overhaul of such items.

DCMA relies on the Procuring Activity's knowledge and involvement to determine whether an item is correctly categorized as a critical item. If DCMA questions the critical categorization of an item, the lack of a critical characterization of an item, or a CSI designation, DCMA will contact the Procuring Office to discuss the reasons behind the decision, gain a better understanding of the situation or customer’s needs, and request additional information. The Procuring Office should contact DCMA personnel whenever

they have a concern, question, or possess additional information important to achieving customer outcomes.

11.4. Knowledge-Based Acquisition

11.4. Knowledge-Based Acquisition

Knowledge-based acquisition is a management approach which requires adequate knowledge at critical junctures (i.e., knowledge points) throughout the acquisition process to make informed decisions. DoD Directive 5000.01 calls for sufficient knowledge to reduce the risk associated with program initiation, system demonstration, and full-rate production. DoD Instruction 5000.02 provides a partial listing of the types of knowledge, based on demonstrated accomplishments, which enable accurate assessments of technology , design maturity , and production readiness .

Implicit in this approach is the need to conduct the activities that capture relevant, product development knowledge. And that might mean additional time and dollars. However, knowledge provides the decision maker with higher degrees of certainty, and enables the program manager to deliver timely, affordable, quality products.

The following knowledge points and ensuing considerations coincide with decisions along the acquisition framework:

Program Initiation . Knowledge should indicate a match between the needed capability and available resources before a program starts. In this sense, resources is defined broadly, to include technology, time, and funding.

Considering the knowledge associated with technology, the knowledge should be based on demonstrated accomplishments. If a technology is not mature, the DoD Component must use an alternative technology or discuss modifying requirements with the users. By requiring proven technology before a program starts, we reduce uncertainty. Rather than addressing technology development and product development, the program manager and Milestone Decision Authority can focus on product development, because they know the technology is available. DoD Instruction 5000.02 enforces this concept with the following policy:

Technology developed in S&T or procured from industry or other sources shall be assessed to determine whether they are considered mature enough to use for product development *(see the "Technology Readiness Assessment (TRA) Guidance). . . . If technology is not mature, the PM shall use alternative technology that is mature and that can meet the user's needs or conduct a dialog with the user to modify the requirements. Technology readiness assessments shall be conducted* by the PM and used by the MDA to assist in determining whether program technologies have acceptable levels of risk based in part on the degree to which they have been demonstrated, including demonstration in a relevant environment, and to support risk mitigation plans prepared by the PM. They will be focused on the specific planned technical solution.

Post-Critical Design Review Assessment . Knowledge should indicate that the product can be built consistent with cost, schedule, and performance parameters. This means design stability and the expectation of developing one or more workable prototypes or engineering development models. DoDI 5000.02 lists the specific factors that contribute to such knowledge.

Production Commitment . Based on the demonstrated performance and reliability of prototypes or engineering development models, knowledge prior to the production commitment should indicate the product is producible and meets performance criteria. DoD Instruction 5000.02 lists some of the specific factors that contribute to such knowledge.

Full-Rate Production Decision . Based on the results of testing initial production articles and refining manufacturing processes and support activities, knowledge prior to committing to full-rate production should indicate the product is operationally capable; lethal and survivable; reliable; supportable; and producible within cost, schedule, and quality targets.

11.5. Technical Representatives at Contractor Facilities

11.5. Technical Representatives at Contractor Facilities

Program managers should maximize the use of Defense Contract Management Agency (DCMA) personnel at contractor facilities. The program manager should only assign technical representatives to a contractor's facility as necessary. Technical representatives shall not perform contract administration duties as outlined in Federal Acquisition Regulation (FAR) Section 42.302(a) .

DCMA was established to perform contract administration for the Department of Defense. DCMA is expected to operate in an independent, consistent, transparent and collaborative manner while performing a wide variety of contract oversight functions.

DCMA prioritizes and balances it's Contract Management activities to reduce acquisition risk by focusing limited resources on the highest risk processes, products, and programs. DCMAs mission is best achieved when there is open communication and teaming between DCMA and its acquisition partners and when there is a full understanding of all program risks and acquisition objectives.

While DFARS 242.202 allows for limited exceptions to DCMA performing contract administrative functions, it is not a prudent use of limited DoD resources for buying activities to duplicate the contract administration functions assigned to DCMA. Similarly, DCMAs acquisition partners are not authorized to audit DCMA operations. In our constrained fiscal environment, organizations should not be expending precious funds to perform functions budgeted elsewhere by the Department. This duplication may create additional costs for Industry, and ultimately the Department; these are costs that we cannot afford.

Where a Program Manager determines that they require technical representatives at a contractors facility to perform non-contract administration service, technical duties, and to provide liaison, guidance, and assistance on systems and programs, per DFAR 242.74, the program manager may assign technical representatives following the procedures outlined in DFARS Procedures, Guidance, and Information (PGI) 242.7401.

Per DFAR PGI 242.74, when the program, project, or system manager determines that a technical representative is required, the manager shall issue a letter of intent to the contract administration office commander listing the assignment location, starting and ending assignment dates, technical duties assigned, delegated authority, and support required from the contract administration office. Any issues regarding the assignment of a technical representative should be resolved promptly. However, final decision on the assignment remains with the program manager. Issues regarding the assignment of technical duties that cannot be resolved between the program office and the on-site DoD contract administration office will be elevated.

The program, project, or system manager will furnish the designated technical representative a letter of assignment of delegated technical duties, with copies to the contract administration office, the contracting officer, and the contractor, at least 30 days before the assignment date (or termination date). Any changes to the requirements of the assignment letter will be made by a new letter of intent and processed in accordance with paragraph (1) of this section.

The contract administration office normally provides the technical representative with office space, equipment, supplies, and part-time clerical support. The program, project, or system manager provides supervision, technical direction, administrative services (e.g., pay, travel, maintenance of personnel records), and, when required, full-time clerical support.

The program manager or designee and the contract administration office, at the local level, shall negotiate a memorandum of agreement (MOA) delineating their functional

administrative interrelationships, with annual updates as necessary. The agreements may be included in an existing MOA, if one exists, or as a separate MOA.

The technical representative shall keep the contract administration office commander fully informed of matters discussed with the contractor. The contract administration office shall also keep the technical representative fully informed of contractor discussions that relate to technical matters within the purview of the technical representative's assigned duties.

11.6. Contractor Councils

11.6. Contractor Councils

The Defense Contract Management Agency (DCMA) supports the formation of management, sector, and/or corporate councils by each prime contractor under DCMA cognizance that provide Acquisition Category (ACAT) I, ACAT IA, or ACAT II program support. These councils provide an interface with the Contract Management Office Commander; the Defense Contract Audit Agency Resident Auditor; representatives from all affected acquisition management activities (including program managers, Item Managers, and Standard Procurement System Component Team Leaders), or designated representatives for any of the above listed individuals. Acquisition managers or designees should support both council activities and council-sponsored Working-Level Integrated Product Teams. Acquisition managers should assist the councils and keep all the stakeholders informed about issues affecting multiple acquisition programs, work issues quickly, and elevate unresolved issues to appropriate levels for resolution. These councils may identify and propose acquisition process streamlining improvements. Acquisition managers should assist and encourage councils to coordinate and integrate program audit and review activity, support and promote civil-military integration initiatives, and accept contractor Standard Procurement System proposals and other ideas that reduce total ownership cost while meeting performance-based specifications.

The program office staff should interface with contractors' councils, keeping in mind that such councils are not federal advisory committees under the Federal Advisory Committee Act . The staff may find that these councils strengthen the corporate relationship with the Department of Defense, provide an interface between company representatives and acquisition managers, communicate acquisition reform initiatives, or even resolve issues. In leading corporate endeavors, such as Standard Procurement System proposals, civil-military integration ideas, or other initiatives designed to achieve efficiencies for the company, these councils may ultimately produce savings for the Government.

11.7. Property

11.7.1. Government Property in the Possession of Contractors (GPPC)

All program managers should prevent the unnecessary furnishing of Government Property. The program manager should assign GPPC management authority within the program office, and identify needed actions, reviews, and reports. Decisions about acquisition, retention, disposition, and delivery requirements should be well informed and timely. GPPC no longer needed for current contract performance or future needs should be promptly disposed of or reutilized in accordance with applicable laws and regulations; or stored under a funded storage agreement. The program manager should document decisions regarding GPPC in the contract file.

GPPC includes Government property that is not "owned" by the program manager, but is "used" on the program. Government property may only be furnished to contractors under the criteria, restriction, and documentation requirements addressed in Federal Acquisition Regulation 45.102 and Procedures, Guidance, and Information 245.105.

11.7.2. Contractor Acquired Property

Contractor acquired property is property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.

DoD policies, processes, and practices are structured on delivery, receipt and acceptance of property. This aligns and is consistent with other DoD processes and practices (e.g., Wide-Area Work Flow , Unique Item identification). (**Note:** The Wide-Area Flow site access is conditional based on registration and identification of user roles.) Although the DoD may have title to some property, e.g., property acquired, fabricated, or otherwise provided by the contractor for performing a contract, such property has not yet been delivered.

Upon delivery to the Government, contractor acquired property should be recorded in the appropriate property accountability system. If this property is subsequently provided to a contractor for follow-on contracts, it will be managed as government furnished property. Consistent with DoD Instruction 5000.64 , there is no requirement for accountability by DoD Components for such property prior to delivery to the Government. Third parties (to include contractors) have stewardship responsibility, to include creating and maintaining records of all Government property accountable to the

contract, consistent with the terms and conditions of the contract or third party agreement, for the Government property in their care.

11.7.3. Government Furnished Property

"Government-furnished property" means property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract.

Although the Department of Defense may not have physical custody, to maintain effective property accountability and control and for financial reporting purposes, DoD Components are required to establish records and maintain accountability for property (of any value) furnished to contractors as Government Furnished Property.

11.8. Modeling and Simulation (M&S) Support to the Entire Product

11.8. Modeling and Simulation (M&S) Support to the Entire Product

Modeling and Simulation capabilities can significantly improve the efficiency and effectiveness of conceptualization, development, experimentation, test, and sustainment activities during the life cycle of DoD systems. The program manager should employ M&S resources and products during system design, test and evaluation, modification, upgrade, and operations and sustainment.. The program manager should collaborate with the weapon system operational users, analysis agencies, test and training activities (e.g. government laboratories and facilities), and consider industry inputs during M&S program planning. Planning should include the application, support, documentation, and reuse of M&S resources, including data and analyses generated outside the program of record, as well as from the program of record; and the integration of M&S across functional disciplines.

The following additional considerations are useful during M&S planning activities:

- Plan for M&S and make necessary investments early in the acquisition life cycle.
- Incorporate M&S tools to improve the requirements development process.
- Employ M&S tools to assist in the evaluation of contractor proposals.
- Develop system models in preparation for use across a wide range of disciplines (e.g. use of CAD/Cam for training manuals, etc.).
- Identify or define standards and technical requirements that support re-use or leverage of M&S resources and products throughout the system life cycle to the greatest extent possible. Where it is necessary to invest in M&S development, ensure that licensing is appropriate, and avoid exclusive rights of developer.
- Use and reuse models and simulations, modified as appropriate to the task, in order to provide consistent and efficient test planning, pre-test results prediction, posttest evaluation, and the validation of system interoperability; and to supplement design qualification, actual test and evaluation, manufacturing, and post-production and operational support.

- Employ verified, validated models and simulations, and ensure credible applicability for each proposed use.
- Use data from other activities (e.g. development test) during weapon system development to assist in model, simulation, and data validation.
- Involve the developmental and operational test agencies in M&S planning early in the application of M&S to efficiently support both developmental test and operational test objectives.
- Have the Defense Intelligence Agency review and validate threat-related elements of the models and simulations.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 12 - Defense Business System Definition and Acquisition Business Capability Lifecycle (BCL)

12.0. Overview

12.0. Overview

The purpose of this chapter is to provide guidance for executing the Business Capability Lifecycle (BCL) and is intended for use with existing policy for the definition and acquisition of defense business systems (DBS). It is intended to serve as a reference to support all Department of Defense (DoD) staff with responsibilities throughout a DBSs lifecycle.

12.0.1. Contents

This overview discusses the Business Capability Lifecycle (BCL) at a very high level and includes the major BCL tenets and a summary of the BCL process. Following the overview, the chapter includes the following sections:

Section 12.1., Business Capability Definition Phase, provides an overview of the Business Capability Definition (BCD) Phase process and an explanation of the rigorous up-front analysis conducted during BCD Phase activities that result in the Problem Statement section of the Business Case.

Section 12.2., Investment Management Phase, provides an overview of the Investment Management (IM) Phase process and an explanation of IM Phase activities that result in the expansion of the Problem Statement into the Business Case and the development of the Program Charter.

Section 12.3., Execution, provides an overview of the last four phases of BCL and an explanation of the activities for each of these phases that result in a fully designed, developed, tested, deployed, and sustained increment of capability (materiel and non-materiel solution) that satisfies the specific outcomes defined in the Business Case.

Section 12.4., DBS-Specific Criteria, provides an overview of criteria specific to defense business systems (DBS) and BCL.

Section 12.5., Tools and Methods, provides information on the various tools and methods used in conjunction with BCL activities, including an explanation of a Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P) analysis and an explanation of outcomes and measures development.

12.0.2. BCL Introduction

12.0.3. Tenets

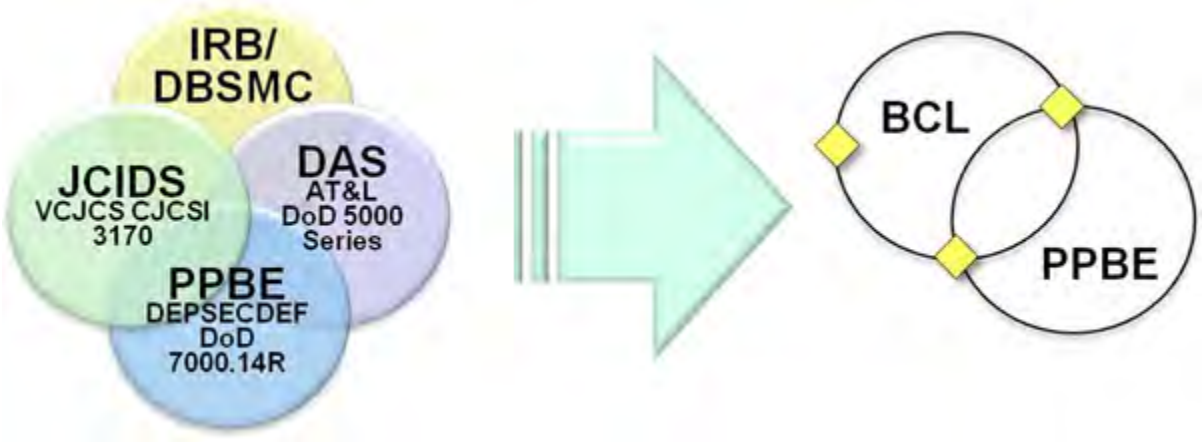
12.0.4. Process

12.0.2. BCL Introduction

The Department has instituted the Business Capability Lifecycle (BCL) to address the unique challenges of information technology (IT) - recognizing that the deliberate weapon systems acquisition process is not agile enough to meet the speed at which new IT capabilities are being introduced to the market.

BCL is the overarching framework for the planning, design, acquisition, deployment, operations, maintenance, and modernization of defense business systems (DBS). It promotes rapid delivery of business capability by facilitating a process tailored to the unique requirements of DBS. It is based on industry best practices, studies, and emerging legislation. It realigns three separate Offices of the Secretary of Defense (OSD) oversight processes into a single process, per Figure **12.0.2.F1** .

Figure 12.0.2.F 1 Re-Alignment of Major DoD Processes for Business Systems



BCL mandates delivering capability quickly within 18 months or less, recognizing that new and evolving IT requires frequent upgrades and that requirements must be reprioritized and new ones will emerge. The goal of BCL is to enable the acquisition and deployment of DBS capabilities to match the speed at which they become viable. Industry and government have learned the big-bang approach to delivering IT seldom meets user expectations; the time-lag between requirements and delivery is often too long.

BCL is modeled on the commercial best practice of iterative capability releases. It requires rigorous up-front analysis of a problem or capability gap to identify it's root cause and determine whether a materiel (i.e., technical) solution is required to solve it and what non-technical factors must support it in order to make it work. Finally, BCL streamlines and integrates decision (milestone) information requirements using the Business Case Template and Program Charter Template, which can be accessed on the Office of the Deputy Chief Management Officer (DCMO)s BCL webpage .

12.0.3. Tenets

1. Rapidly deliver capability to end-users using an incremental approach. This approach delivers increased capability over time, recognizing up-front the users need for future capability improvements. Incremental delivery provides capability to end-users earlier so it can be used, evaluated, modified, sustained, and / or discarded as necessary. Instead of defining all capability improvements up front or implementing new technologies before they are mature, improvements are deferred to future increments. This approach also recognizes that all capability usually cannot and should not be delivered in one big-bang increment.

In the Business Capability Lifecycle (BCL), an increment is delivered in less than 18 months from its Milestone (MS) B to Full Deployment Decision (FDD) and:

- Is a useful and supportable operational capability that can be developed, tested,

produced, deployed, and sustained;
- May consist of multiple capability releases to facilitate delivery, while abiding by Milestone Decision Authority (MDA)-approved BCL time-limited delivery rules; and
- Must be fully-funded.

More information on incremental delivery and time-limited development is available in section **12. 4 .1** , *Time-Limited Development* .

2. Enable rapid decision-making by streamlining oversight . As depicted in Figure **12.0.2.F1** , BCL is governed by an integrated decision-making framework and is the implementation methodology for title 10 United States Code (U.S.C) section 2222.

- The MDA has overall responsibility for DBS acquisition decisions and issues Acquisition Decision Memorandums (ADMs) at appropriate decision points **.**
- Investment Review Boards (IRBs) provide: The structure that integrates requirements, investment and acquisition reviews along with portfolio management for DBS; and, Act as the Overarching Integrated Product Teams (OIPTs) for Major Automated Information Systems (MAIS) DBS to advise the MDA for acquisition purposes.
- The Defense Business Systems Management Committee (DBSMC) makes final decisions over granting obligation authority (i.e., certification decisions) via the IRB process for all DBS and capabilities (i.e., requirements) costing $1M over the current Future Years Defense Program (FYDP).
- For DBS that are not MAIS, DoD Components are expected to establish similar processes and procedures as described in policy and this DAG chapter.

More information on governance and oversight processes and procedures are detailed in section **12.4.2** **,** *BCL Governance.*

3. Focus on activity and decision making at the appropriate level, by the appropriate role. BCL uses the principle of Tiered Accountability by assigning responsibilities to the lowest appropriate and permissible statutory and regulatory level. This approach strengthens accountability, reduces bureaucracy, and accelerates positive outcomes. In addition, the Functional Sponsor, who represents the user(s) and champions the needed capability throughout BCL, plays a critical role in delivering successful capability. The Functional Sponsor works with the Program Manager (PM) during the entire process, and while the PM is responsible for the materiel portions of the capability, the Functional Sponsor is responsible for the remaining Doctrine, Organization, Training, Leadership and education, Personnel, Facilities, and Policy (DOT_LPF-P) portions of the solution, for justifying the program, for securing funding, and for eventually ensuring the solution has met the need that the user(s) originally identified. This approach ensures that the PM is predominantly focused on executing the materiel portion of the program, not on the entire spectrum of DOTMLPF-P activities.

4. Base acquisition decisions on risk and rigor, not document format. The objective is to bring the right information and people to the point of decision-making while eliminating non-value-added documents. This tenet is based on the assumption that decisions should be based on the risk of delivering the capability to cost and schedule and how prepared the program is to do so, not whether the program has produced an over-abundance of properly formatted documentation with the "right approvals.

Supporting this tenet, BCL (1) encourages tailoring, both the process and information requirements, and (2) the use of a Business Case and Program Charter. From a program structuring / process perspective, the goal should be to design and scope a program that will deliver capability rapidly, while tailoring out unneeded or non-value added steps. The goal of tailoring information requirements by decision authorities should only require PMs and other participants in the defense acquisition process to present the minimum information necessary to establish the program baseline, describe program plans, understand program status, and make informed decisions; tailoring in information requirements by the MDA is the recommended approach to achieve this. In general, tailoring should consider multiple factors including program size, scope, risk, urgency of need, and technical complexity. The PM proposes and the MDA approves tailoring decisions in an ADM.

BCLs use of a Business Case (which integrates program-level plans and information for decision makers) and a Program Charter (which outlines roles, responsibilities, and organizational agreements) reduces the amount of documentation that must get coordinated, particularly at the Office of the Secretary of Defense (OSD) level, reducing time and cost. Program-level documentation may still be coordinated and approved within the Component, but does not need to be approved by OSD. This approach places focus on the need, the solution, and the risk not the amount of documentation.

The Business Case Template and Program Charter Template are available on the Office of the Deputy Chief Management Officer (DCMO)'s BCL webpage .

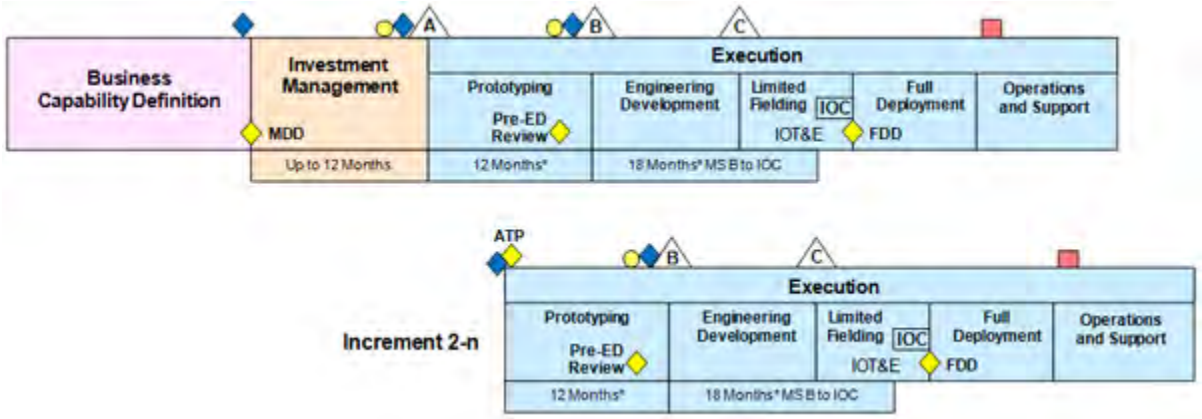
5. Employ outcomes and performance-based measures. Successful capability delivery relies upon the ability to track progress toward completion. BCL integrates the early development of outcomes and associated measures throughout the process. Outcomes define what good looks like to indicate when success has been achieved at varying levels (strategic, business, program, etc.). Performance measures identify the performance-based metrics that provide visibility to the outcomes progress towards completion. BCL supports a top-down decomposition process of outcomes and performance measures development, where high-level outcomes are developed early on and then decomposed further into business and program outcomes as more detail is learned throughout BCL phases. More information on measures and outcomes development is in section 12.5.3 *Outcomes and Measures Development* .

12.0.4. Process

The Business Capability Lifecycle (BCL) is composed of seven phases: Business Capability Definition (BCD), Investment Management (IM), Prototyping, Engineering Development, Limited Deployment, Full Deployment, and Operations and Support (O&S). At the highest level, the BCL Model can be viewed in three main segments BCD, IM, and Execution.

The BCL Model is depicted in Figure **12.0.4.F1** .

Figure 12.0.4.F1 BCL Model



BCD and IM consist of pre-acquisition activities that are critical to implementing a successful acquisition program during Execution. A well-run program may spend upwards of 2/3 of its time on pre-Execution activities for the initial increment. Thus, BCL places considerable emphasis on analysis, critical thinking, requirements development and refinement, and scoping before Execution begins. It requires a Functional Sponsor to define outcomes and measures for declaring success during the BCD Phase before a solution is chosen and executed in subsequent phases. The model drives an iterative approach to capability delivery, which enables the Program Manager (PM) and Functional Sponsor to apply lessons learned to subsequent increments, to continuously refine requirements, and to rapidly deliver increased capability to end-users.

The Investment Review Board (IRB) / Defense Business Systems Management Committee (DBSMC) governance framework is a critical element of BCL and weaves together the requirements, investment, and acquisition processes for Defense Business Systems (DBS). The IRBs provide cross-functional expertise to the Milestone Decision Authority (MDA) (for MAIS acquisitions) and perform investment and portfolio management oversight for all DBS. More information on the IRB / DBSMC processes is located in the DoD IT Defense Business Systems Investment Management Process Guidance" June 2012..

12.1. Business Capability Definition (BCD) Phase

12.1.1. Purpose, Outputs, and Outcomes

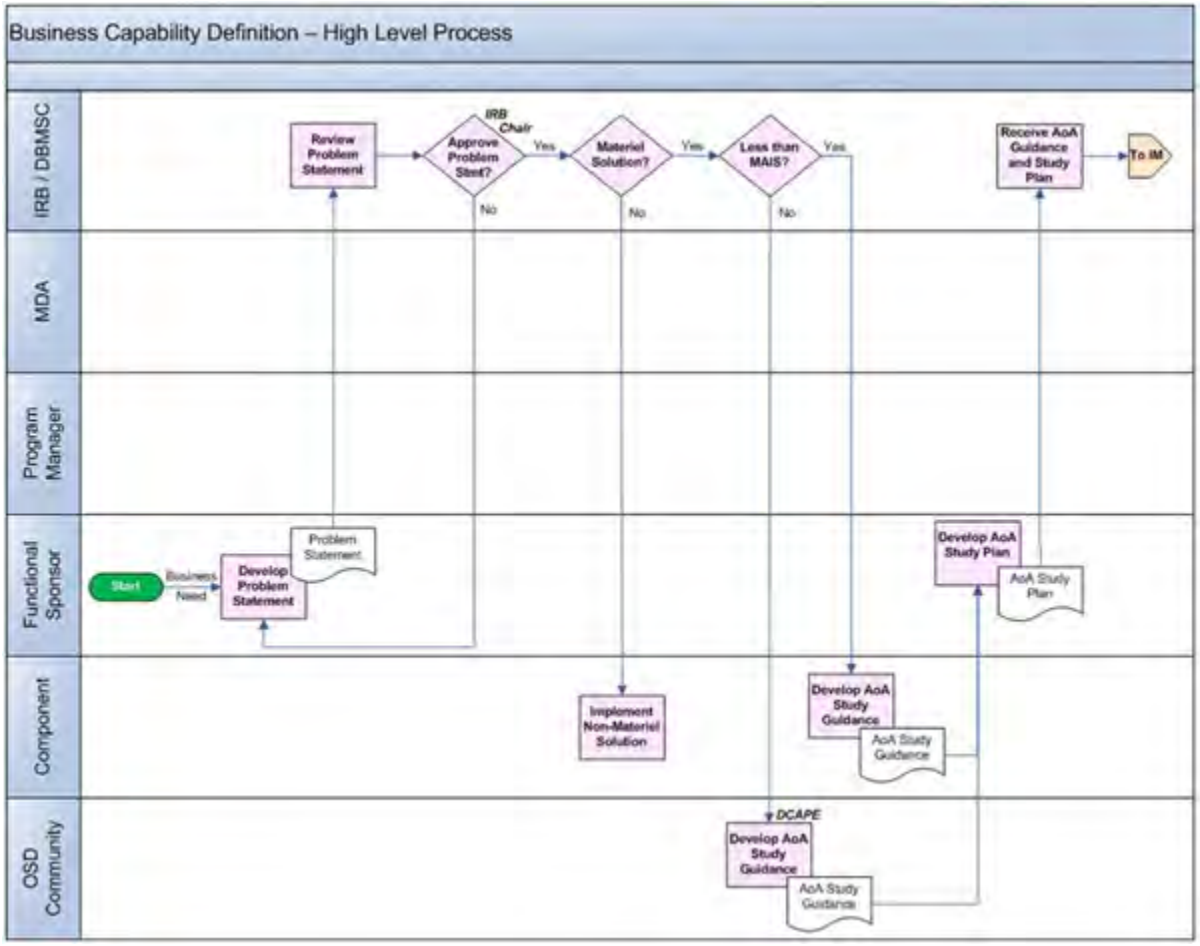
The purpose of the Business Capability Definition (BCD) Phase is, upon the identification of a problem, need or gap, to analyze it, understand it, and scope it.

The outputs and outcomes of the BCD Phase are:

- The outcome is a thorough understanding of the problem, need or gap at a root cause level and the successful identification of the desired outcome (or, "what good looks like" when the problem is eventually solved);
- Completion of a clearly-defined and scoped Problem Statement; and
- Informed decision-makers at the Component and Office of the Secretary of Defense (OSD) levels.

12.1.2. BCD Phase Process

Figure 12.1.2.F1 - BCD Phase High Level Process Flow



The Business Capability Definition Phase (BCD) Phase begins with identification of a business need (*note* : it can also be considered a problem, symptom, gap, opportunity or myriad other things, but in the Business Capability Lifecycle (BCL) and throughout this Chapter it is referred to as a "problem" or "business need"). Multiple activities occur in this phase, including clearly defining the problem and it's root cause(s); conducting an "As-Is" and "To-Be" Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P) Analysis; conducting high-level Business Process Re-engineering (BPR) through the Functional Sponsor's assessment of the desired outcomes; proposing a solution mix (either solely non-materiel, or a mix of materiel and non-materiel); and defining / validating High-Level Outcomes (HLOs) and measures that scope it. These activities result in a Problem Statement, the main output of the BCD Phase.

Once the Component has approved the Problem Statement, the Functional Sponsor will forward it to the Investment Review Board (IRB) for review and IRB Chair approval. If

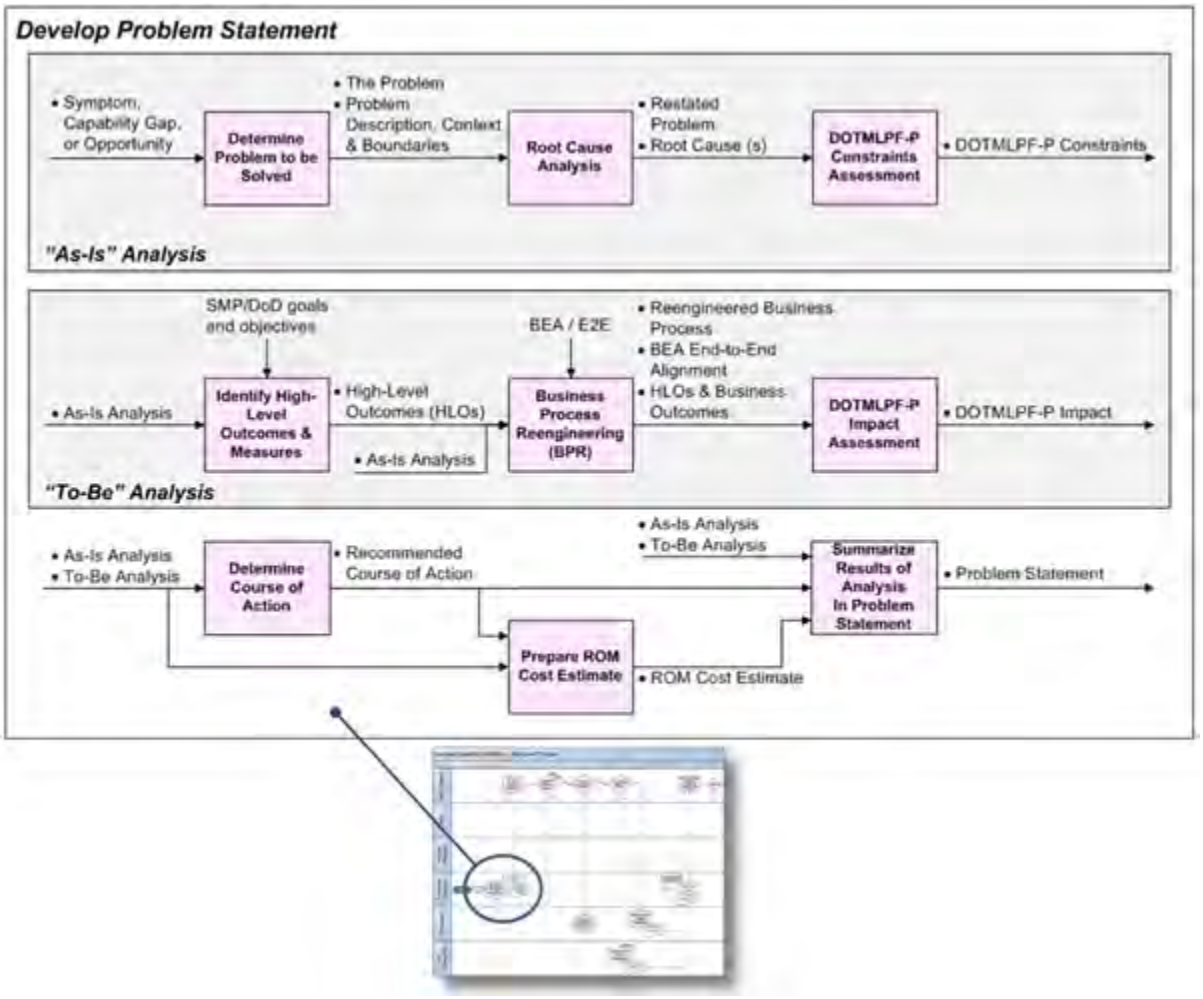
approved, the IRB Chair will subsequently direct the development of Analysis of Alternatives (AoA) Study Guidance to allow the Component to develop an AoA Study Plan for approved Problem Statements that contain a materiel component.

TIP: It is critical that functional users, who not only have an understanding of the problem but are also invested in its outcome, are involved in BCD Phase analysis to ensure the problem is well-understood and outcomes are developed correctly from the outset.

12.1.3. BCD Phase Activities

In the Business Capability Lifecycle (BCL), the Business Capability Definition Phase (BCD) Phase consists of rigorous analysis activities, the output of which is the Problem Statement (sections 1-3 of the Business Case Template, available on the Office of the Deputy Chief Management Officer (DCMO)'s BCL webpage). The final Problem Statement can be developed either step-by-step as BCD Phase analysis activities are completed or after all analysis has been completed. The activities involved in developing the Problem Statement are depicted in Figure **12.1.3.F1** .

Figure 12.1.3.F1 - Decomposition of "Develop Problem Statement" Process Step



TIP: When conducting the BCD Phase analysis, consider the following questions:

1. What is the problem?
2. Who is affected by the problem?
3. When does the problem occur, and how often?
4. What is the root cause(s) of the problem?
5. What is the business value of solving the problem?
6. How will we know when the problem has been solved?

12.1.3.1. "As-Is" Analysis

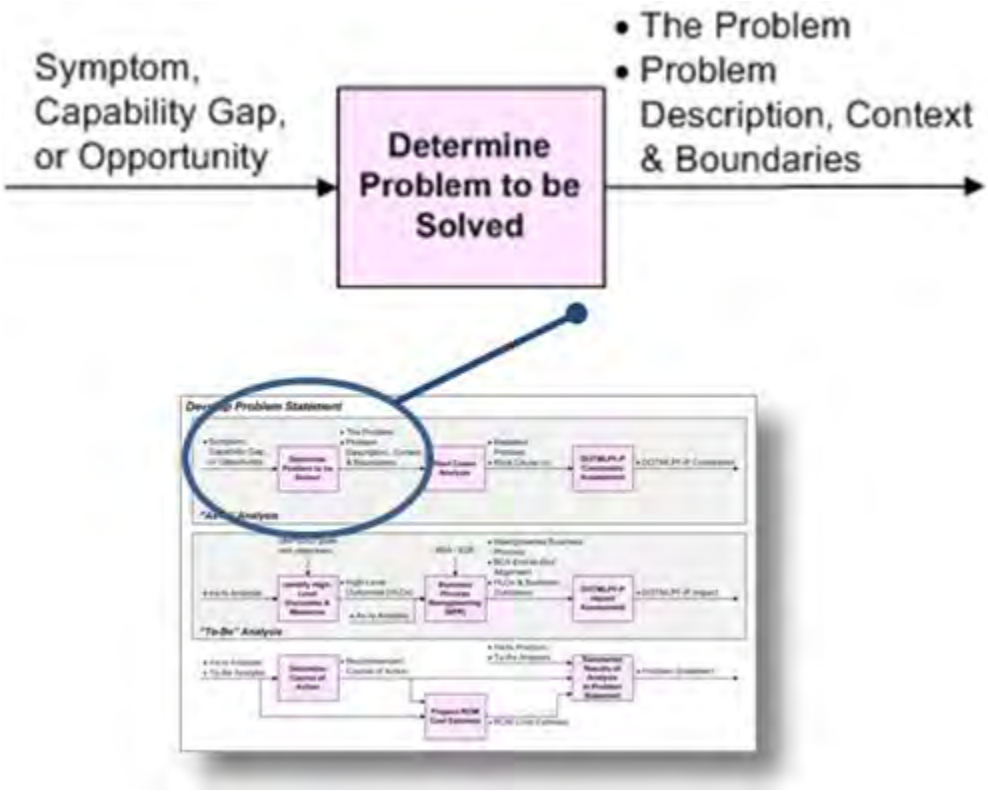
During Business Capability Definition (BCD) Phase "As-Is" Analysis, users / functional experts take the problem that has been identified, put it into appropriate context (organizational, environmental, etc.) and conduct both a Root Cause and Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and

Policy (DOTMLPF-P) Analysis (or, a DOTMLPF-P Constraints Assessment).

Determine Problem to be Solved. The purpose of this activity is to analyze a business need (whether an actual need, or a perceived need) that has been identified by a user in an organization.

The business need is analyzed by users and functional subject matter experts (SME) who understand the business processes and environment in which the business need exists. This analysis results in a concise definition of the problem.

Figure 12.1.3.1.F1 - Determine Problem to be Solved Context



The analysis must take into consideration the functional scope and organizational span of the problem - who is affected by it and where (i.e., Component-only or Enterprise-wide). It also includes describing the problem in further detail and providing context and boundaries (i.e., functional scope and organizational span), which expresses the problem in a manner that is specific, testable, and quantitative in nature.

It is important to bound this analysis to ensure it does not reach into the territory of specific, potential solutions ("a system will fix this" or "an Oracle ERP is the answer") and focuses simply on defining the problem.

The following is a summary of the Determine Problem to be Solved activity along with

an example:

- *Inputs.* Symptom, capability gap, opportunity, etc. (problem / business need).
- *Process.* User(s) in DoD identify a problem or business need and refer it to the decision-maker (i.e., the Functional Sponsor) whose responsibility it is to investigate the business need and determine if development of a Problem Statement is warranted. The Functional Sponsor then engages participants to analyze the business need and identify the underlying problem to be solved. They determine other characteristics of the problem including a problem description, the context of the problem, and the boundaries of the problem.
- *Outputs.* The Problem; problem description, context, and boundaries.

Example. Security clearances.

1. Someone in the DoD identifies what they believe to be a problem or business need and informs a leader within their organization.

User-identified problem. It takes too long to get a security clearance, which is adversely impacting an organization's ability to effectively operate. The Problem is reported up the chain, possibly by an HR Supervisor or the Security Manager of organization, to the Functional Sponsor.

2. The Functional Sponsor directs a team to analyze the problem that was identified.

Analyze and Validate. *The Problem: It takes too long to get a security clearance.* Problem is decomposed and validated with anecdotes such as: The end-to-end processing of an initial top secret clearance took 311 days; GAO has reported concerns of the quality of investigative and adjudicative work in processing clearances; it is impossible for facility security officers to get clearance information in a timely manner.

3. Team provides information to Functional Sponsor, including a more in-depth description, organizational / environmental context, and boundaries.

Problem Description, Context, and Boundaries. All Federal agencies requiring cleared staff are adversely impacted by the inability to deploy/redeploy staff in an efficient and timely manner. Clearance approvals are provided by multiple organizations utilizing various standards and procedures through use of cumbersome and disparate legacy data systems.

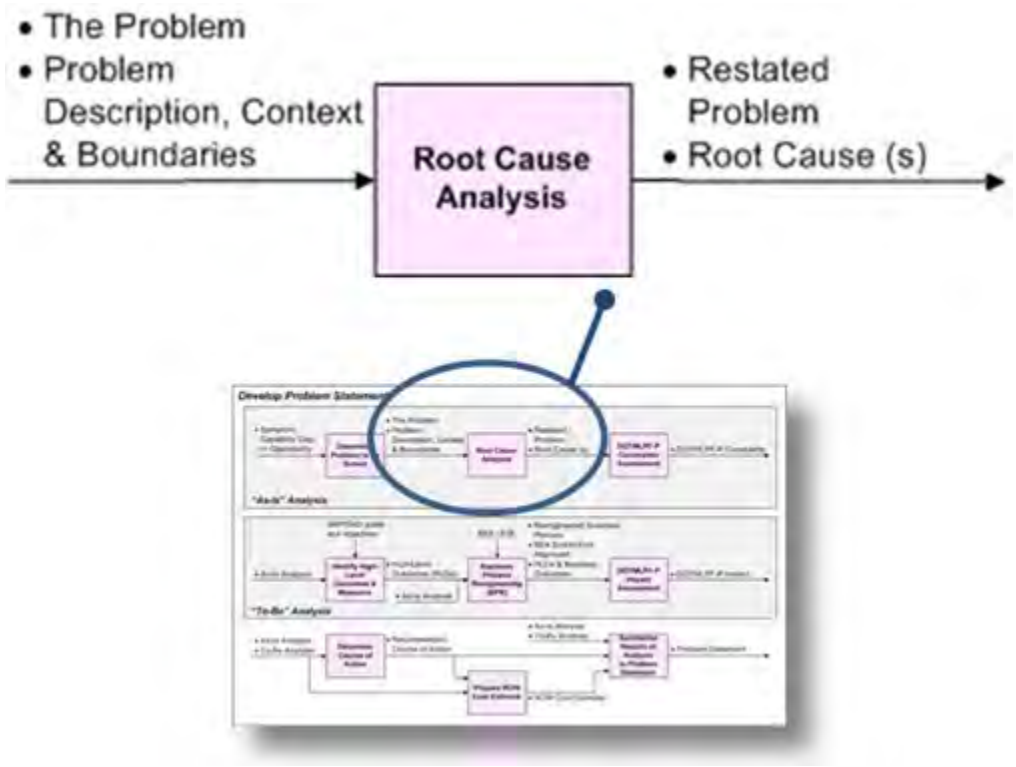
This information, which is intended to provide a better understanding of the problem, will feed Root Cause Analysis.

Root Cause Analysis. One of the issues the Department faces with successfully fielding information technology (IT) business capabilities is making the leap from problem to solution too quickly, resulting in a solution that doesn't meet the fundamental

business need but rather provides temporary "band-aids" for its symptoms. The tendency to "do something now!" must be appropriately balanced with a process that mitigates the risk of fixing a symptom vs. it's root cause(s). Within BCL, the expectation is that functional SMEs will analyze the problem to ensure complete understanding of it's true or root causes.

Root Cause Analysis is a structured approach to determining a problem's causal factors and identifying what behaviors, actions, inactions, or conditions need to be changed in order to eliminate the problem.

Figure 12.1.3.1.F2 - Root Cause Analysis Context



TIP: There are many definitions of a "root cause". The United States Air Force Air War College defines a "root cause" as " *the fundamental breakdown or failure of a process which, when resolved, prevents a recurrence of the problem* ".

(To view the following link, copy and paste it into your browser)
http://www.au.af.mil/au/awc/awcgate/nasa/root_cause_analysis.pdf

There is no single methodology for performing Root Cause Analysis and various approaches (such as brainstorming, "5-Whys" analysis, and Cause and Effect [Fishbone] diagrams) can yield satisfactory results. A good option is to consult your Component's Lean Six Sigma point-of-contact for guidance.

For example, the "5-Whys" analysis starts by asking **" *why did the problem occur?"*** and then takes the answer and asks that same question of the answer. This question and answer cycle is repeated until you reach the fundamental process element that failed. Regardless of the methodology used, it is imperative that the Root Cause Analysis is thorough to ensure that resources are focused on the right item.

The following is a summary of the Root Cause Analysis activity along with an example:

- *Inputs* . The Problem; problem description, context, and boundaries.
- *Process.* Using SMEs, the Functional Sponsor will engage in decomposing the problem to drill down to its root causes, differentiate symptoms from the problem, and update the Problem Statement, if appropriate, based on findings.
- *Outputs* . A restated Problem (if appropriate), and a list of Root Causes.

Root Cause Analysis Example. Security clearances.

1. If a team has not yet been formed, the Functional Sponsor at this point should establish a team to conduct Root Cause Analysis. SMEs may be involved at multiple levels of the security clearance process.
2. The team examines the problem, context, and discovers what may be symptoms *or* root causes:

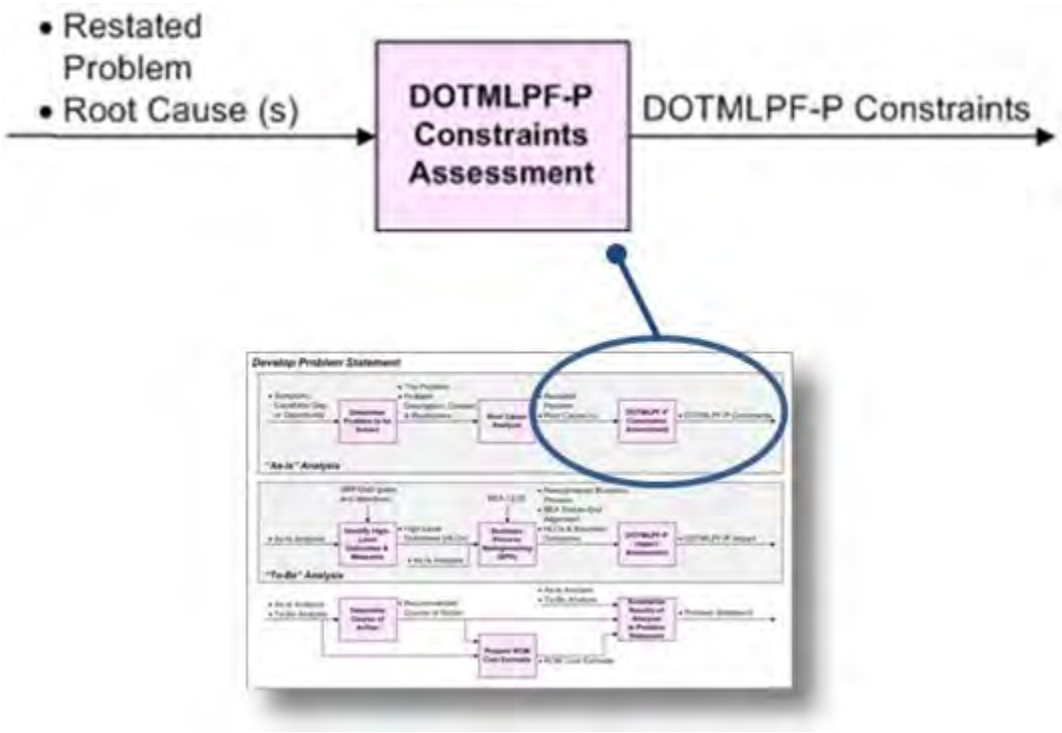
Results. Lack of reciprocity of clearances, delays in fulfilling agencies' missions and completing national security-related contracts, and increased costs of government.

3. Based on expert judgment, the team analyzes the information to derive root causes apart from symptoms. Some of the root causes on security clearances were:

Root Causes. Data and processes are not standardized across agencies; there are difficulties obtaining information from some national, state and local record providers; and, not enough resources are available to handle the number of security clearance requests.

DOTMLPF-P Constraints Assessment, "As-Is" Analysis. This analysis presents functional SME insight into how existing process(es) work. Too often the Department has seen a problem jump to a materiel solution without a thorough assessment of whether or not the problem can be solved by modifying or eliminating a DOT_LPF-P constraint. The "As-Is" DOTMLPF-P Analysis may prevent this from happening by highlighting DOTMLPF-P constraints on the "As-Is" state.

Figure 12.1.3.1.F3 - DOTMLPF-P Constraints Assessment Context



These causal factors are referred to as "DOTMLPF-P constraints" and help determine whether the problem can be solved by eliminating DOT_LPF-P constraints. For example, "changing the Component-level policy will achieve the desired outcomes". It is important to understand the impacts and consequences of implementing non-materiel changes just as much as materiel changes - revising policy or enhancing training programs, for example, can have obvious benefit's but may also add cost and risk that must be mitigated. It is highly likely that DOT_LPF-P factors or underlying business processes are contributing to the problem, and will in fact contribute to the solution.

Similar to Root Cause Analysis, there is no single methodology for conducting DOTMLPF-P analyses. However, methods for DOTMLPF-P are available in the DAG, JCIDS documents , as well as other DoD policy issuances, directives, instructions, regulations, and laws. Further direction on conducting a DOTMLPF-P analysis in the context of BCL is included in section **12.5.2** , *DOTMLPF-P Analysis.*

TIP: It is possible that the solution can be entirely DOT_LPF-P, consisting of, for example, a combination of policy, Component-level guidance, BPR, and re-training solutions. Completing this analysis thoroughly may help determine that a materiel solution is not needed at all - or that the problem has many more factors that need to be solved (i.e., is more complex) than originally thought.

The following is a summary of the DOTMLPF-P Constraints Assessment, "As-Is"

Analysis Activity along with an example:

- *Inputs* . The Problem (restated, if necessary) and list of root cause(s).
- *Process.* The Functional Sponsor / functional SME team assesses the "As-Is" state, considering each DOTMLPF-P element and analyzing the existing constraints that inhibit the ability to solve the problem or the business need. The team determines the DOTMLPF-P constraints and summarizes their assessment in the Business Case.
- *Outputs* . Identification of DOTMLPF-P Constraints in the "As-Is" state.

DOTMLPF-P Constraints Assessment Example . Following is an example summary output of a "As-Is" DOTMLPF-P Analysis (*note* : more detailed information does not need to appear in the Business Case, and may be kept as "working / program-level papers"):

Table 12.1.3.1.T1 - Example of High-Level Constraints from "As-Is" DOTMLPF-P Analysis

DOTMLPF Element	Constraint
Doctrine:	Operating procedures are not in-place. Creates disorganization, noncompliance, and non-standardization.
Organization:	Organization is not properly staffed to meet the agreed service level commitments. Adds time to process.
Training:	Personnel do not have access to training, and training programs differ between organizations.
Materiel:	The system does not collect the information required. Cannot share information properly between systems, creating stovepipes and rework.
Leadership and Education:	The command does not have the resources at its disposal to correct the identified issues.
Personnel:	Qualified and trained personnel are not readily available for the occupational specialties.
Facilities:	The call center is operating at capacity and cannot expand to accommodate the new services that are planned.
Policy **:**	No joint policy exists between organizations.

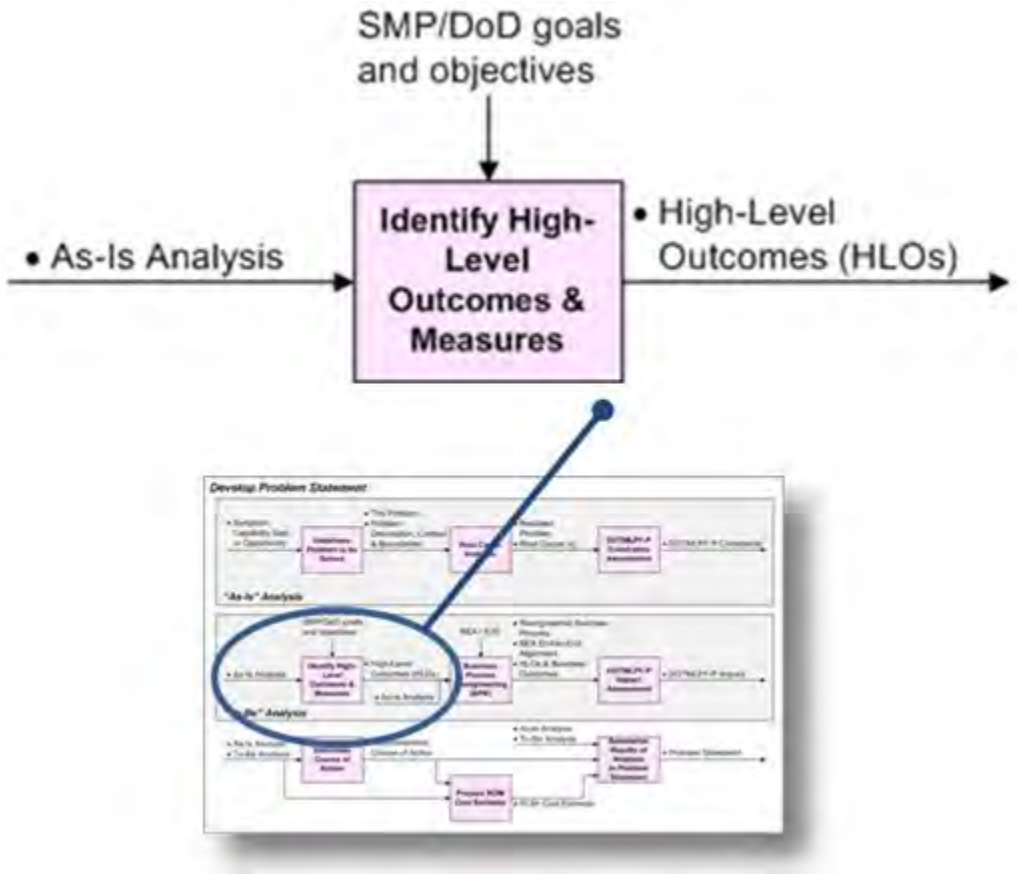
12.1.3.2. "To-Be" Analysis

The "To-Be" Analysis consists of the identification of High-Level Outcomes (HLOs) and measures, Business Process Re-engineering (BPR), and a "To-Be" Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and

Policy (DOTMLPF-P) Analysis.

Identify High-Level Outcomes (HLOs) and Measures. The Functional Sponsor (who represents the needs of the user[s] that originally identified the problem) is ultimately responsible for declaring whether the needed capability has been delivered. Therefore, measurable High-Level Outcomes (HLOs) must be identified up-front so all stakeholders know what constitutes success. Too often programs begin without a clear understanding of what the end-state should be and subsequently development (and corresponding costs) becomes endless.

Figure 12.1.3.2.F1 - Identify HLOs and Measures Context



HLOs and corresponding measures must be established to chart progress toward success and are an integral part of driving the "To-Be" process. HLOs also help scope the effort and align it with Department and Component goals and objectives. Their corresponding measures should be developed by taking into account benefit's, risks, assumptions, and constraints. Later in the BCL process, different and more specific levels of measures will be used for outcome-based testing and determining whether the criteria for Initial Operating Capability (IOC) and Full Deployment have been met.

More information on the outcome development process that begins in the BCD Phase

and extends throughout BCL can be found in section **12.5.3** , *Outcomes and Measures Development* .

> **TIP:** Major updates to a Business Case once it has been approved require review and re-approval by appropriate authorities, which may ultimately cause a delay in capability delivery. Therefore, it is imperative that the analysis of "what good looks like" is performed as thoroughly as possible, and HLOs and their associated measures provide a definitive baseline for testing during the Execution Phase. The Problem Statement, once approved, should not change.

The following is a summary of the Identify HLOs and Measures activity along with an example:

- *Inputs* . "As-Is" Analysis (the Problem; problem description, context, and boundaries; root causes; and DOTMLPF-P Constraints).
- *Process.* The Functional Sponsor will work with the functional team to capture the overall outcome ("what will be different when we're done?" or "what does good look like when we're done?"). Next, considering strategy, goals, and objectives (Department and Component), the Functional Sponsor will determine HLOs and corresponding measures, as well as associated benefit's, risks, assumptions, constraints, and dependencies for each HLO.
- *Outputs* . HLOs (including associated measures, benefit's, risks, assumptions, constraints, and dependencies).

Risk identification started during this activity begins a continuous process of risk management throughout the lifecycle of the program. This is a good point to establish a formal process of identifying, documenting, managing, and mitigating risks. An example of risk documentation is shown in section **12.2.3.2** , *Define Risks and Risk Mitigation,* Table **12.2.3.2.T2** .

HLOs and Measures Identification Example. Security clearances.

1. The Functional Sponsor engages functional / SME team in determining what good would look like to them when the problem is solved, that is, what a HLO would be for the problem "The security clearance process takes too long":

HLO: Obtain security clearances in less time than it currently takes.

2. The Functional Sponsor then identifies what strategic (Strategic Management Plan (SMP), Department, and / or Component) goal or objective that HLO supports:

Strategic linkage: Enhance the DoD Civilian Workforce (DoD SMP Business Goal #4).

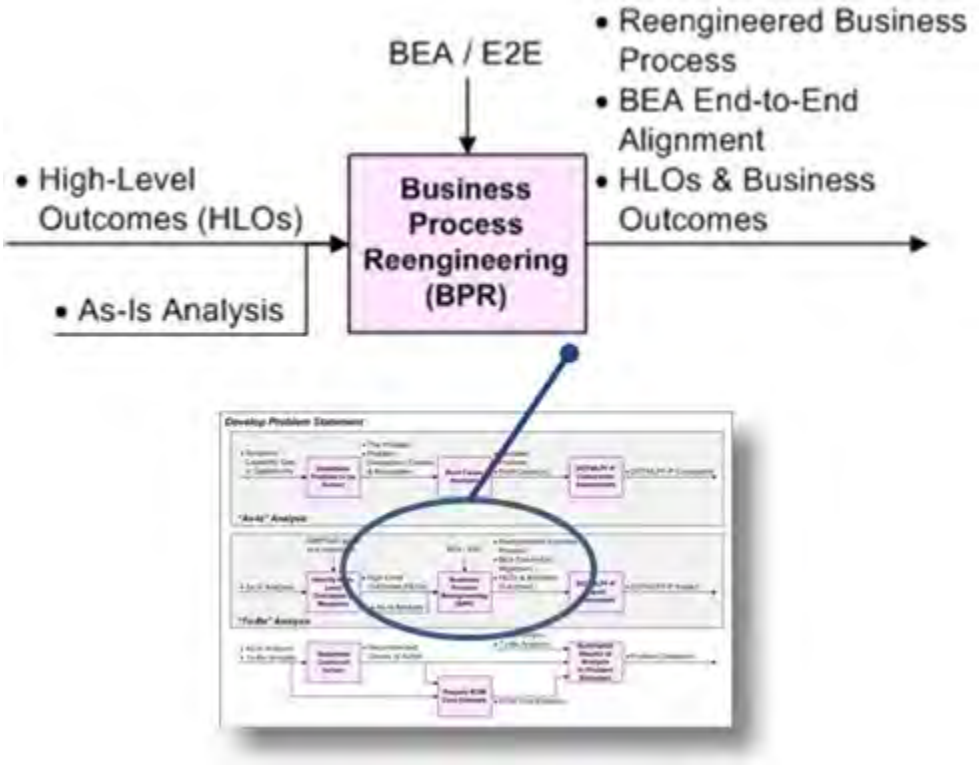
3. Based on the determined HLO, the Functional Sponsor works with the team to determine a quantitative metric for the success of the HLO:

- (metric) Days from application to clearance granted.
- (measure) Current: 444 days; Target: 60 days.

HLO's corresponding metric and measure:

Business Process Re-engineering (BPR). Driven by the HLOs, the Functional Sponsor leads BPR and analyzes existing business workflows and processes to determine what, from a process perspective, needs to change in order to achieve these outcomes. Items may include eliminating non-value added process steps, consolidating separate functional tasks into end-to-end cross-functional processes, and integrating business functions as much as possible to improve business operations and to achieve the desired outcome(s). BPR is a continuous process and requires a rethinking of why the "As-Is" process came to be and how it can be improved to achieve efficiencies.

Figure 12.1.3.2.F2 - BPR Context



BPR is initially conducted during the BCD Phase as a complement to DOTMLPF-P analysis and to prepare for conducting an AoA.

There must be an understanding of the "As-Is" processes for BPR to be effective so that defects and issues can be identified and eliminated in the eventual "To-Be" state. The ideal business process is defined during the initial BPR and specific, actionable business outcomes will be developed based on the HLOs and potential courses of action will emerge (more information on the outcome development process is located in

section **12.5.3** , *Outcomes and Measures Development*).

More information on BPR, see the Office of the Deputy Chief Management Officer (DCMO)'s BPR webpage .

TIP: Content in the Business Case's Problem Statement should not be replicated in a BPR Assessment Form. Refer to the original content through reference or hyperlink.

End-to-End (E2E) Process Alignment . For BCL, a primary input to conducting BPR is aligning HLOs to the Department's End-to-end (E2E) Business Process Flows, which are mapped to the Business Enterprise Architecture (BEA) . Business outcomes and activities developed during initial BPR should align to an E2E Business Process and corresponding E2E Flows to show which E2Es will be affected if the "To-Be" state is realized.

The DoD has currently identified15 E2E Business Flows which represent a combination of mature, industry best practices and DoD-specific business functions. Each E2E Business Flow is a value chain that represents a set of integrated business functions that fulfill a need identified by the organization. E2Es are cross-functional, cutting across organizational boundaries. By streamlining business processes using an end-to-end approach, organizations can create consistent data models, eliminate data redundancies, eliminate the need for duplicate data entry, eliminate the need for manual reconciliations between DBS and reduce the total life-cycle costs of the organization's DBS.

The Functional Sponsor will identify which E2E(s) will be affected by matching HLOs and business outcomes to the E2E Flows. More information on the E2Es, including instructions on how to allocate Business Processes to Business Flows and document them in the Business Case can be found in section **12.5.4** , *BEA and BCL.* Additional information and reference material are available on the DCMO's BEA webpage .

The following is a summary of the BPR activity along with an example:

- *Inputs* . "As-Is" Analysis (including: the Problem; problem description, context, and boundaries; root causes; and DOTMLPF-P Constraints); and HLOs (including measures, benefit's, risks, assumptions, constraints, and dependencies).
- *Process.* The Functional Sponsor involves SMEs in business process analysis and BPR. The team proceeds to define the "To-Be" state by identifying new and modified business processes to address the Problem and achieve the "vision" defined by the HLOs. They consider both evolutionary (e.g., enhancements) and revolutionary (e.g., re-engineering) opportunities to define the future state. The team may elect use of modeling techniques to create a rigorous view of the "As-Is" state and "To-Be" state. An important asset at the disposal of the re-engineering team is the BEA, which includes a suite of business models derived

out of E2E business flows. Leveraging the BEA through the E2Es, the team aligns, maps, and decomposes processes. Refer to section **12.5.4** *, BEA and BCL* and the DCMO's BEA webpage .

The results of the BPR and the E2E alignment are summarized in the Business Case by showing the decomposition of the HLOs into subordinate business outcomes. The important characteristics of each business outcome are also defined - specifically measures, benefit's, risks, assumptions, dependencies and constraints.

- *Outputs* . Re-engineered business process, BEA E2E alignment, and business outcomes (including measures, benefit's, risks, assumptions, constraints, and dependencies).

BPR/E2E Alignment Example . Security clearances:

1. Determine the business outcome(s) that support achieving each HLO applicable to the security clearances problem:

HLO: Streamline clearance process

Business Outcome: Establish a "Determinations Store"

Business Outcome Definition: Will provide Security Officers with a listing of security clearance determinations, eliminating the unnecessary processing of clearance applications for applicants with prior clearance investigations or adjudicative determinations

2. Align the business outcomes to the BEA's E2E Business Process Flows and then drill-down to underlying Business Processes and Business Capabilities applicable to the security clearances problem:

Business Outcome: Establish a "Determinations Store"

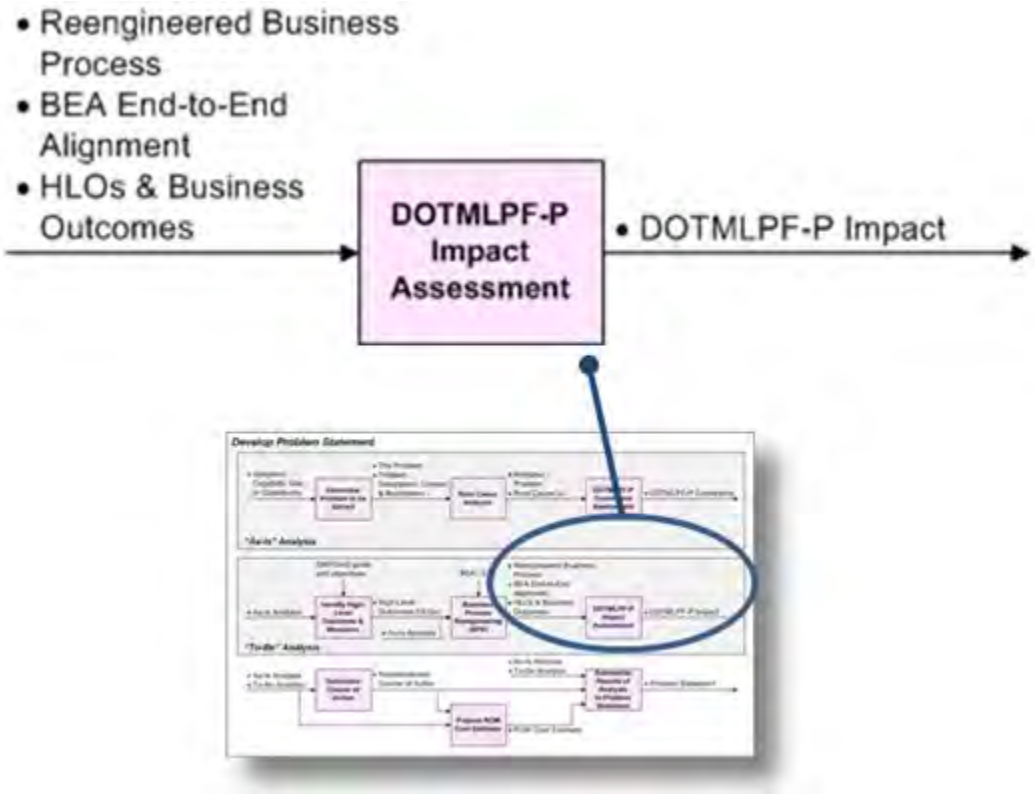
BEA E2E Business Flow : Hire to Retire (H2R)

Business Process : Manage Human Resources Access Control Programs

Business Capability: Manage Personnel Security

DOTMLPF-P Impact Assessment, "To-Be" Analysis. Based on all previous activities and analyses, a DOTMLPF-P Impact Assessment is conducted in conjunction with BPR to determine the impact of a transition to the "To-Be" state. This helps to ensure that all elements of DOTMLPF-P are considered in order to avoid hidden impacts as much as possible, and to realize that it may take multiple DOTMLPF-P elements to solve the problem and achieve the HLOs.

Figure 12.1.3.2.F3 - DOTMLPF-P Impact Assessment Context



The "To-Be" state is unconstrained by tradeoffs or limitations of alternative solutions, since no specific alternatives have been analyzed (**Note:** the Analysis of Alternatives (AoA) is conducted in the IM Phase, after a Materiel Development Decision (MDD) is granted). The results of "To-Be" Analysis are outcome-based and are critical in determining which DOTMLPF-P elements must be addressed to achieve the HLOs and business outcomes.

The following is a summary of the DOTMLPF-P Impact Assessment, "To-Be" Analysis activity along with an example:

- *Inputs* . Initial re-engineered business process, HLOs and business outcomes (including measures, benefit's, risks, assumptions, constraints and dependencies), and BEA E2E Alignment.
- *Process.* The Functional Sponsor and the SME team consider the DOTMLPF-P elements that will be impacted in the transition to the "To-Be" state. A summary of the analysis is documented in the Problem Statement section of the Business Case, and includes a list of each DOTMLPF-P Impact (i.e., the actions or changes to realize the "To-Be" state).
- *Outputs* . Identification of DOTMLPF-P Impacts (and potentially, a new or modified business process).

DOTMLPF-P Impact Assessment Example. Table **12.1.3.2.T1** is an example summary output of a "To-Be" DOTMLPF-P analysis (**Note:** more detailed information does not appear in the Business Case and is kept as "working papers"):

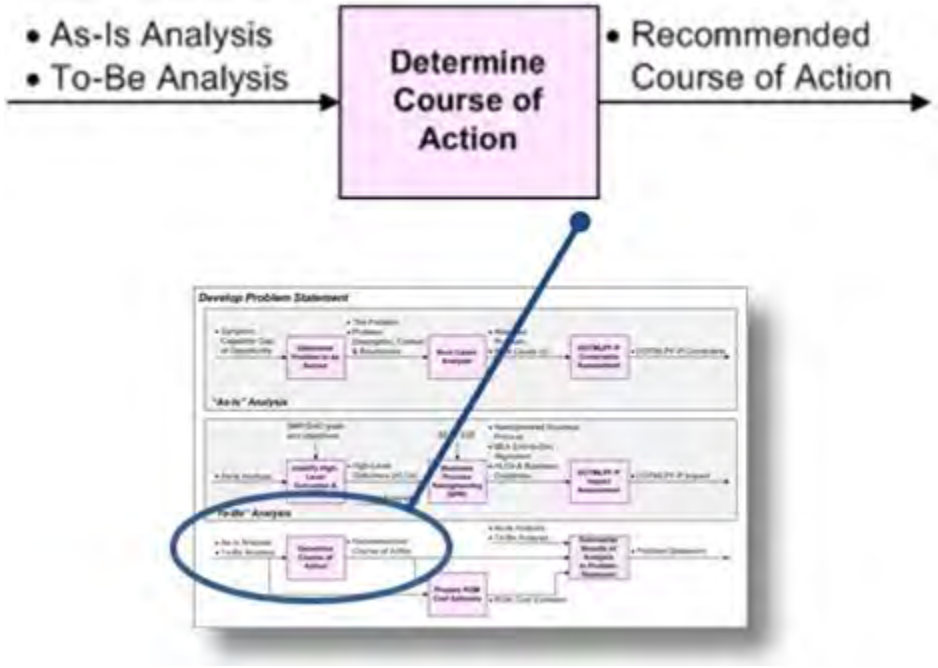
Table 12.1.3.2.T1 - Example of High-Level impacts from "To-Be" DOTMLPF-P Impact Assessment Analysis

DOTMLPF Element	Impact
Doctrine:	Development of new and revised operating procedures is required.
Organization:	Organization changes are required in order to achieve the agreed service level commitments.
Training:	A new training course is required and Personnel need ongoing access to the training.
Materiel:	The existing system must be enhanced or replaced in order to collect the information required by the new policy.
Leadership and Education:	No impact identified.
Personnel:	All Personnel in the call center will be trained for the revised Roles defined for the enhanced or new system.
Facilities:	As a result of BPR, operational improvements will increase the capacity of the existing call center and accommodate the new services that are planned.
Policy **:**	No impact identified.

12.1.3.3. Remaining BCD Phase Activities

Determine Recommended Course of Action. Based on completed analyses, the Functional Sponsor must decide whether a materiel solution is required to solve the problem. Assuming the Functional Sponsor's recommended course of action consists of a materiel solution he or she determines what areas to analyze during the Investment Management (IM) Phase and offers recommendations as to the appropriate solution mix (materiel and non-materiel) that will achieve the defined outcomes.

Figure 12.1.3.3.F1 - Determine Recommended Course of Action Context



No specific solutions are recommended at this point, but based on the analysis conducted, sufficient information is available to inform decision makers that a Materiel Development Decision (MDD) may be required to move forward in the process and, if so, enable an Analysis of Alternatives (AoA) to explore specific materiel solution options.

The Functional Sponsor's recommendation(s) is one of the factors that the Investment Review Board (IRB) Chair will consider when reviewing and determining whether to approve the Problem Statement. The Functional Sponsor's recommendation should also include any DOTMLPF-P impacts.

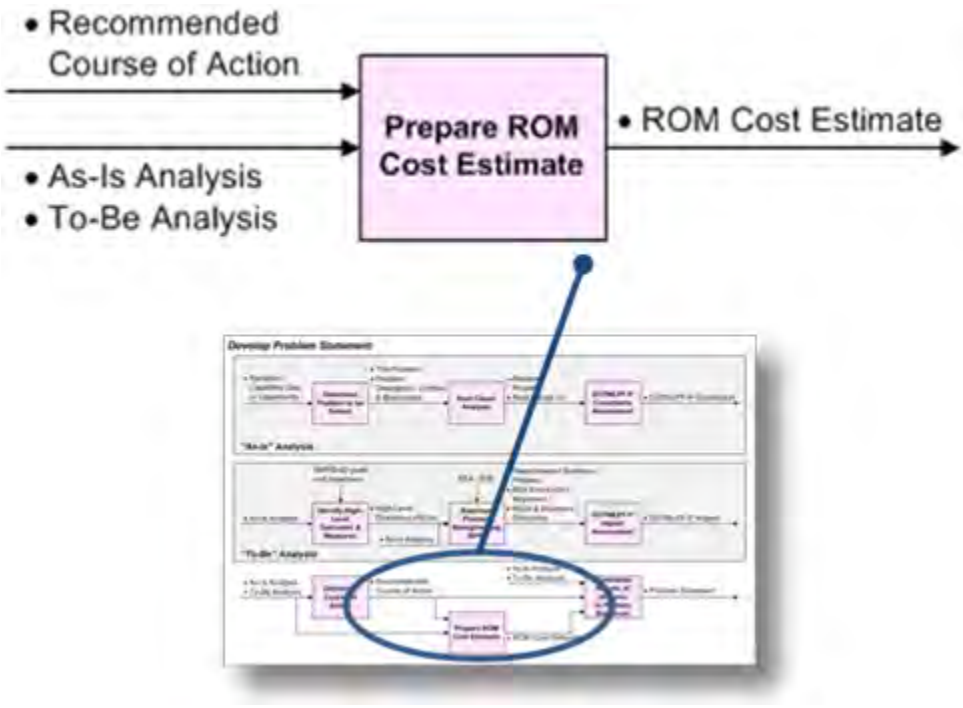
The following is a summary of the Determine Recommended Course of Action activity:

- *Inputs.* "As-Is" Analysis, "To-Be" Analysis.
- *Process.* The Functional Sponsor will review the "As-Is" Analysis and "To-Be" Analysis and select a course of action for further analysis in the IM Phase, if a material component is required. This information will be summarized in the Problem Statement and reviewed by the IRB Chair for approval.
- *Outputs* . Recommended course of action.

Prepare ROM Cost Estimate **.** Based on the Functional Sponsor's recommendation(s), a Rough Order of Magnitude (ROM) cost estimate is developed. The ROM provides a general picture of the level of effort required to solve the problem and the relative size (MAIS or non-MAIS) of what the effort might cost. According to GAO-09-3SP, March 2009 , "Best Practices for Developing and Managing Capital Program Costs", a ROM is

"developed when a quick estimate is needed and few details are available. Usually based on historical ratio information, it is typically developed to support what-if analyses and can be developed for a particular phase or portion of an estimate to the entire cost estimate...."

Figure 12.1.3.3.F2 - Prepare ROM Cost Estimate Context



It is important to provide a best guess for the ROM as it will be an indicator of the level of oversight required after Problem Statement approval.

The following is a summary of the Prepare ROM Cost Estimate Activity:

- *Inputs.* "As-Is" Analysis, "To-Be" Analysis.
- *Process.* The Functional Sponsor will use appropriate SMEs in developing a ROM; it is essentially the gross estimate to bridge the gap between the "As-Is" state and "To-Be" state. At this point in the process there is limited information available to yield a detailed estimate but only a gross estimate is needed to help determine the level of oversight for a potential program. One estimating technique to consider is Analogy (see DAU's Teaching Note on Cost Estimating Methodologies, February 2011 for more information).
- *Outputs* . ROM Cost Estimate.

Summarize Results of Analysis in Problem Statement . Results of (BCD) Phase activities are summarized in the Problem Statement by the Functional Sponsor. This summarization should provide decision makers with the essential information about the business need to make an informed decision supporting the IRB Problem Statement

Review. Considerations for this activity are outlined in Figure **12.1.3.3.F4** .

Figure 12.1.3.3.F3 - Summarize Results of Analysis in Problem Statement Context

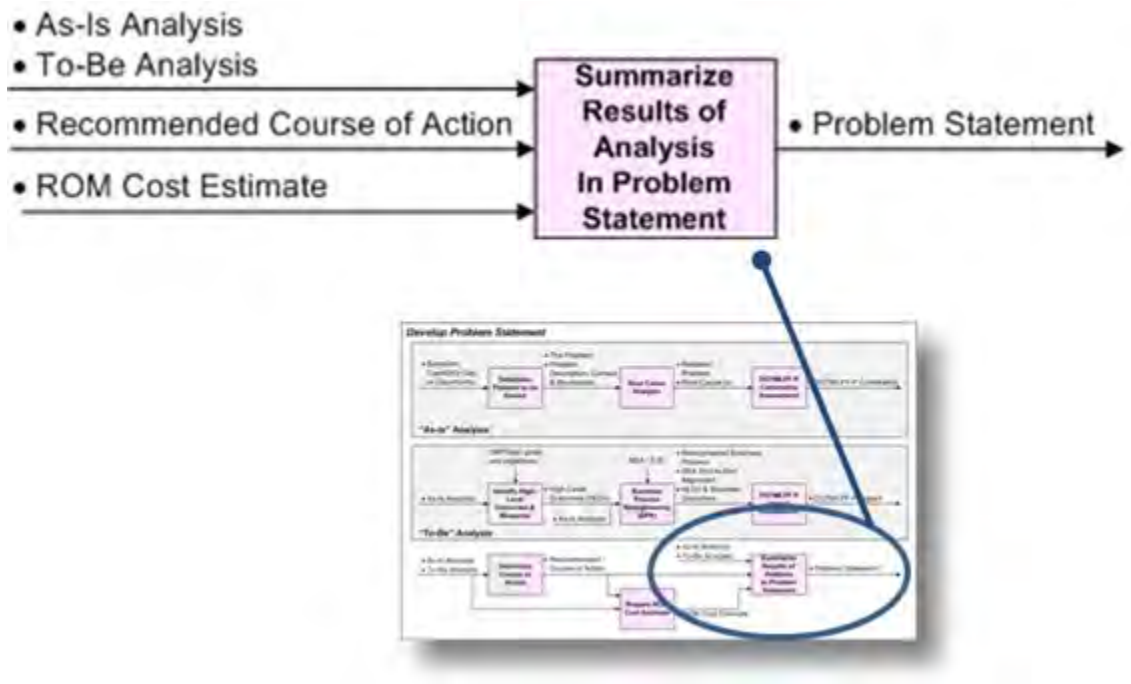


Figure 12.1.3.3.F4 - Considerations Prior to IRB Submission

When compiling the Problem Statement, and before presentation to the IRB, the Functional Sponsor should determine whether the following questions have been adequately answered / addressed:

1. Does the Problem Statement concisely and convincingly demonstrate that the business need exists and merit's solving?
2. Have comprehensive Root Cause and DOTMLPF-P analyses been performed?
3. Has this business need / problem already been solved in the Department, as discovered through initial research?
4. Have specific and measurable success factors been defined and agreed upon among the functional and stakeholder community?
5. Do initial BPR efforts result in enough streamlining and efficiencies to warrant further analysis and continued investment?
6. Is it clear what the Functional Sponsor is seeking from the decision maker, and what steps / activities will take place after the decision?

The following is a summary of the Summarize Results of Analysis in Problem Statement

activity:

- *Inputs.* Results of BCD Phase activities (Business Process Re-engineering BPR) results (driven by HLOs) "As-Is" Analysis outputs, "To-Be" Analysis outputs, recommendation(s) (COA), ROM cost estimate).
- *Process.* The Functional Sponsor summarizes the output of the BCD Phase in the appropriate sections of the Problem Statement (Business Case Section 3), either as phase activities are completed or at the end of the BCD Phase (prior to IRB submission). The Functional Sponsor will also complete the Executive Summary and Introduction sections (Business Case Sections 1 and 2) in preparation for the IRB Problem Statement review.
- *Outputs* . Business Case Sections 1-3.

12.1.3.4. IRB Preparation

Once the Functional Sponsor determines that the Problem Statement is ready for Investment Review Board (IRB) review, it is submitted to the IRB Support Staff. Procedures for IRB submittal can be located in the "Defense Business Systems Investment Management Process Guidance", June 2012 . The package must include Sections 1-3 of the Business Case signed by the Functional Sponsor and a summary slide containing a short description of the problem, the desired outcome or "what good looks like", the ROM Cost Estimate, and the proposed business value to the Department / end-user.

At the IRB, a review is conducted that will generally address items #1-6 of Figure **12.1.3.3.F4** , in addition to the Enterprise and portfolio implications of the need and the Functional Sponsor's recommendation(s) for the way ahead. The IRB Chair will approve or disapprove the Problem Statement or may send it back to the Component for additional work. For an IRB Chair-approved Problem Statement, one of the following occurs:

- If the recommended course of action contains no materiel elements, BCL is exited and the Component will complete / implement non-materiel activities (i.e., policy / process changes, training development, etc.) and report back to the IRB on progress of implementation as directed by the IRB Chair, as appropriate;
- If the recommended course of action contains a materiel element but the cost is expected to fall under the MAIS threshold, subsequent BCL Phases will be executed at the Component level while investment certification activities will utilize the IRB process; or
- If the recommended course of action contains a materiel element and the cost is expected to exceed the MAIS threshold, the Component will execute BCL Phases at the OSD level and utilize the IRB process for investment certification activities.

12.1.3.5. Materiel Development Decision (MDD) Preparation

In preparation for a Materiel Development Decision (MDD), the Director, Cost Assessment and Program Evaluation (DCAPE) (for expected MAIS-level efforts) or the Component-equivalent (for those efforts that are expected to be below MAIS-level, based on the ROM) will develop Analysis of Alternative (AoA) Study Guidance and the Functional Sponsor will complete and submit an AoA Study Plan, based off the approved AoA Study Guidance.

Information on developing the AoA Study Plan and sample AoA Study Plan outlines can be found in DAG Chapter 3, Section 3.3, "Analysis of Alternatives" . The AoA Study Plan should take into account the HLOs and corresponding measures developed during BCD as well as the results of the initial BPR, as these will provide valuable input to how each alternative will be evaluated.

The Study Guidance and Study Plan, along with the approved Problem Statement, will be reviewed by the MDA at the MDD. Based on the ROM:

- Functional sponsors of MAIS-level initiatives will submit the Study Plan through the IRB Chair to the MDA.
- Functional sponsors of below MAIS-level initiatives will submit the Study Plan through appropriate governance channels at the Component level.

The BCD Phase ends with approval of the Problem Statement by the IRB Chair and submission of the AoA materials to the IRB Chair (or, appropriate Component-level governance forum). If a Problem Statement is solely non-materiel, the BCD ends when the Problem Statement is approved since no AoA will be required.

12.2. Investment Management (IM) Phase

12.2.1. Purpose, Outputs, and Outcomes

The purpose of the Investment Management (IM) Phase is to conduct an Analysis of Alternatives (AoA), recommend a preferred Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) solution and deliver a plan (i.e., Business Case) to satisfy the business need in the approved

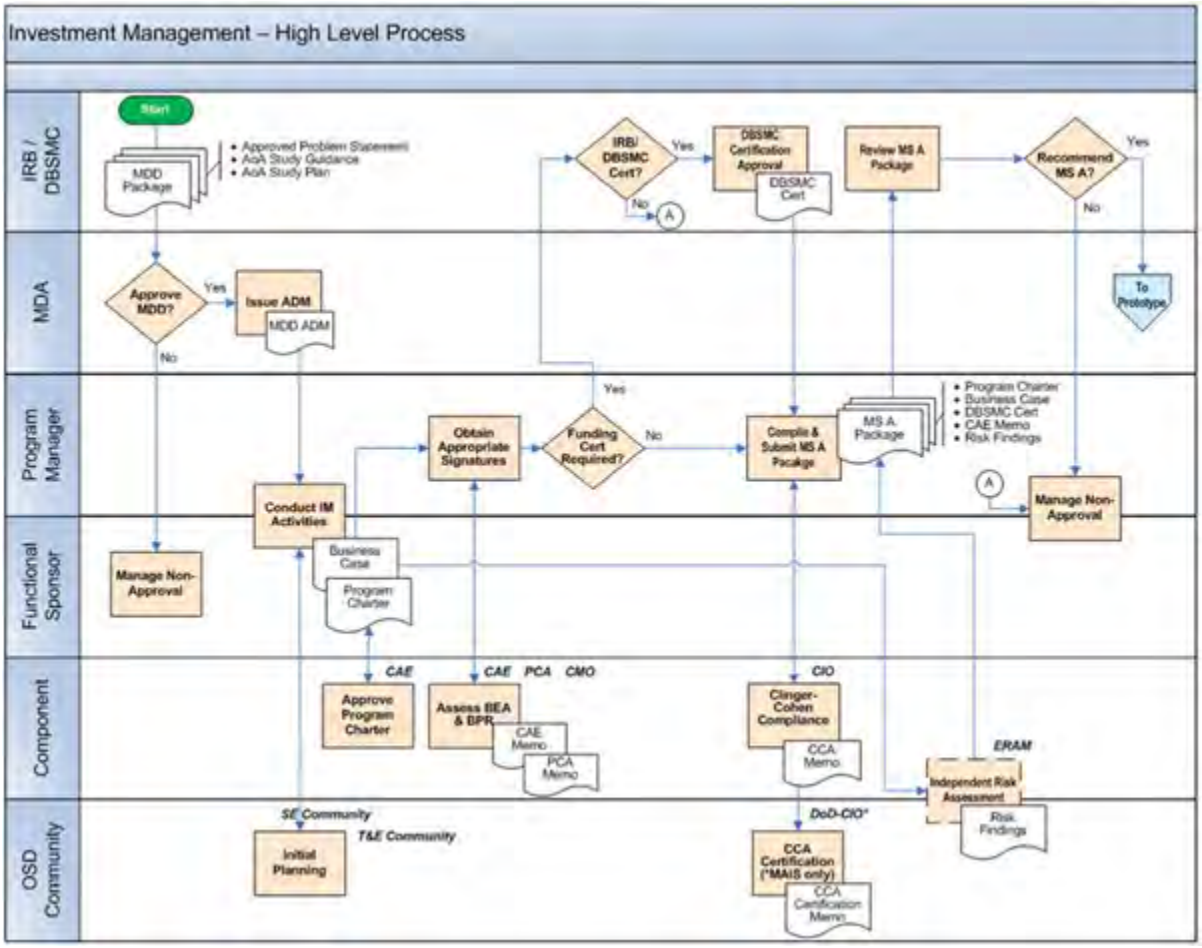
Problem Statement. It is an iterative process that will result in a strategy and plan that can be executed to field useful capability.

The outputs and outcome of IM Phase activity are:

- A completed AoA that enables the Functional Sponsor and program manager (PM) to recommend a preferred solution for solving the business need;
- A well-defined business and technical management approach that describes how the effort will achieve its objectives using the preferred solution-set. The Business Case is the summary level document for those functional plans and strategies.
- A Program Charter defining roles and responsibilities for the potential program; and,
- Certification of funds to proceed through the next BCL phase;

12.2.2. IM Phase Process

Figure 12.2.2.F1 - IM Phase High Level Process Flow



At the Materiel Development Decision (MDD) the Milestone Decision Authority (MDA), in most cases, will approve entry into the Investment Management (IM) Phase. However, it is possible that the MDA may specify a different entry point (phase) into BCL if the technology supporting the materiel solution has been demonstrated and is well-understood, and the potential program is defined well enough to begin in a later phase. If this is the case, the program shall proceed to the designated entry point and perform the appropriate activities as specified in that phase and the MDD Acquisition Decision Memorandum (ADM).

During the IM Phase a Program Manager (PM) is typically assigned early on and will work with the Functional Sponsor to begin managing the materiel portion of IM Phase activities.

The IM Phase begins with an analysis to describe the requirements for the materiel solution and an Analysis of Alternatives (AoA) to select a preferred solution. Based on the preferred solution, the Functional Sponsor and PM will conduct activities necessary to define a program and develop a well-documented plan to deliver the outcomes defined in the IRB Chair approved Problem Statement. Planning documents are developed as appropriate (e.g., systems engineering, test & evaluation) for the program and are expected to evolve as the program matures; prior to Milestone (MS) A, some plans are merely strategies to be refined into plans when more facts are known.

The results of IM Phase activities are summarized in a Business Case that provides decision makers with on overview of the proposed solution including the acquisition and contracting approach. The Program Charter, that outlines the managerial methods and standards for governing the program, is also developed during this phase.

Also, prior to the end of IM Phase, the PM must schedule an independent risk assessment (Enterprise Risk Assessment Methodology (ERAM) is required for MAIS) approximately 120 days prior to MS A review. An ERAM is required for all MAIS DBS prior to a MS A or B review. The program manager will collaborate with the risk assessment team to incorporate findings and recommendations into the program's risk mitigation plan. No additional documentation is created by the program for a risk assessment, as it is based on existing program documentation. Detailed risk assessment findings will be provided to the Functional Sponsor, PM, Investment Review Board (IRB) Chair, and MDA. Summary ERAM findings are presented at the IRB.

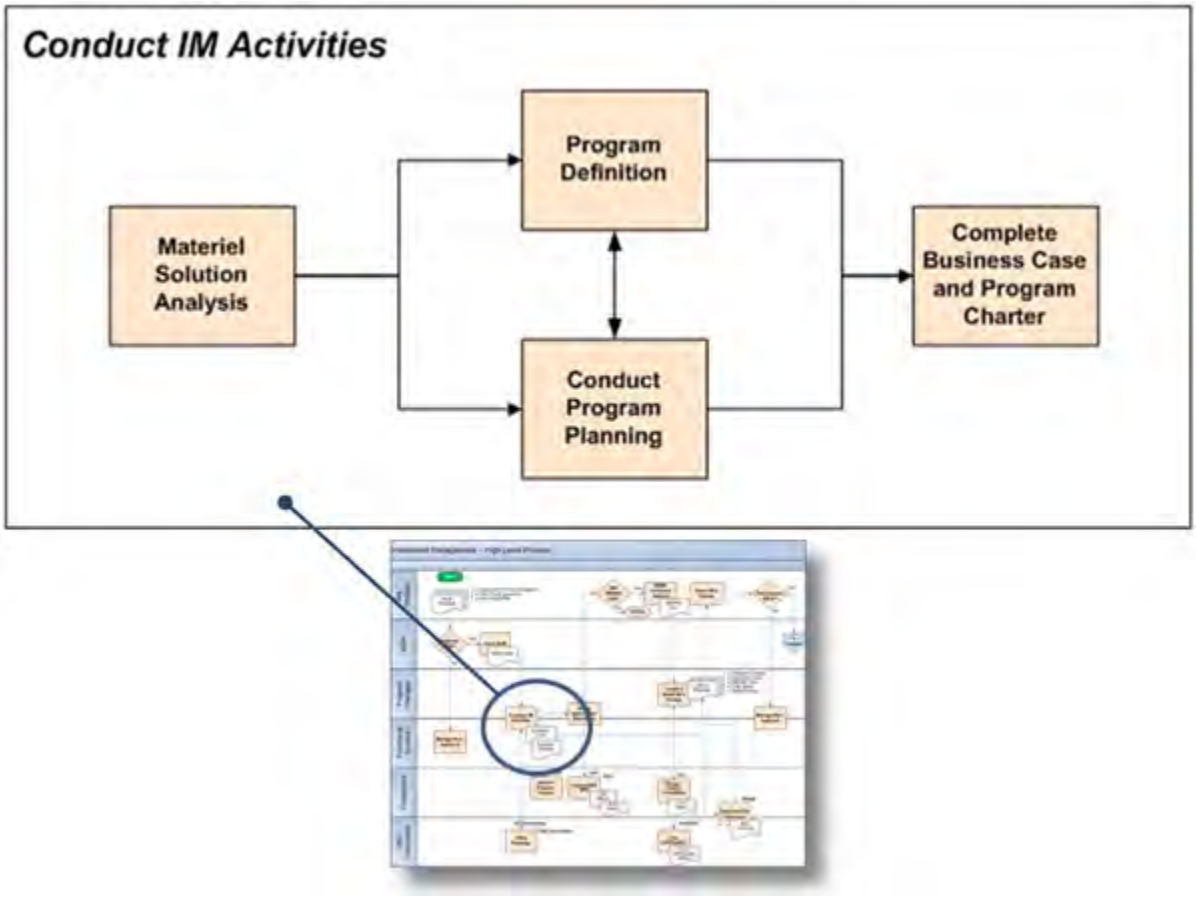
The IM Phase ends when the phase activities are complete and summarized in the Business case, and the PM compiles and submits the MS A acquisition decision package to the IRB for review and the IRB Chair forwards a MS A recommendation to the MDA .

12.2.3. IM Phase Activities

The Investment Management (IM) Phase involves numerous activities beginning by conducting a detailed materiel solution analysis and subsequently developing a program

plan based on the results of this analysis. These activities are depicted in more detail in Figure **12.2.3.F1** . The goal of IM Phase activities is to develop an efficient and effective plan to fulfill the business need documented in the Problem Statement. The results of IM Phase analysis and activities are summarized in a Business Case and a Program Charter, the two key documents used by decision-makers throughout the Business Capability Lifecycle (BCL). The Business Case Template and Program Charter Template are available on the Office of the Deputy Chief Management Officer (DCMO)'s BCL webpage .

Figure 12.2.3.F1 - Decomposition of IM Phase Activities

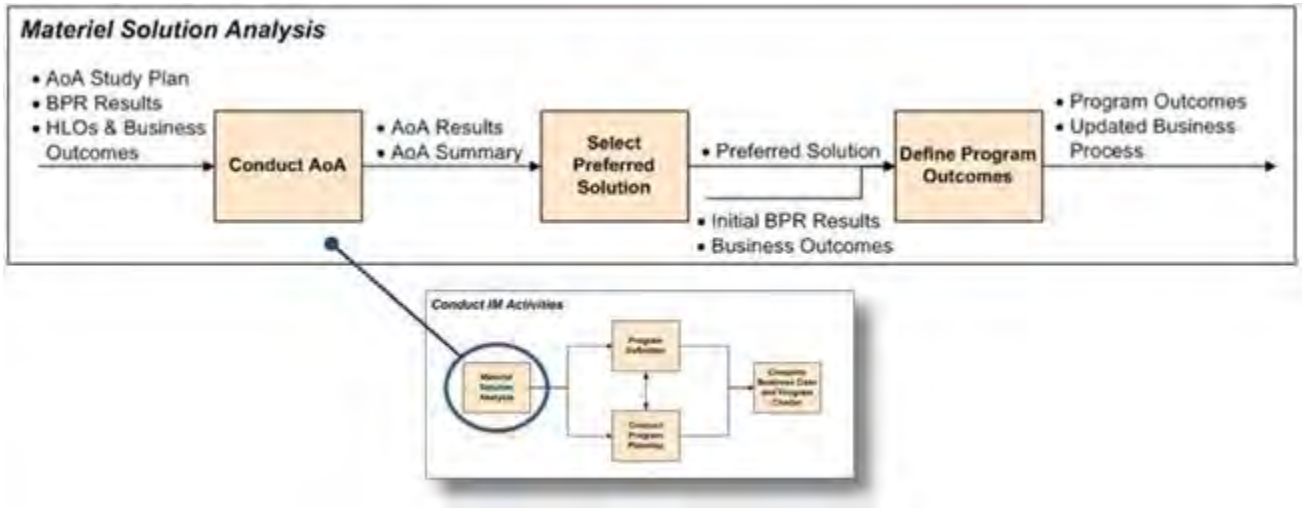


12.2.3.1. Conduct Materiel Solution Analysis

Conducting a Materiel Solution Analysis enables the Functional Sponsor to describe the needed requirements to achieve the high-level outcomes (HLOs) and business outcomes defined in the Problem Statement. Activities completed during the Material Solution Analysis include: conducting an analysis on each of the selected alternatives per the Analysis of Alternatives (AoA) Study Guidance along with their associated Doctrine, Organization, Training, Leadership and education, Personnel, Facilities, and Policy (DOT_LPF-P) impacts and risks; comparing each alternative against how well it will address the HLOs, business outcomes and their corresponding measures to solve

the business need; selecting a preferred solution based on criteria outlined in the AoA Study Guidance and Plan; and, developing and defining program outcomes. These activities are depicted in further detail in Figure **12.2.3.1.F1 .**

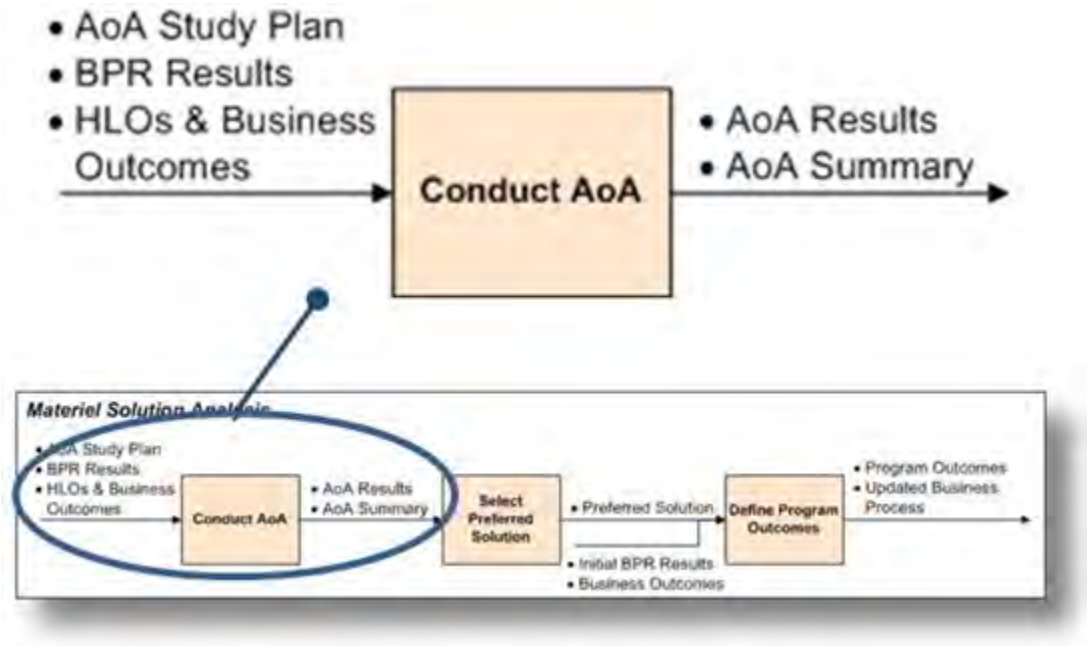
Figure 12.2.3.1.F1 - Decomposition of Materiel Solution Analysis



Conduct Analysis of Alternatives (AoA).

The AoA is an analytical study that is intended to compare the business capability, performance potential, operational effectiveness, cost, and risks of a number of potential alternative solutions to address the problem identified in the Problem Statement. Detailed information about conducting an AoA - including how to develop an AoA Study Plan - can be found in DAG Chapter 3, Section 3.3, "Analysis of Alternatives" .

Figure 12.2.3.1.F2 - Conduct AoA Context



Whereas JCIDS uses the Initial Capabilities Document (ICD) to guide the AoA, the AoA conducted during the IM Phase utilizes information from the Problem Statement and is directed by the AoA Study Guidance and Plan. It is critical that the results of the DOTMLPF-P Impact Assessment conducted during the BCD Phase are leveraged during the AoA.

During the AoA, the Functional Sponsor will leverage a team to assess each defined alternative and determine which will best solve the problem. Each alternative must be evaluated in terms of how well it addresses the HLOs, business outcomes, and measures in the Problem Statement and how well it fits into the "To-Be" state as defined by the initial Business Process Re-engineering (BPR). Any potential solution must also have the ability to become Business Enterprise Architecture (BEA) -compliant. A cost analysis (total life-cycle or total ownership, as appropriate) and cost effectiveness analysis on each alternative is conducted in addition to market research. The summary of these results is provided in the Business Case. The summary must include, at a minimum:

- A high-level explanation of the AoA process / methodology used;
- The type of market research conducted;
- The preferred alternative selection resulting from the AoA;
- Benefits and risks from the preferred alternative selection; and
- Any other information the Functional Sponsor deems appropriate for decision makers.

TIP: The HLOs and associated measures developed during the BCD phase should have been written to be independent of a particular solution (i.e., solution agnostic).

Something to avoid is the following scenario found during a GAO audit: DoD and service officials responsible for conducting AoA's indicated that often proposed capability requirements are so specific that they effectively eliminate all but the service sponsor's preferred concepts instead of considering other alternatives (GAO-09-655, September 2009).

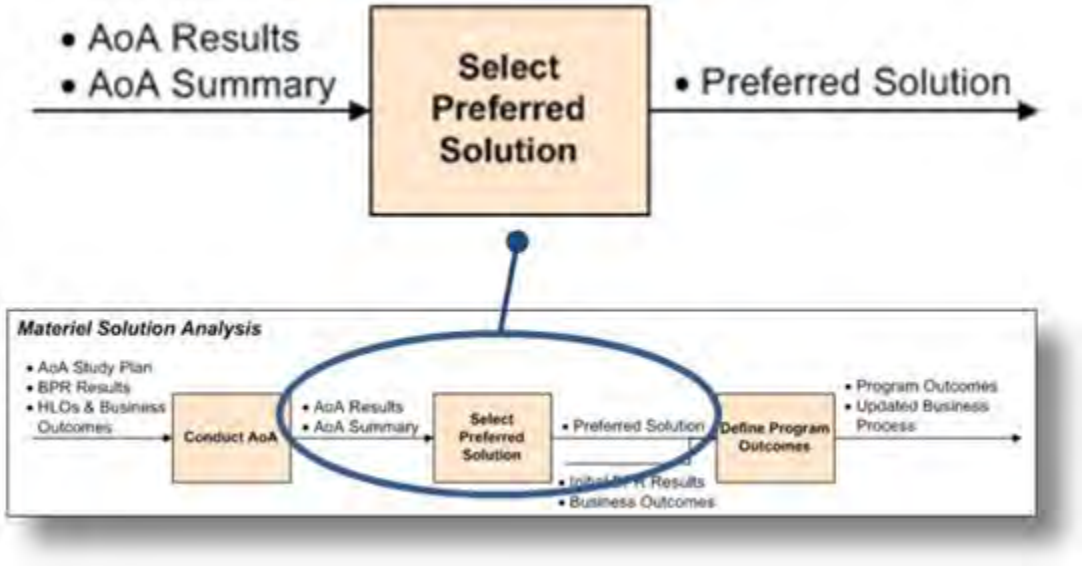
The following is a summary of the Conduct AoA activity:

- *Inputs.* AoA Study Plan (based on the approved Problem Statement and AoA Study Guidance), initial BPR results, HLOs and business outcomes, and corresponding measures.
- *Process.* The Functional Sponsor coordinates an AoA study team/working group and assesses each alternative using the approved AoA Study Guidance and AoA Study Plan. Together, the Functional Sponsor and team will, at a minimum, conduct market research, perform cost analysis and provide a summary of the alternatives (and the preferred solution) in the Business Case.
- *Outputs.* Solution options (AoA results), AoA summary documented in the Business Case.

Select Preferred Solution.

Once all alternatives have been analyzed according to the AoA Study Plan, the Functional Sponsor selects the best-value solution in terms of cost, best fit for providing the desired business capability, performance, support and other factors, for solving the problem as defined in the Problem Statement. The selection process takes into consideration impacts of potential tradeoffs, and the principles of Better Buying Power .

Figure 12.2.3.1.F3 - Preferred Solution Selection Context



TIP: The "best value" alternative does not always mean the least expensive. According to DoD ESI Best Value Toolkit , "best value" is defined as "the expected outcome of an acquisition that, in the Government's estimation, provides the greatest overall benefit in response to the requirement" . Thus, selecting a preferred solution should take into account other factors than just cost, such as performance or time, and most fundamentally, meeting the needs of the user.

The following is a summary of the Select Preferred Solution activity along with an example:

- *Inputs* . AoA results, AoA Summary.
- *Process.* Guided by the AoA Study Plan, the Functional Sponsor and the technical team, including appropriate subject matter experts (SMEs), analyze potential solutions by conducting a best-value determination (including consideration of Better Buying Power principles, tradeoffs, etc.). The resulting analysis will yield the preferred solution. The overall analysis is then summarized in the Business Case.
- *Outputs* . Preferred solution.

Preferred Solution Selection Example. An example of the preferred solution selection process comes from a general commercial off-the-shelf (COTS) software selection.

1. The Functional Sponsor and technical team review the following AoA results presented in a table format:

Solution Option 1: COTS (i.e., Oracle Financial Management (FM) software)

Solution Option 2: Hybrid solution (i.e., Oracle FM software and custom development)

Table 12.2.3.1.T1 - Example AoA Results

Alternative	Benefit's	Risks	Type of Cost Analysis	Cost Estimate
Oracle Financial Management e-business suite	Widely used commercially/ in DoD	High number of system interfaces	Life Cycle Cost (LCC)	$96M
Oracle FM+ custom development	Greatest chance of achieving HLOs	Complex software development	LCC	$110M

2. As part of the best-value determination, the Functional Sponsor and technical team perform tradeoff analysis. The purpose is to re-evaluate and update the unconstrained "To-Be" BPR conducted during the Business Capability Definition (BCD) Phase by analyzing it against the alternatives. The objective is to minimize software customization and to identify tradeoffs between the re-engineered "To-Be" state and the alternatives. Tradeoffs are those aspects of the re-engineered "To-Be" state that will need to be modified based on the selected alternative such as interfaces to other systems, business rules, and reports. Statute mandates that the commercial business process should be adopted to minimize customization of COTS products as opposed to customizing COTS software to match legacy practices. As a result of the analysis, the team develops the following conclusions about the two alternatives:

Alternative 1: Oracle Financials requires extensive tradeoffs in desired business capability, i.e., it does not allow for the type of feeder systems mandated by DoD Policy, and commercial business processes are different than the original "To-Be" process.

Alternative 2: Oracle Financials + custom development requires minimal tradeoffs; this will cost more and take more time. Also, the final software application will no longer be COTS.

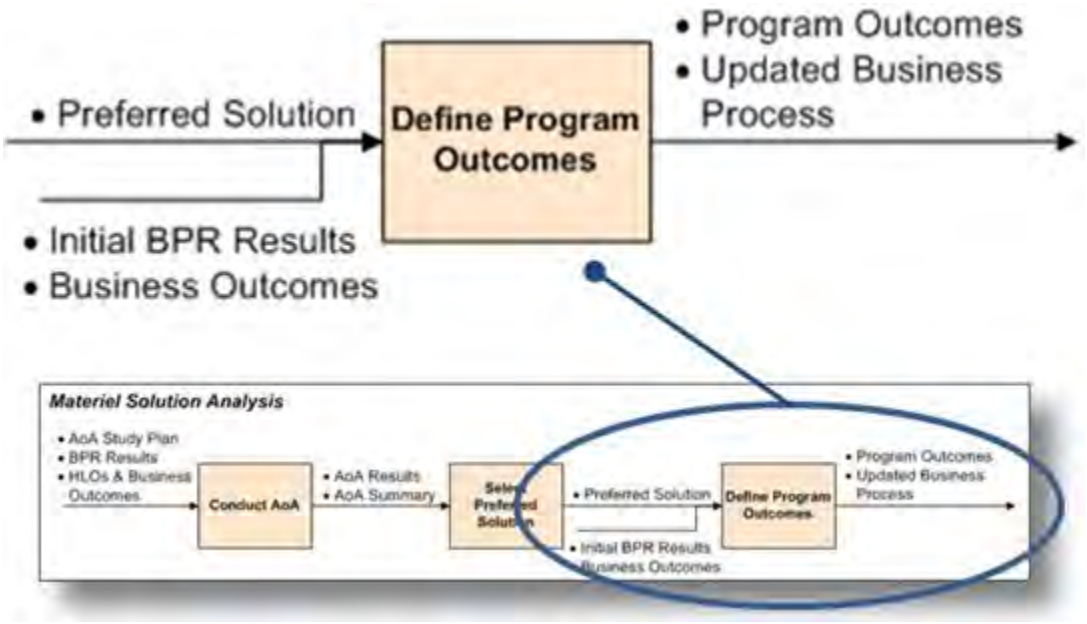
3. After careful consideration using best-value determination, the team selects the COTS alternative (Oracle Financials software) as their preferred solution. The team determined that it is feasible that the policy can be changed (added risk), and adopting the commercial business processes will help deliver the desired outcomes but will require additional training.

Define Program Outcomes.

After a solution has been selected as a result of the AoA, the Functional Sponsor along

with the Program Manager performs solution-specific BPR. This activity includes updating the "To-Be" process based on the business process inherent to the solution in addition to defining and prioritizing program outcomes based on the decomposition of HLOs and business outcomes first defined during the BCD Phase. The connected top-down framework of outcomes from a strategic to a more detailed level ensures continuity between the HLOs and program outcomes, and provides the basis for developing more specific system-level requirements to be tested against during Execution.

Figure 12.2.3.1.F4 - Define Program Outcomes Context



Program outcomes defined during the IM Phase should be specific enough to allow the association of functional requirements and non-functional requirements (i.e., DOT_LPF-P) during and beyond the Prototyping Phase. For example, if a program outcome identified during IM is: "Administration capability for role-based authorization", then an associated functional requirement may be: "The system shall enable a user with the role of System Administrator to assign one or more roles to a user of the system".

TIP: Detailed system-level requirements do not typically belong in the Business Case and should be kept at the program-level with other detailed program-level operational or execution-level documentation.

The following is a summary of the Define Program Outcomes activity along with an example:

- *Inputs.* Preferred solution, initial BPR results, HLOs and business outcomes and their corresponding measures, benefit's, risks, assumptions, constraints, and dependencies.

- *Process.* The Functional Sponsor decomposes the HLOs and business outcomes into more specific program outcomes (e.g., what specific functions the potential program will perform) based on the initial BPR results, the preferred solution, and any previous requirements tradeoffs. Up to now, the business outcomes/Capabilities have been driven by the BEA-defined end-to-end (E2E) business flows, business processes, and capabilities. Now that a preferred solution has been selected the "To-Be" business process may have to be revised to accommodate the preferred solution and any tradeoffs made during the analysis. If the updated business process ("To-Be) causes gaps between it and the BEA a determination will have to be made regarding issuing a waiver or filling the gap in the BEA for its next release. Program outcomes must also have associated measures, benefit's, risks, assumptions, constraints, and dependencies. A summary of this information is then documented in the Business Case as appropriate.
- *Outputs.* Program outcomes and their measures, benefit's, risks, assumptions, constraints, and dependencies; and, the updated business process.

Program Outcome Definition Example. An example of defining program outcomes comes from the Defense Agencies Initiative (DAI):

1. The Functional Sponsor determined the program outcome that aligns to the HLOs and business outcome(s):

HLO: Accurate, useful, reliable and timely financial data and management information

Business Outcome: Consistency with financial and Information Assurance standards

Program Outcome: Financial controls/internal controls

Program Outcome Definition: Ensure financial controls and internal controls are embedded in the financial solution to prevent material weaknesses, and ensure budgetary integrity by establishing financial control over funds, obligations, assets, and liabilities.

2. The Functional Sponsor conducts additional BPR refinement, if necessary. In this example, the Functional Sponsor has determined the initial BPR was silent on audit trails so an additional program outcome was added to the business outcome as follows:

HLO: Accurate, useful, reliable and timely financial data and management information

Business Outcome: Consistency with financial and Information Assurance standards

Program Outcome: Audit Trail

Program Outcome Definition: A record of transactions is referenced on-demand to:

trace activities to original documents and verify account balances.

3. The Functional Sponsor specified characteristics of the program outcome including: measurements, benefit's, risks, assumptions, constraints, and dependencies:

Program Outcome: Implement Financial / internal controls

Measurement: Compliance with the financial / internal controls requirements as defined in OMB Circular A-123.

Current Baseline Value: 0%

Targeted Threshold Value: 75%

Targeted Objective Value: 100%

Benefit's: Integrity of financial information

Risks: Ability to achieve component consensus on information requirements; quality of legacy data

Assumptions: Financial information will be entered correctly into the system

Constraints: The information must be reported to Congress annually

Dependencies: The solution requires multiple interfaces

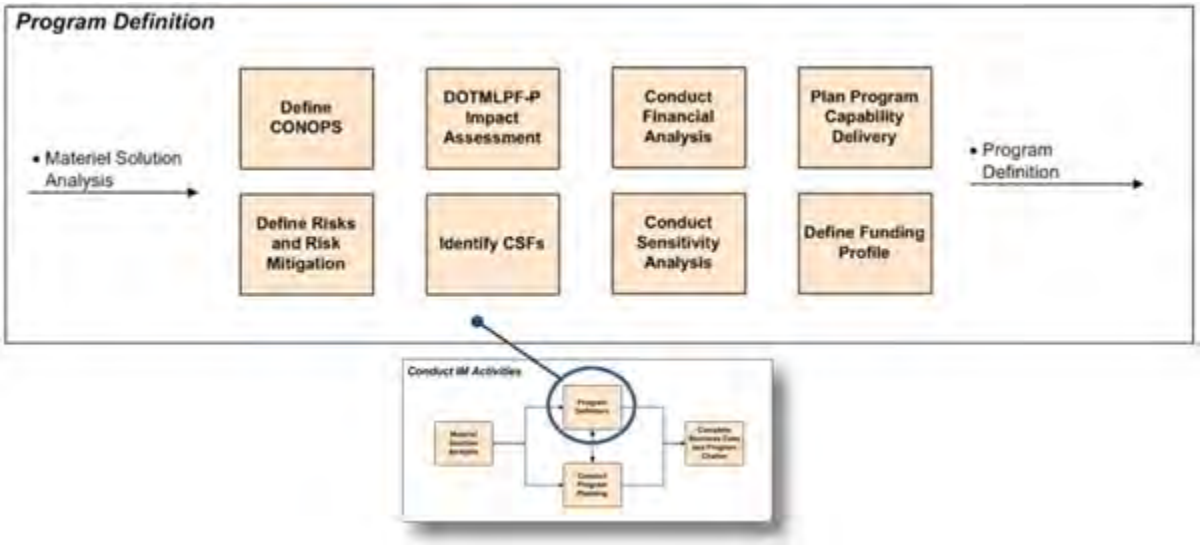
12.2.3.2. Program Definition

12.2.3.2. Program Definition

Once the Materiel Solution Analysis is complete, the program manager and Functional Sponsor must define and describe the potential program in preparation for future reviews and decisions by the Investment Review Board (IRB) and / or Milestone Decision Authority (MDA) prior to and during program execution. This includes: defining a properly scoped Concept of Operations with assumptions; updating the Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P) Assessment; identifying any additional risks and developing a risk mitigation plan; identifying Critical Success Factors (CSFs); conducting a financial and sensitivity analysis; developing a funding profile and a capability delivery schedule; and, preparing the necessary information to be summarized in the Business Case and Program Charter. The order of activities conducted during Investment Management (IM) is based on what makes sense for a particular program; in fact, many of the activities may be conducted simultaneously. It's important to note that during Program Definition various program-level documents will start to be developed to capture key information

that will inform program planning. These activities are depicted in Figure 12.2.3.2.F1 .

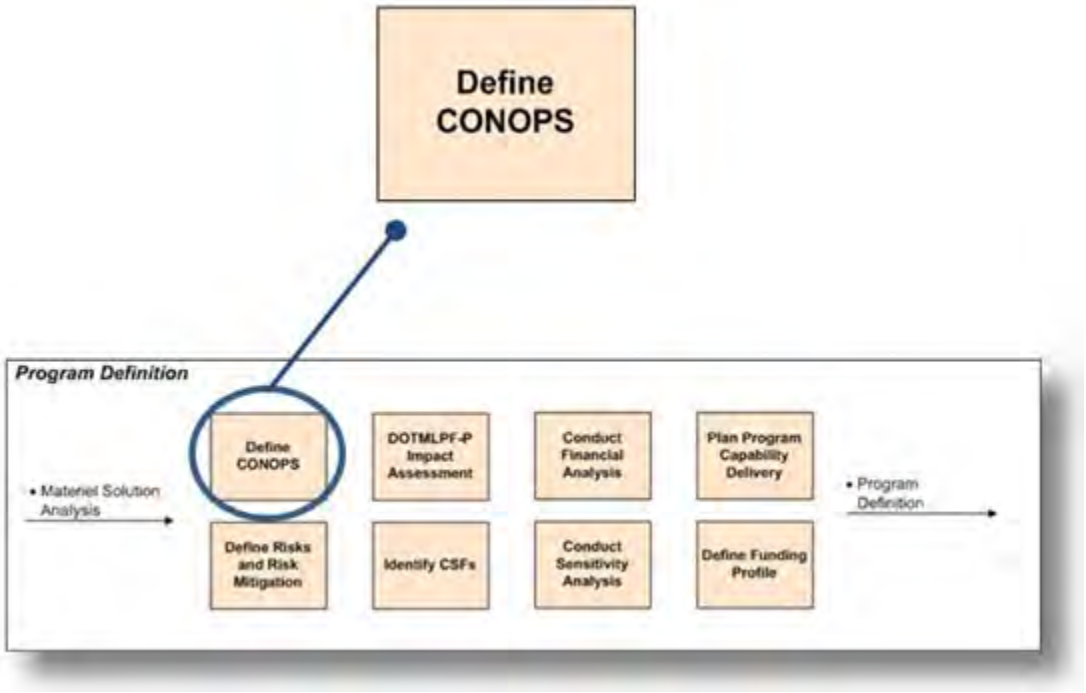
Figure 12.2.3.2.F1 - Decomposition of Program Definition



Define Concept of Operations (CONOPS).

The purpose of this activity is to describe the characteristics of a proposed program from the viewpoint of an individual who will use the system. The Concept of Operations (CONOPS) is used to communicate the quantitative and qualitative program characteristics to all stakeholders. It evolves from a concept and describes, at a minimum, how the proposed set of capabilities will be integrated to achieve desired outcomes. Ideally it offers a clear methodology to realize the program goals and objectives (i.e., outcomes, while not intending to be an implementation or transition plan).

Figure 12.2.3.2.F2 - Define CONOPS Context



At a minimum, the CONOPS should include: the working relationships of key stakeholders using or contributing to the solution; how the various levels of outcomes defined will integrate to solve the problem; and a high-level view of the architecture for the solution, such as an OV-1 diagram (operational view).

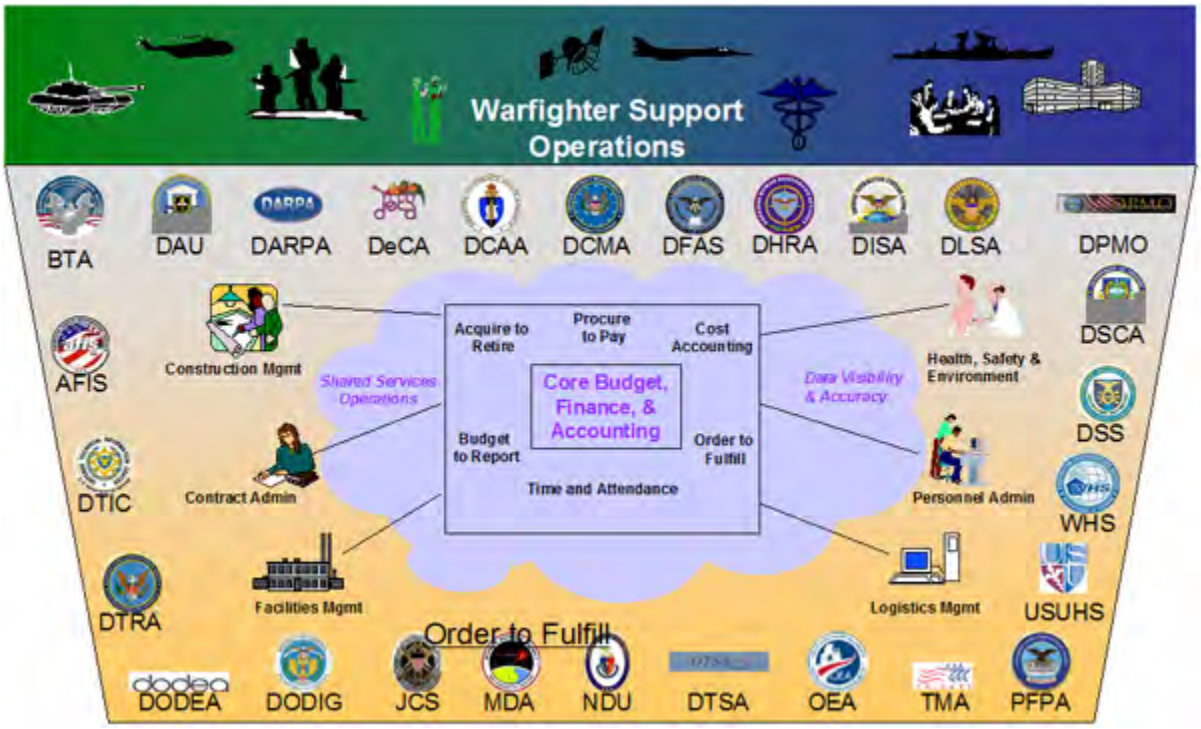
TIP: Remember that the CONOPS provides decision makers with a general overview of the potential program based on the preferred solution. While creating the CONOPS, it may be helpful to consider what, as a decision maker, you would like to see presented that would give you the best overall picture of how the potential program will be structured.

The following is a summary of the Define CONOPS activity along with an example OV-1 depiction from program documents:

- *Inputs.* Preferred solution, program outcomes, and updated business process resulting from the Materiel Solution Analysis.
- *Process.* The Functional Sponsor and program manager utilize expert judgment based on their collective knowledge of business and information technology (IT) systems to provide a vision that best conveys to decision makers how the system (preferred solution) would operate from a user perspective.
- *Outputs.* CONOPS, including an OV-1 diagram. This is summarized / depicted in the Business Case.

CONOPS Example. An example of an OV-1 diagram, shown in Figure **12.2.3.2.F3** , ***is from the Defense Agencies Initiative (DAI) Program:***

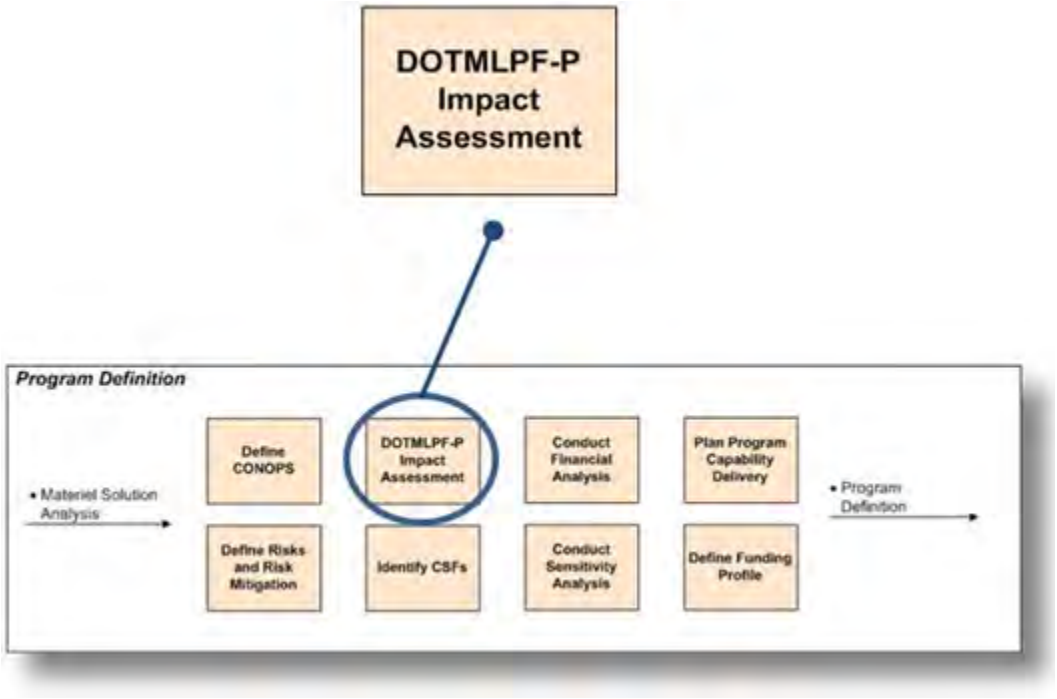
Figure 12.2.3.2.F3 - Example of an OV-1 Diagram



DOTMLPF-P Impact Assessment.

The purpose of this analysis is to understand the effects on any DOT_LPF-P elements now that the Functional Sponsor has selected the preferred materiel solution. The results may differ from the "To-Be" DOT_LPF-P assessment performed during the Business Capability Definition (BCD) Phase, particularly if a COTS product is chosen and the "To-Be" process needs to be changed to minimize customization. In summary, the process is meant to identify which non-materiel elements must be addressed to deliver the capability as intended. The Functional Sponsor is responsible and accountable for implementing non-materiel components of the solution.

Figure 12.2.3.2.F4 - DOTMLPF-P Impact Assessment Context



The Functional Sponsor and PM lead the effort to determine which changes, if any, need to be made to the previous "To-Be" assessment performed in the BCD Phase. This DOTMLPF-P Impact Assessment is based on emerging information resulting from the preferred solution, updated Business Process Re-engineering (BPR), and the program outcomes and corresponding measures defined in the previous activity.

The following is a summary of the DOTMLPF-P Impact Assessment activity along with an example of the summary output that may appear in the Business Case (*Note* : more detailed information does not need to appear in the Business Case, and may be kept as "working papers"):

- *Inputs.* Preferred solution, program outcomes, and updated business process resulting from the Materiel Solution Analysis.
- *Process.* Functional and acquisition subject matter experts (SMEs) consider the DOTMLPF-P elements that will be impacted within the "To-Be" state based on the preferred solution and any evolving BPR changes. A summary of the impact is recorded in the Business Case.
- *Outputs.* Identification of DOTMLPF-P Impacts. A summary of the analysis recorded in the Business Case, which includes a list of each DOTMLPF-P Impact and how it must change if the "To-Be" business process is realized. Any risks not associated with addressing the impacts should be identified and added to the program's risk management tool.

DOTMLPF-P Impact Assessment Example. An Example DOTMLPF-P Impact

Assessment is based on using a commercial off-the-shelf (COTS) package per the revised "To-Be" business process, as summarized in the Business Case:

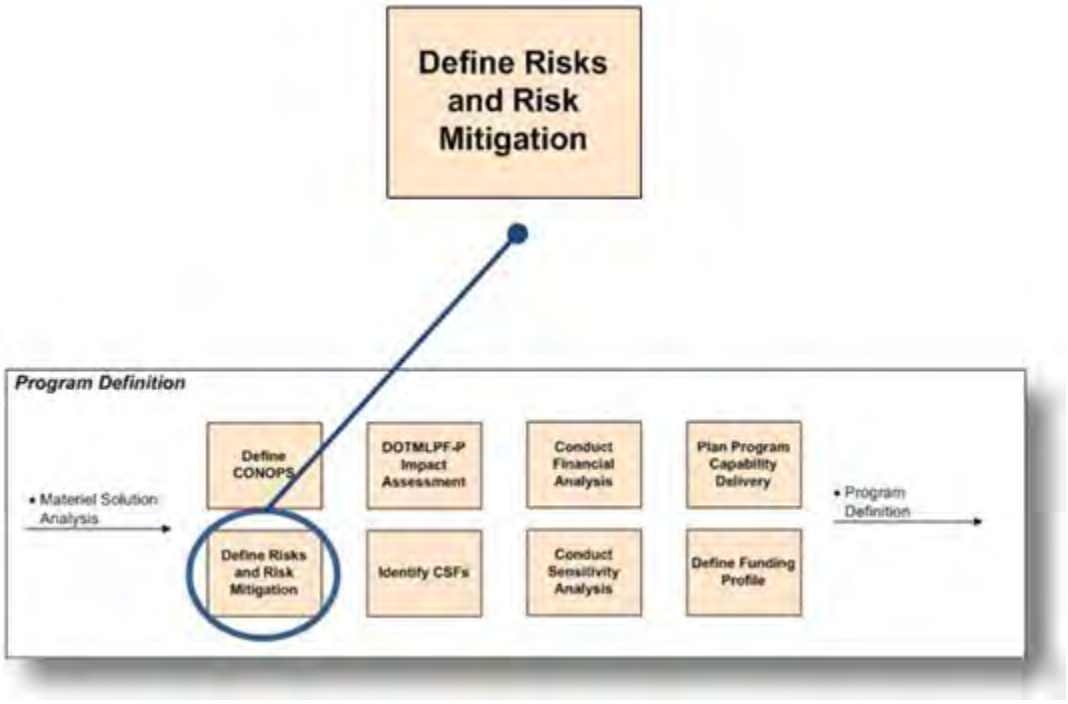
Table 12.2.3.2.T1 - Example of a "To-Be" DOTMLPF-P Impact Assessment

DOTMLPF Element	Impact
Doctrine:	Development of new and revised operating procedures is required.
Organization:	Organization changes are required in order to accommodate the built-in COTS business flow and BPR.
Training:	A new training course is required and Personnel need ongoing access to the training.
Materiel:	The COTS package must be configured and existing systems must be enhanced or replaced to optimize the capabilities and business processes. Will require some custom code to build interfaces.
Leadership and Education:	No impact identified.
Personnel:	All Personnel in the call center will be trained for the revised Roles defined for the enhanced or new system.
Facilities:	The COTS package will require new servers and must run on the GiG. New network equipment must be upgraded at various locations to facilitate increase in transactions.
Policy **:**	The policy mandating the use of existing accounting system must be changed to allow for optimal use of COTS and minimizing interfaces and customization to overcome data quality/standards issues.

Define Risks and Risk Mitigation.

Eliminating all risk is not feasible. Identifying risks early and continuously throughout the lifecycle and developing a plan to mitigate them is part of successful program management. Most business executives ask the following questions: what problem are we trying to solve; what's the benefit; how much will it cost; and what are the risks? Having an effective risk mitigation strategy will go a long way towards gaining buy-in from senior leadership and provide the program manager with information to plan for risk management.

Figure 12.2.3.2.F5 - Define Risks and Risk Mitigation Context



For information on identifying, mitigating and tracking risk, refer to sections 3 and 5 respectively of the Risk Management Guide for DoD Acquisition, August 2006 .

TIP: Generally, the Risk Management Guide refers to outputs from activities occurring later in the process (i.e., developing a work breakdown structure (WBS), earned value management (EVM), testing); however, based on lessons-learned, the chances of success are dramatically increased by effective risk mitigation. Therefore BCL encourages risk identification and mitigation early and continuously throughout the life of the program.

The following is a summary of the Defining Risks and Risk Mitigation activity along with an example:

- *Inputs.* DOTMLPF-P impacts, all risks identified to-date.
- *Process.* Based on the risk management plan in the Program Charter, SMEs from the functional and technical teams consider each of the previously identified risks (associated with DOTMLPF-P impacts) and identify any additional "hidden" risks. The SMEs will estimate the probability of each risk occurring and impact if the risk occurs and then identify the appropriate risk mitigation counter-measures. The SMEs forward all this information to the program manager to incorporate into the program's risk management plan. The program manager must initiate a method for tracking risk based on the risk management approach; define risk management activities and summarize key high risk elements in the Business Case. Detailed output of risk analysis is typically recorded in a risk

register or risk log at the program execution level and an individual is assigned responsibility to each risk. For additional information on risk management, view the Risk Management Guide for DoD Acquisition, August 2006 .

- *Outputs.* Prioritized Risks, Risk Mitigation Strategy.

A risk register or risk log is a repository of identified risks for the program. For each risk, additional information is included such as the risk's probability of occurrence, impact of occurrence, planned counter-measures (or risk mitigation), risk owner, and other pertinent information. An example of risk register or risk log is shown in Table **12.2.3.2.T2** .

Risk and Risk Mitigation Example Summarized in the Business Case .

Table 12.2.3.2.T2 - Example of the Output of Risk and Risk Mitigation Activity

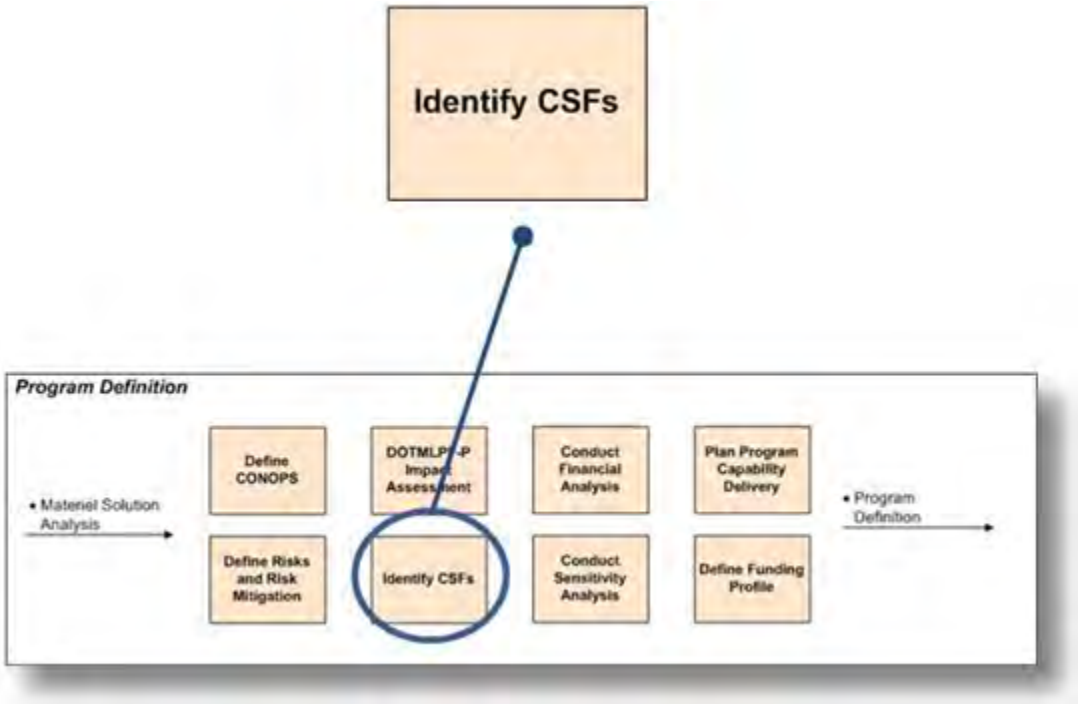
Risk	**Probability of Occurrence**	**Impact of Occurrence**	**Risk Mitigation**	**Risk Owner**
Inability to meet non-discretionary deadline for designated high-priority business capabilities.	High	Medium	Defer discretionary requirements to future Increment - manage customer expectations when this mitigation strategy is exercised. Monitor earned progress and *shift resources* from lower priority work when indicators suggest the schedule could be at risk.	PM

System interface from a required feeder system is not ready on-time for implementation.	High	High - may cause delay or additional resources	Sign an MOU/MOA with each system interface owner. Include technical reps in design discussions and publish a formal interface design specification. Conduct early testing of data exchanges. Develop contingency plan in case a suitable workaround becomes necessary.	PM

Identify Critical Success Factors.

Critical Success Factors (CSFs) inform stakeholders of those elements that are deemed must-haves for the potential program to succeed and identify the factors that stakeholders agree must be implemented to achieve Initial Operational Capability (IOC). The advantage of identifying CSFs is that they are simple to understand and they help focus attention on major concerns. This will influence requirements tradeoff analysis conducted during the Prototyping Phase as the Functional Sponsor and program manager define and scope each increment of capability delivery.

Figure 12.2.3.2.F6 - Identify CSFs Context



The following is a summary of the Identify CSFs activity along with an example list of CSFs summarized in the Business Case:

- *Inputs.* High impact risks and risk mitigation strategy, preferred solution, program outcomes and DOTMLPF-P impacts from the "To-Be" assessment.
- *Process.* From the inputs listed above, the program manager (PM), Functional Sponsor and SMEs from the functional and technical teams develop a list of prioritized CSFs. CSFs are the elements deemed as must-haves for the program to achieve the desired outcomes and may include factors outside the program manager's control. The CSFs become candidates for subsequent program management planning. For example: a CSF is proposed for the use of a requirements management tool. The program manager decides the tool is both essential and cost effective, so plans are made to acquire, install, and operate the tool.
- *Outputs.* List of CSFs summarized in the Business Case.

TIP: CSFs should differ from Key Performance Indicators (KPIs) which are measures that quantify management objectives, along with a target or threshold, and enable the measurement of strategic performance.

Example Critical Success Factors.

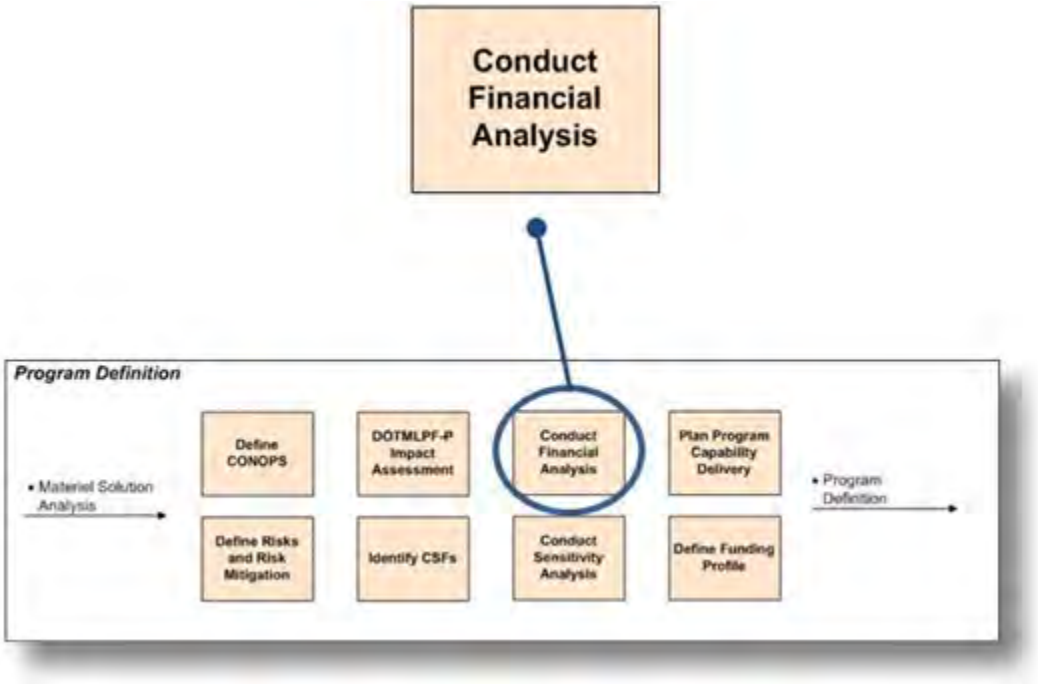
- Commitment from Functional Sponsor and executives
- Adequate training and change management

- Team knowledgeable in implementing large-scale ERP
- User involvement

Conduct Financial Analysis.

A financial analysis evaluates the cost and benefit of the proposed program in relation to the current "as-is" operation in order to define the planned investment and obtain greater efficiency and productivity in defense spending (i.e., Better Buying Power). For a MAIS program, an Economic Analysis (EA) is also conducted to evaluate alternatives for meeting objectives based on the present value of life-cycle costs and financial benefit's.

Figure 12.2.3.2.F7 - Conduct Financial Analysis Context



More detailed guidance for developing and preparing EA and Life-Cycle Cost (LCC) estimates can be found in DAG Chapter 3, Section 3.6, "Major Automated Information Systems Economic Analysis" and Section 3.7 "Principles for Life-Cycle Cost (LCC) Estimates" . The LCC estimate and EA are summarized in the Business Case for the MS A and MS B reviews.

Below are basic inputs, processes, and outputs of the Conducting a Financial Analysis activity:

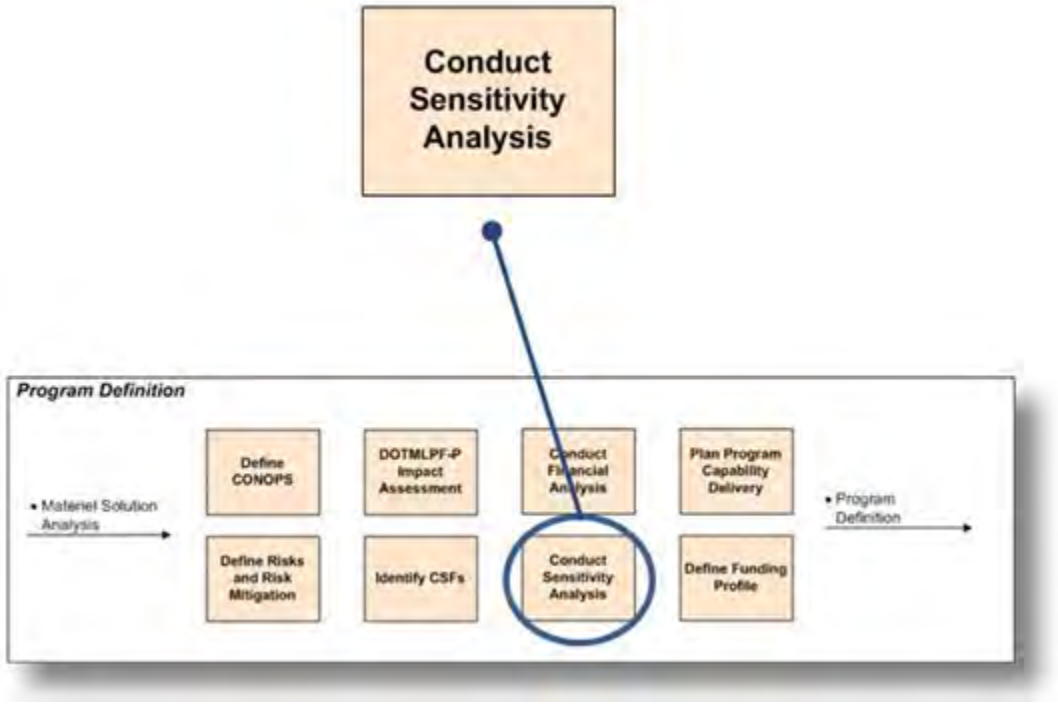
- *Inputs.* Concept of operations (CONOPS), Material Solution Analysis results.
- *Process.* The program manager and Functional Sponsor will develop the analytic approach and scope for preparing the LCC estimate. Based on the results of the

Material Solution Analysis and the CONOPS, they will conduct the following activities:
    - Develop the program's Work Breakdown Structure (WBS) for all work necessary to: 1) meet requirements; 2) manage risks; and 3) obtain greater efficiency and productivity in defense spending (i.e., Better Buying Power).
    - Based on the WBS, prepare the LCC Estimate using planned estimating techniques.
    - Estimate the financial benefit's based on the qualitative benefit's documented in the Business Case.
    - Prepare a high-level, resource-loaded milestone schedule.
    - For MAIS programs, conduct an EA, including a calculation of return on investment (ROI).
- *Outputs.* WBS, Schedule, LCC Estimate, and financial benefit's estimate; an EA for MAIS programs.

Conduct Sensitivity Analysis.

Sensitivity analysis is based on cost, schedule and performance (requirements prioritization) trades and is used to help the program manager and Functional Sponsor evaluate the effect on estimates when assumptions or cost-drivers change. As a result of this analysis, they can then plan appropriate actions and determine how increments will be developed to meet prescribed time-limit's and avoid prospective schedule delays and cost overruns.

Figure 12.2.3.2.F8 - Conduct Sensitivity Analysis Context



The result may be refinement of time, cost and performance boundaries of the program and a corresponding increase in the degree of confidence in the LCC Estimate. This is the initial step where the PM is going to define what can be done in the first increment, and what needs to be done in follow-on increments.

More information and guidance can be found in DAG Chapter 3, Section 3.7.2.4, "Assess Risk and Sensitivity" .

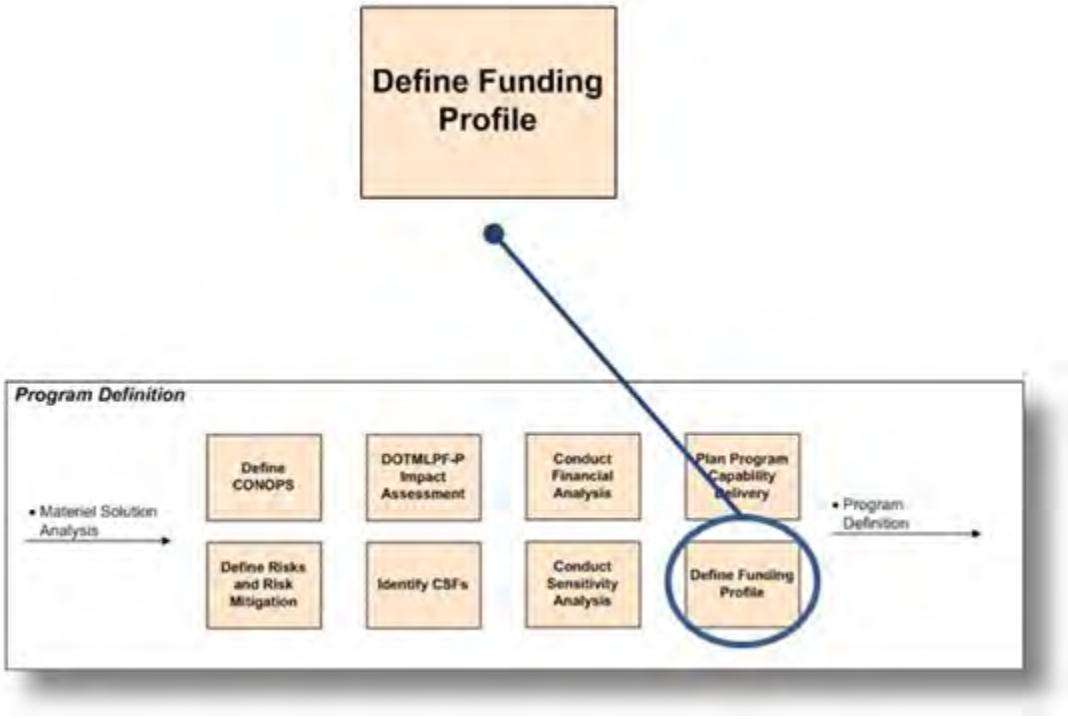
The following is a summary of the Conduct Sensitivity Analysis activity:

- *Inputs.* LCC Estimate, Financial Benefit's Estimate, financial risks, assumptions, parameters for the sensitivity analysis, and, for MAIS programs, an EA.
- *Process.* The PM, Functional Sponsor, and analyst(s) will plan the data and parameters for conducting sensitivity analysis. They will review the resulting sensitivity analysis report and plan appropriate actions to help avoid prospective schedule delays and cost overruns. The planned actions may affect the time, cost, and performance boundaries being defined for the program as well as increase the degree of confidence in the LCC Estimate. Sensitivity analysis may need to be conducted in conjunction with risk management planning in order to consider qualitative and quantitative risk management information.
- *Outputs* . Results of Sensitivity Analysis.

Define Funding Profile.

Once the Financial and Sensitivity Analyses are complete, and in conjunction with resource management activities of program management, the program manager will prepare a Funding Profile that documents the proposed overall strategy for funding the program. Defining a Funding Profile is essential for ensuring program stability over its planned lifecycle and for providing a disciplined approach for program managers to execute their programs within cost and available funding. The Functional Sponsor is ultimately responsible for ensuring that funding is identified and obtained.

Figure 12.2.3.2.F9 - Define Funding Profile Context



The Define Funding Profile activity includes considerations from every other activity conducted during the Investment Management (IM) Phase. During the Define Funding Profile activity, the Functional Sponsor and program manager reviews the Business Case and determines that the Funding Profile adequately supports the program being planned. This should include a review of:

- Requirements (i.e., the planned high-level outcomes (HLOs) and business and program outcomes) to ensure the program is funded in order to meet those requirements;
- Planned deliverables of the program to ensure they are adequately funded - for example preparing and implementing the Test Plan; and
- Other aspects of the program to verify adequate funding, such as: the Acquisition Approach, potential risks as a result of the Sensitivity Analysis, and the Financial

Risks considered as a part of the Risk Management process. This includes verification of adequate funding for the costs associated with planned risk mitigation activities.

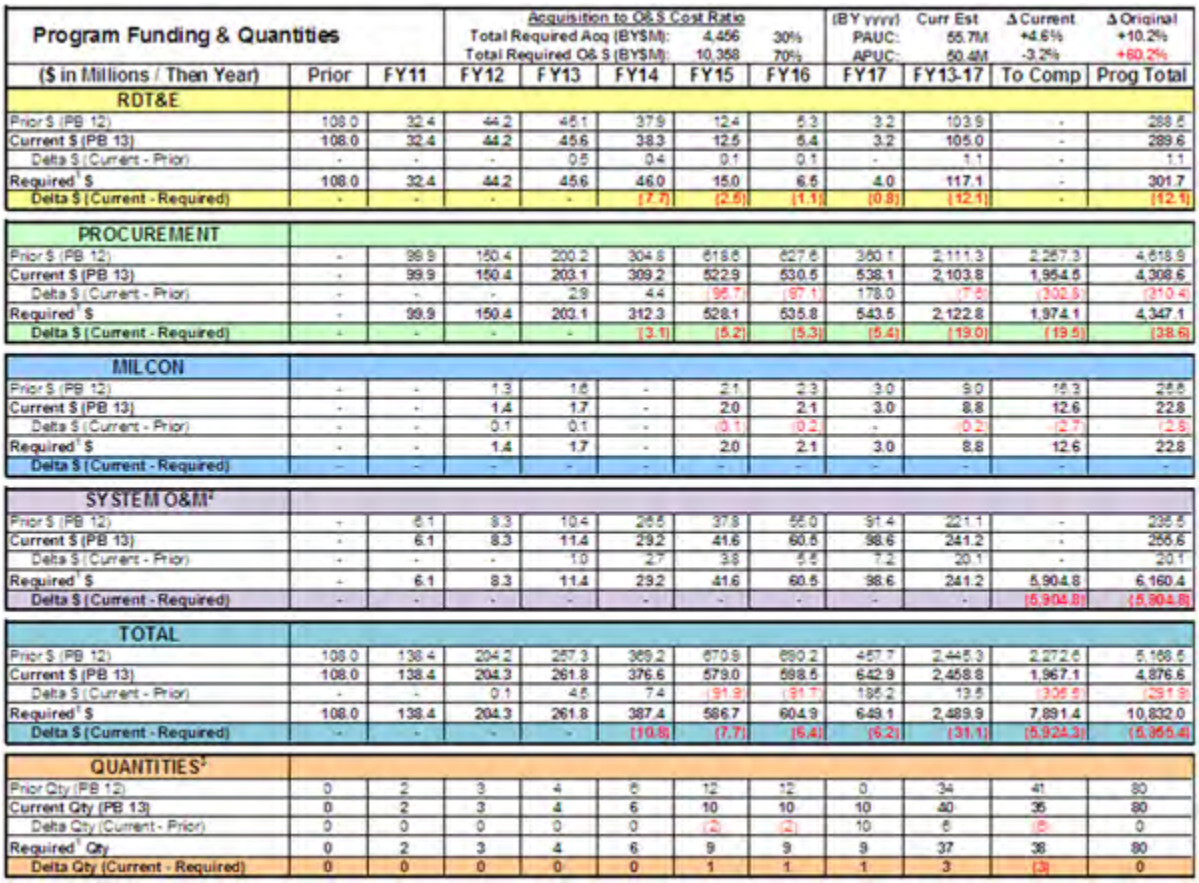
TIP: Generally, not all risks are avoidable so Funding Profile development should also include a verification that planned costs are reasonable in order to manage the issues that result from risks that materialize.

The following is a summary of the Define a Funding Profile activity along with an example Funding Chart:

- *Inputs.* Results of Sensitivity Analysis, financial risks, assumptions, parameters (including budget information).
- *Process.* The program manager will prepare a funding profile.
- *Outputs.* Funding profile (including a funding chart).

Funding Chart Example . Example of the latest Funding Chart used at a Defense Acquisition Board (DAB) . **(**Note: Requires login with password or Common Access Card)**

Figure 12.2.3.2.F10 - Example Funding Profile

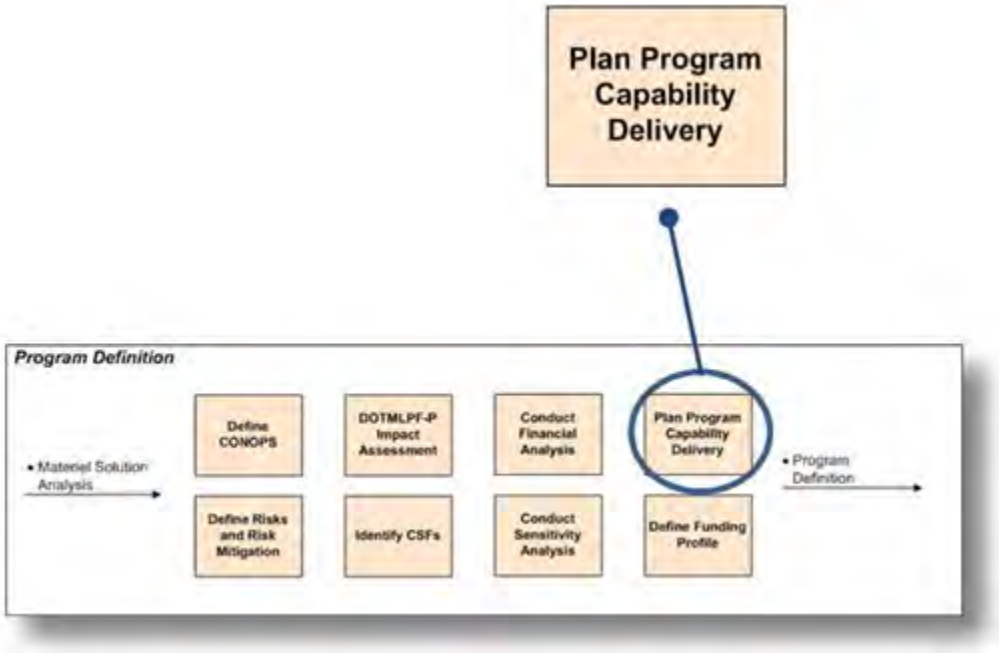


Program Funding & Quantities			Acquisition to O&S Cost Ratio					(BY yyyy)	Curr Est	Δ Current	Δ Original
			Total Required Acq (BY$M):			4,456	30%	PAUC:	55.7M	+4.6%	+10.2%
			Total Required O& S (BY$M):			10,358	70%	APUC:	50.4M	-3.2%	+60.2%
($ in Millions / Then Year)	Prior	FY11	FY12	FY13	FY14	FY15	FY16	FY17	FY13-17	To Comp	Prog Total
RDT&E											
Prior $ (PB 12)	108.0	32.4	44.2	45.1	37.9	12.4	5.3	3.2	103.9	-	288.6
Current $ (PB 13)	108.0	32.4	44.2	45.6	38.3	12.5	6.4	3.2	105.0	-	289.6
Delta $ (Current - Prior)	-	-	-	0.5	0.4	0.1	0.1	-	1.1	-	1.1
Required[1] $	108.0	32.4	44.2	45.6	46.0	15.0	6.5	4.0	117.1	-	301.7
Delta $ (Current - Required)	-	-	-	-	(7.7)	(2.5)	(1.1)	(0.8)	(12.1)	-	(12.1)
PROCUREMENT											
Prior $ (PB 12)	-	99.9	150.4	200.2	304.8	618.6	627.6	360.1	2,111.3	2,257.3	4,618.9
Current $ (PB 13)	-	99.9	150.4	203.1	309.2	522.9	530.5	538.1	2,103.8	1,954.5	4,308.6
Delta $ (Current - Prior)	-	-	-	2.9	4.4	(95.7)	(97.1)	178.0	(7.5)	(302.8)	(310.4)
Required[1] $	-	99.9	150.4	203.1	312.3	528.1	535.8	543.5	2,122.8	1,974.1	4,347.1
Delta $ (Current - Required)	-	-	-	-	(3.1)	(5.2)	(5.3)	(5.4)	(19.0)	(19.5)	(38.6)
MILCON											
Prior $ (PB 12)	-	-	1.3	1.6	-	2.1	2.3	3.0	9.0	16.3	25.8
Current $ (PB 13)	-	-	1.4	1.7	-	2.0	2.1	3.0	8.8	12.6	22.8
Delta $ (Current - Prior)	-	-	0.1	0.1	-	(0.1)	(0.2)	-	(0.2)	(2.7)	(2.9)
Required[1] $	-	-	1.4	1.7	-	2.0	2.1	3.0	8.8	12.6	22.8
Delta $ (Current - Required)	-	-	-	-	-	-	-	-	-	-	-
SYSTEM O&M[2]											
Prior $ (PB 12)	-	6.1	8.3	10.4	24.6	37.8	56.0	91.4	221.1	-	235.6
Current $ (PB 13)	-	6.1	8.3	11.4	29.2	41.6	60.5	98.6	241.2	-	255.6
Delta $ (Current - Prior)	-	-	-	1.0	2.7	3.8	4.5	7.2	20.1	-	20.1
Required[1] $	-	6.1	8.3	11.4	29.2	41.6	60.5	98.6	241.2	5,904.8	6,160.4
Delta $ (Current - Required)	-	-	-	-	-	-	-	-	-	(5,904.8)	(5,904.8)
TOTAL											
Prior $ (PB 12)	108.0	138.4	204.2	257.3	369.2	670.9	690.2	457.7	2,445.3	2,272.6	5,168.5
Current $ (PB 13)	108.0	138.4	204.3	261.8	376.6	579.0	598.5	642.9	2,458.8	1,967.1	4,876.6
Delta $ (Current - Prior)	-	-	0.1	4.5	7.4	(91.9)	(91.7)	185.2	13.5	(305.5)	(291.9)
Required[1] $	108.0	138.4	204.3	261.8	387.4	586.7	604.9	649.1	2,489.9	7,891.4	10,832.0
Delta $ (Current - Required)	-	-	-	-	(10.8)	(7.7)	(6.4)	(6.2)	(31.1)	(5,924.3)	(5,955.4)
QUANTITIES[3]											
Prior Qty (PB 12)	0	2	3	4	6	12	12	0	34	41	80
Current Qty (PB 13)	0	2	3	4	6	10	10	10	40	35	80
Delta Qty (Current - Prior)	0	0	0	0	0	(2)	(2)	10	6	(6)	0
Required[1] Qty	0	2	3	4	6	9	9	9	37	38	80
Delta Qty (Current - Required)	0	0	0	0	0	1	1	1	3	(3)	0

Plan Program Capability Delivery.

To provide best-value to the Department and deliver planned business capabilities to the user within BCL time constraints, the program manager and Functional Sponsor should properly scope and allocate the delivery of planned business capabilities (i.e., Program Outcomes) for the potential program across multiple increments. This approach provides the program manager and Functional Sponsor with the ability to deliver high-value business capabilities and flexibility to reduce overall program risk by creating more manageable increments of work.

Figure 12.2.3.2.F11 - Plan Program Capability Delivery Context



This is a high-level program plan depicting the planned number of increments. Ultimately each increment will be planned in detail and summarized in the Business Case at a high level during the Prototyping Phase; however, for now, this is an estimated overall plan that should include, at a minimum, the overall capability to be delivered, the planned number of increments, and key program-driven events.

The following is a summary of Plan Program Capability Delivery activity:

- *Inputs.* Life-Cycle Cost Estimate, estimated schedule and performance from the Financial Benefit Analysis.
- *Process.* The program manager and Functional Sponsor review the cost, schedule, and performance planned for the potential program during the Program Definition section of the IM Phase (i.e., the Financial Benefit Analysis). They plan the program capability delivery approach based on prioritized requirements. Increments are defined to support the program capability delivery approach. The Program Capability Delivery Plan can be best depicted in a graphic summarized in the Business Case.
- *Outputs.* Capability Delivery Plan summarized in the Business Case.

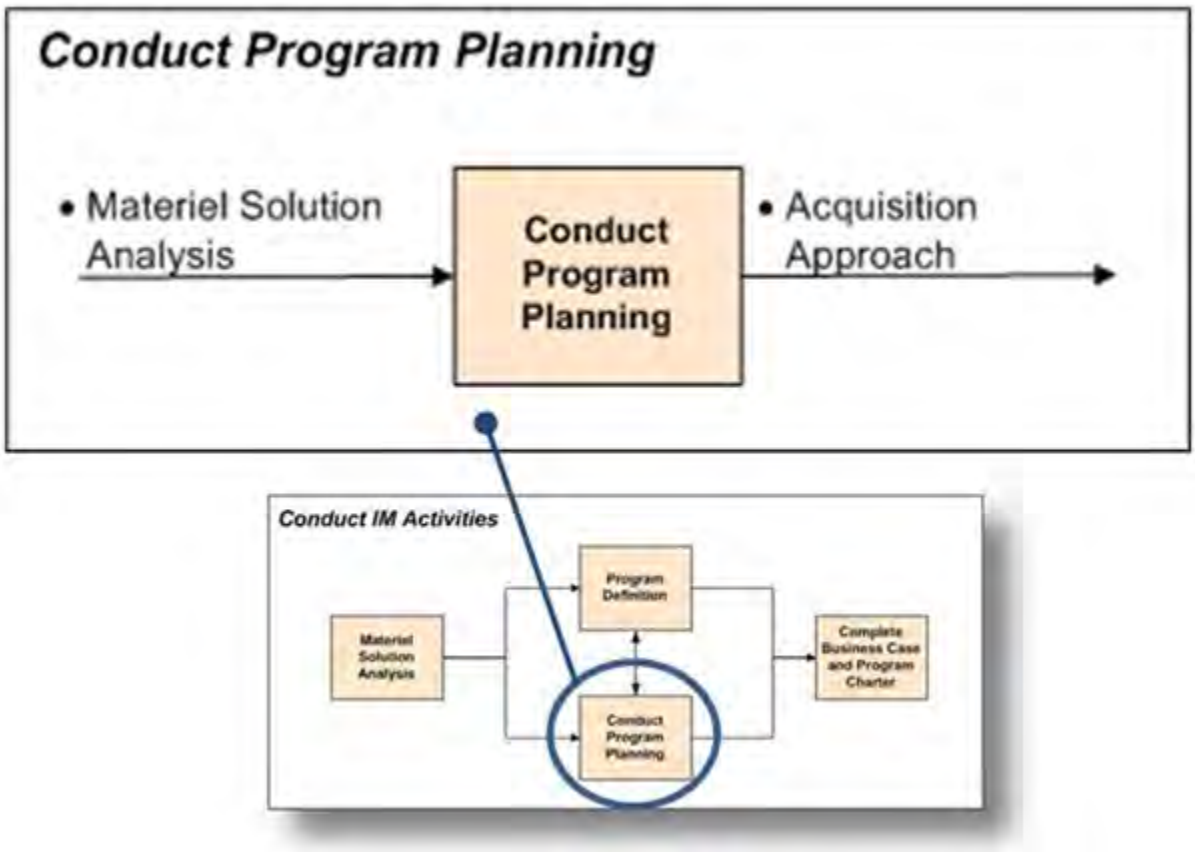
12.2.3.3. Conduct Program Planning

12.2.3.3. Conduct Program Planning

Program Planning activities begin after the Material Solution Analysis has been completed and in conjunction with Program Definition activities and includes, but is not

limited to, developing plans for the following: test and evaluation, systems engineering, lifecycle sustainment, data migration and management, information assurance (IA), and interface design and management. This activity is demonstrated in Figure **12.2.3.3.F1** .

Figure 12.2.3.3.F1 - Conduct Program Planning



Office of the Secretary of Defense (OSD)-level templates are available to facilitate Program Planning activities (e.g., TEMP , SEP, PPP, LCSP) and can be used as-is or tailored to support the selected solution, as many were originally developed for weapon systems acquisition. It is recommended that the program manager collaborate with OSD subject matter experts (SMEs) and agree to which sections are appropriate for the acquisition of a DBS and the current program in particular, or to validate the use of program-created templates. The intent and spirit of the information developed using templates and program-level documentation is to plan and execute a program - the templates are for convenience and discipline to ensure a critical piece of information is not overlooked by a busy team - not for "checking the box" on every single element. These program-level artifacts must be made available at the request of a decision-maker. Program-level documents are developed for program use and are summarized in the Business Case for decision makers (see Section 6, "Information Summaries" in the Business Case Template). Program-level information developed is referenced in Table **12.2.3.3.T1** by the corresponding OSD template names, though it is the information generated through the process of developing the information requirement

(template or document) that is the critical factor not the creation and completion of a document. In general, the Business Case integrates information requirements from traditional stand-alone templates to provide a summary-level integrated view of the program for decision making, reducing coordination time at the OSD-level. It is not expected or reasonable, however, that the Business Case will suffice as the only program documentation.

Table 12.2.3.3.T1 - Acquisition Approach Information Requirement Summaries

Program-level Information Requirement	**Information in the Business Case**
Acquisition Strategy	
Market Research	
Program Protection Plan (PPP)	
Information Assurance (IA)	
Systems Engineering Planning	*Information Requirement Summaries* :
Data Management Strategy	
Technology Development Strategy	Acquisition Approach
Information Support Plan (ISP)	
Lifecycle Sustainment Planning	
Test and Evaluation Planning *(incl. test and evaluation strategy)*	

The Acquisition Approach, the components of which are described in more detail in the following paragraphs, is the main output of the Conduct Program Planning activity.

Acquisition Approach . Integrates the following information requirements from traditional stand-alone acquisition templates to provide a summary-level view of the Acquisition Approach:

- ***Develop an Acquisition Approach (Strategy).*** Includes: competition strategy; impact of previous phase results on the competition strategy for the upcoming phase; and the role of the competition strategy to facilitate execution of the acquisition. It also summarizes the training plan including the planned training materials and planned user training. It identifies the planned major contracts and a summary of other contract information. Reference the schedule as appropriate. No acquisition sensitive information should be included in the Acquisition Approach.

An affordability target should be established prior to MS A and documented in the Business Case along with cost growth controls. In addition, "should cost" estimates must be developed for both MAIS and non-MAIS programs and should be used throughout subsequent phases of BCL to drive contracting strategies and to track program and contractor performance. The Business Case should also address methods

to incentivize contractor productivity and innovation.

Reference: Better Buying Power

- ***Conduct Market Research.*** Market research is conducted to determine whether there are commercial off-the-shelf (COTS) products that meet the defined requirements in the Business Case, could be modified to meet requirements, or could meet requirements when it is necessary to modify those requirements to a reasonable extent. It helps determine the availability and suitability of COTS products and the degree they have: interfaces with broad market acceptance; standards-organization support; and, stability.

Market research conducted in the Business Capability Definition (BCD) phase and Investment Management (IM) Phase helps: establish an understanding of commercially available solutions; identify potential suppliers; identify small business capabilities; and, initiate development of strategies to promote competitive best value acquisitions. The results of completed market research and plans for future market research are summarized in the Acquisition Approach of the Business Case for review at MS A.

Systems engineering planning, conducted during the Prototyping phase, supports architecture design and market research. That market research also supports the Analysis of Alternatives (AoA). Results of completed market research and plans for future market research are summarized in the Acquisition Approach of the Business Case for review at Pre-Engineering Development (Pre-ED). The Pre-ED review is a prerequisite to issuing a final Request for Proposal (RFP) for the Engineering Development phase and beyond for the increment.

Market research, tailored to program needs, should continue throughout the acquisition process and into Operations and Support (O&S). Use of COTS products requires periodic monitoring of the commercial marketplace through market research activities and alignment, when appropriate, of affected business and technical processes. This may impose additional cost, schedule, and performance risks that need to be assessed in the program's risk management plan (RMP).

- ***Develop Program Protection Plan (PPP).*** Summarize the protection scheme/plan for Critical Program Information (CPI) and Critical Functions and Components Protection. Guidance is located in the Program Protection Plan (PPP Outline & Guidance, July 2011). Other key aspects of PPP related to cost and schedule are summarized in cost and schedule information in the Business Case. Key aspects of PPP related to roles and responsibilities and standards and methods are summarized in the Program Charter. Potential for integration with IA and ISP information, as appropriate.
- ***Develop Information Assurance (IA) Strategy.*** Guidance is located in Appendix E of the Program Protection Plan Outline & Guidance, July 2011 . For a DBS, summarize applicable critical items in the Acquisition Approach of the Business Case.

- ***Systems Engineering Planning.*** Effective systems engineering planning is essential to the success of a program. One important measurement of that success is a Technical Performance Measure (TPM) for Reliability, so that should be included as one of the critical success factors of the Business Case . The summary of systems engineering planning in the Business Case is approved, at MS A, Pre-ED, and MS C, by the Director, Systems Engineering .

Defined content for the summary of systems engineering planning is the architecture and interface definition and management includes:

- a list of planned technical baseline artifacts;
- design considerations critical to achieving the program's technical requirements;
- technical performance measures and metrics;
- planned engineering tools;
- results of previous phase SE activities and planned SE activities for the next phase; and
- identification of the plans containing: the physical architecture diagram, the system functional architecture diagram, and the SV-1 - Systems Interface Description diagram.

Other important systems engineering managerial methods and standards are incorporated into the Program Charter including:

- program requirements management, traceability, and verification;
- configuration and change management;
- technical staffing and organization management; and
- use of technical reviews.
- ***Develop Data Management Strategy and Technical Data Rights.*** Data Management Strategy and Technical Data Rights content is traditionally addressed in the Technology Development Strategy or Acquisition Strategy (TDS/AS) for weapons systems. The information comparable to the TDS/AS for DBS is contained in the Acquisition Approach and is outlined below, but it is suggested that you should review Section 7.6 of the TDS/AS regarding Technical Data Rights Strategy.

Summarize the Technical Data Rights Strategy for meeting data rights requirements and to support the overall competition strategy, including:

- Analysis of the data required to prototype, develop, deploy and sustain the system (e.g., conceptual data model (DIV-1), logical data model (DIV-2));
- Approach to provide for rights, access, or delivery of technical data the government requires for the systems total life cycle sustainment;
- Approach for using open systems architectures and acquiring technical data rights;
- Approach to including a priced contract option for the future delivery of technical data and intellectual property rights not acquired upon initial contract award; and

- Analysis of the risk that the contractor may assert limitations on the government's use and release of data.

For additional information on this subject, refer to DAG Chapter 2, Section2.2.14 "Data Management Strategy and Technical Data Rights" ; and DAG Chapter 5, Section 5.1.6.3, "Contracting for Technical Data" and 5.1.6.4, "Data Management Strategy" .

- ***Information Support Plan (ISP).*** Includes preparation for and interoperability planning in four critical areas: Information Needs; Information Timeliness; Information Assurance (IA); and Net-Enabled (through the Net-Ready KPP). Refer to Enclosure 4, Attachment 2 of DoDI 4630.8, June 30, 2004 .
- ***Conduct Life-Cycle Sustainment Planning.*** Prior to MS A, lifecycle sustainment planning begins with the AoA, describing the notional high-level product support and maintenance concepts to be used for each alternative. Once the preferred alternative has been selected, these concepts are expanded upon into a strategy for the entire program, based on the technology and acquisition approach. Considerations should include optimizing readiness and minimizing total life-cycle costs. Documentation of lifecycle sustainment planning includes requirements; assessments; support strategy; performance-based agreements; funding; schedule and management; a program support and maintenance strategy; key metrics, system performance indicators or other key drivers; the view of sustainment/logistics contracts, key supportability requirements included in the system and design specifications; and the major product support elements and plan / agreement for acquiring and fielding them. DAG Chapter 5, Section 5.1.2, "Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment" goes into significant depth into sustainment planning and there are several considerations specifically related to DBS for LCSP in the O&S section.
- ***Conduct Test and Evaluation Planning.*** Test and evaluation planning should involve developing an overall test management strategy and test management plan for the program. It is summarized in the Acquisition Approach of the Business Case for the benefit of decision makers. The Test Plan is produced in-lieu-of a Test and Evaluation Master Plan (TEMP) in order to align with needs specific to defense business systems.

During the IM phase, the Test Plan establishes test and evaluation from a strategic level, for government and contractors, in support of the MS A review. It supports the overall program resource requirements, schedule, and performance requirements planned in the Business Case. It identifies the approach for integrated Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E). It is guided by the testing roles, responsibilities, standards and methods to be specified in the Program Charter.

After the IM Phase, the Test Plan matures during Prototyping from a strategy to a plan in support of the review at MS B. This transformation includes the identification of evaluation criteria for testers, and for more detailed documentation at the program level,

ensures that the test plan is useful, executable, and outcome-based.

The following is a summary of the Conduct Program Planning activity:

- *Inputs.* Results of Material Solution Analysis.
- *Process.* Conduct program planning activities as appropriate to the selected solution, which includes, but is not limited to developing plans and/or strategies for the following: test and evaluation, systems engineering, lifecycle sustainment, data migration and management, IA, and interface design and management.
- *Outputs.* Program-level documents (which may follow OSD or Component templates) and summarized in the Business Case and Program Charter.

TIP: Summarizing information from planning / execution-level documents in the Business Case does not relieve BCL users from conducting the rigorous analysis required to make business decisions (i.e., "do your homework!").

12.2.3.4. Complete Business Case and Program Charter

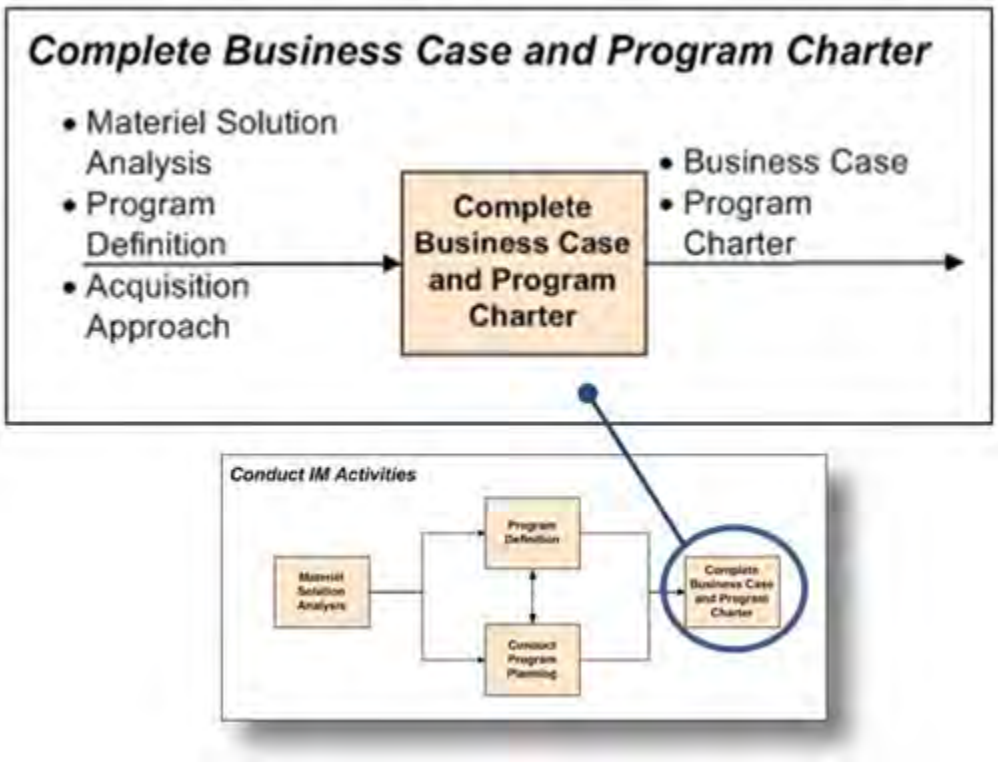
12.2.3.5. MS A Preparation

12.2.3.4. Complete Business Case and Program Charter

Business Case. The business case is the one location where all relevant facts are documented and linked together into a cohesive story. It is an executive-level document used by decision-makers for investment and acquisition decisions.

The Functional Sponsor and the program manager summarize the results of the IM Phase activities in the Business Case and document the managerial methods and standards for executing the potential program in the Program Charter. This summarization should provide decision makers with the essential information about the potential program to make an informed decision supporting a MS A review.

Figure 12.2.3.4.F1 - Complete Business Case and Program Charter



While developing the Business Case, the program manager and the Functional Sponsor should ensure that its content presents the required information at a level appropriately suited for executive-level decision makers, keeping in mind that detailed working papers or detailed analysis should be kept at the program level and available if requested. Before submitting the Business Case for formal review, the program manager and Functional Sponsor may consider the following:

- Is the Executive Summary clear, concise and focused on the problem and it's solution?
- Does the Business Case contain the appropriate level of relevant information to enable a decision and inform decision makers?
- Is the value and the risks inherent in the proposed program clearly explained?
- Is the Functional Sponsor with the capability and authority to deliver the benefit's fully committed to the investment?
- Can all HLOs be quantified so their achievement can be tracked?
- Is the Business Case tailored to the size and risk of the proposed solution?
- Does the Business Case focus on the business capabilities and impact, rather than on technical aspects? (Remember, the Business Case is not a technical proposal.);
- Does the Business Case contain clearly relevant and logical contents which are simple to understand?
- Does the Business Case justify critical elements in a transparent manner?

- Is there clear accountability for and commitment to the delivery of the capability and the management of costs?

The following is a summary of the Business Case portion of the Complete Business Case and Program Charter activity:

- *Inputs* . Results of IM Phase activities (i.e., Material Solution Analysis, Program Definition, Acquisition Approach, and Capability Delivery Plan).
- *Process.* The program manager and Functional Sponsor are responsible for summarizing output of IM Phase analysis in the Business Case. To facilitate development of the Business Case, a Business Case Template is provided for Component use to facilitate informed decision-makers. The template may be tailored to the needs of the program and can be accessed at the Office of the Deputy Chief Management Officer (DCMO)'s BCL webpage .
- *Outputs* . Business Case.

TIP: Before deeming the Business Case complete, the Functional Sponsor should review the Problem Statement to ensure that any discovery during IM does not significantly affect the approved Problem Statement. If significant changes are evident (such as, the fundamental problem has changed or the scope has broadened), it will warrant re-approval by the IRB Chair. The IRB Support staff should be consulted in this circumstance to determine the appropriate way ahead.

Program Charter. The purpose of a Program Charter is to define the manner in which the program will be managed and the governance surrounding the program. It is an agreement between the program team (including contractors), Functional Sponsor and PM and identifies the roles and responsibilities and assigns accountability to each of these individuals or groups. It also contains references to: detailed project plans such as schedules; work breakdown structure; complete risk assessments; etc.

The Program Charter describes the managerial methods and standards for the program and is a tool that helps enable the outcomes described in the Business Case. It is first developed as part of program management planning activity that spans the IM Phase, though it is updated in later phases of BCL as the program matures.

BCL does not prescribe the tools and techniques for performing program management, but does require the preparation of the Program Charter for review and approval by the Component Acquisition Executive (CAE) and for inclusion in the MS A package.

Program Charter Content.

- ***Program Governance and Integration.*** Describes the managerial methods and standards for ensuring that decisions are focused on achieving the outcomes and cost, schedule, and performance constraints defined in the Business Case.
- ***Program Management.*** Includes: process for managing the Program Charter; change management; procedures; practices for monitoring and controlling all

increments within the program; program and increment initiation, closure, and decision documentation.

- ***Scope Management.*** Aligns the activities that identify the deliverables and establish the relationship between product scope and program scope, while setting standards for clear achievable objectives to the Business Case, establishes change management, plans for delivery of program benefit's, defines the program deliverables, and the approach to requirements management.
- ***Schedule Management.*** Provides the plan for schedule tracking, controlling and performance reporting. Applicable earned value management is described, if utilized. A summary schedule of major deliverables and events is provided.
- ***Risk Management.*** Implements the program's risk management plan which defines the approach to risk identification, analysis, and mitigation, in addition to the process for conducting risk reviews and how to escalate risks.
- ***Procurement Management.*** Refers to the acquisition approach (Business Case) and outlines planning for managing acquisition and procurement activities.
- ***Financial Management.*** Establishes a plan for developing and managing program costs; budgeting; and defining the monitoring, forecasting, change controls and performance reporting. Applicable earned value management is described, if utilized.
- ***Stakeholder Management.*** Defines the plan for stakeholder identification, analysis, and management, as well as relationship management.
- ***Communications Management.*** Based on stakeholder management information, outlines a communications management plan, to include format, content, frequency, approval, recipients, and distribution.

The following is a summary of the Program Charter portion of the Complete Business Case and Program Charter activity:

- *Inputs* . Results of IM Phase activities (i.e., Material Solution Analysis, Program Definition, Acquisition Approach, and Capability Delivery Plan).
- *Process.* The program manager, in collaboration with the Functional Sponsor, will review the defined inputs and other available references as they are developed and as they relate to program management (e.g., the WBS developed during the Financial Analysis). Based on these inputs, the Functional Sponsor and program will prepare the appropriate sections of the draft Program Charter using the Program Charter template.
- *Outputs* . The Program Charter.

TIP: To facilitate development of the Program Charter, the Program Charter Template is provided on the Office of the Deputy Chief Management Officer (DCMO)'s BCL webpage . The template may be tailored to unique organizational or program situations.

12.2.3.5. MS A Preparation

When the Functional Sponsor determines that the proposed investment has reached a

level of detail sufficient for a MS A review, the program manager compiles a MS A Package that includes the following documents:

- A Business Case;
- A Program Charter;
- The Defense Business Systems Management Committee (DBSMC) Chair approval memorandum to obligate funds;
- The Component Acquisition Executive (CAE) Memorandum (Compliance and Recommendation), for MAIS; and
- Any additional requirements as outlined in previous acquisition decision memorandums (ADMs).

TIP: Prior to submitting the Business Case as part of the MS A package, the program manager and Functional Sponsor should verify whether the following aspects have been adequately addressed:

1. The investment has value to the enterprise and aligns with enterprise priorities;
2. There is proper management by and support from senior officials for the proposed solution;
3. The scope for the proposed solution has been adequately defined and measures for desired outcomes have been appropriately defined;
4. There is clear evidence that Business Process Re-engineering (BPR) has been or is being conducted;
5. There is clear evidence that the component has to ability to deliver the benefits of the proposed solution within the timelines specified; and
6. There is clear evidence that dedicated resources are working on the highest value opportunities.

For non-MAIS efforts, MS A materials are submitted for review and approval in accordance with Component processes and procedures.

For MAIS or "special interest" programs, the MS A Package is submitted to the appropriate Investment Review Board (IRB) at least 30 calendar days prior to the scheduled review date. The IRB Support Staff will coordinate a review with the IRB Membership (which includes Joint Staff), applicable partner IRBs, and SMEs. The Enterprise Risk Assessment Management (ERAM) team briefs detailed findings to the MDA and the IRB Chair. This coordinated review negates the need for the Functional Sponsor to coordinate separately with OSD and Joint Staff stakeholders.

12.3. Execution

12.3.1. Purpose, Outputs, and Outcomes

12.3. Execution

Execution third segment of BCL and is comprised of the following Phases: Prototyping, Engineering Development, Limited Fielding, Full Deployment, and Operations & Support (O&S).

12.3.1. Purpose, Outputs, and Outcomes

The purpose of Execution is to design, develop, test, deploy, and sustain each increment of capability (materiel and non-materiel solution) by satisfying the specific outcomes defined in the Business Case.

The output is to provide the end-user(s) an operational Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy (DOTMLPF-P) DOTMLPF-P solution that fulfills a need, as defined in the Problem Statement section of the Business Case, using an incremental approach to delivering capability (more information on the incremental approach to delivery capability can be found in section **12.4.1** , *Time-Limited Development*).

12.3.2. Prototyping Phase

12.3.2.1. Purpose, Outputs, and Outcomes

12.3.2.2. Prototyping Phase Process

12.3.2.3. Prototyping Phase Activities

12.3.2. Prototyping Phase

12.3.2.1. Purpose, Outputs, and Outcomes

The purposes of the Prototyping Phase are to:

- Determine the most cost-effective technical and design approach that will satisfy user capability requirements; and
- Conduct risk-reduction activities by: identifying use cases that determine the specific capabilities to be developed during the increment; the technologies to be used; and the approximate schedule for deploying the materiel solution.

TIP: Knowledge gained during this phase may result in: changes to the order in which required capabilities are satisfied; technology trades; and/or movement of requirements to follow-on increments.

The outputs and outcomes of the Prototyping Phase are:

- Functional outcomes (requirements) approved to a threshold / objective level;
- An updated Business Case and Program Charter;
- A draft acquisition program baseline (APB);
- A draft request for proposal (RFP);
- The ability to award a contract immediately upon receipt of a MS B acquisition decision memorandum (ADM); and,
- A materiel solution that has been designed and configured in a relevant test environment to satisfy the outcomes described in the Business Case for the increment under consideration.

12.3.2.2. Prototyping Phase Process

Figure 12.3.2.2.F1 - Prototyping Phase High Level Process Flow (Increment 1)

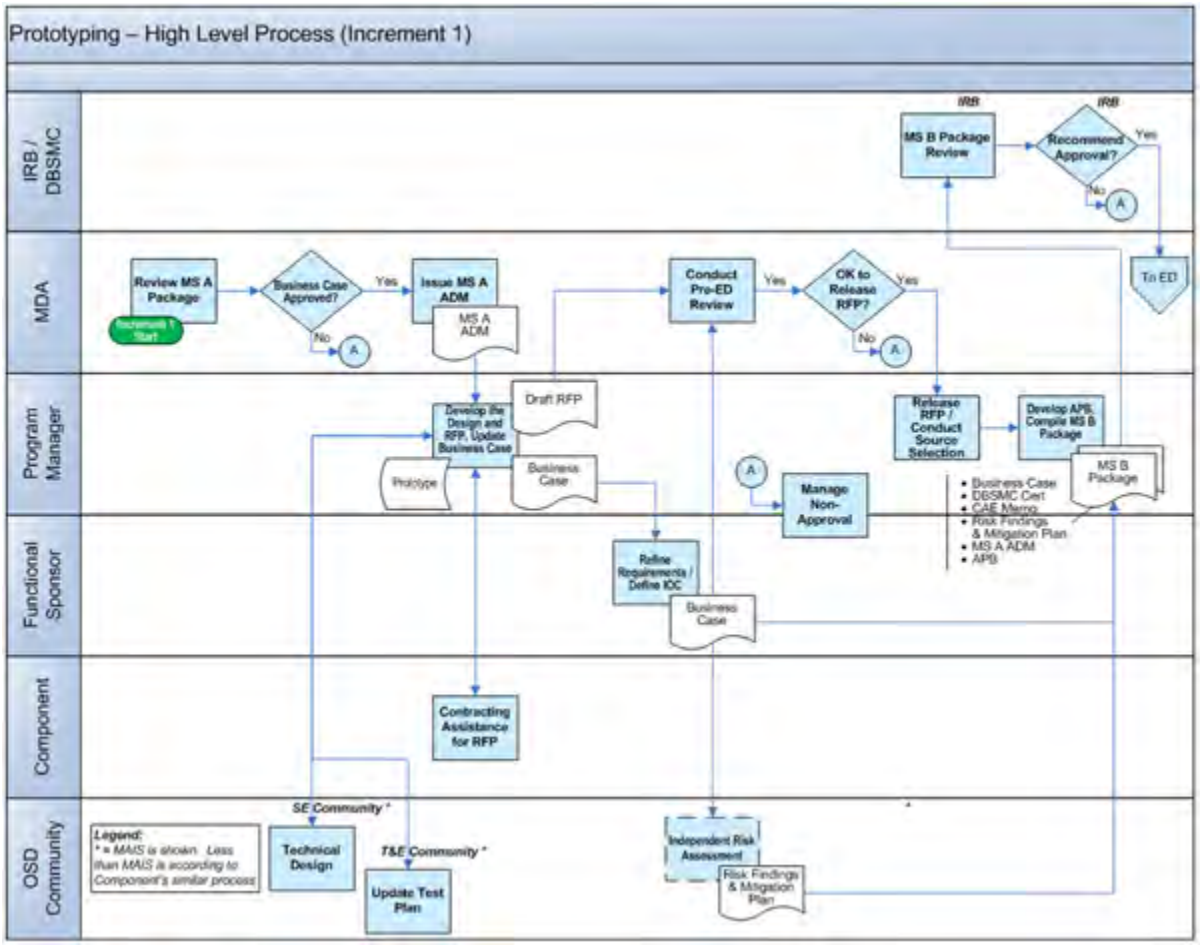
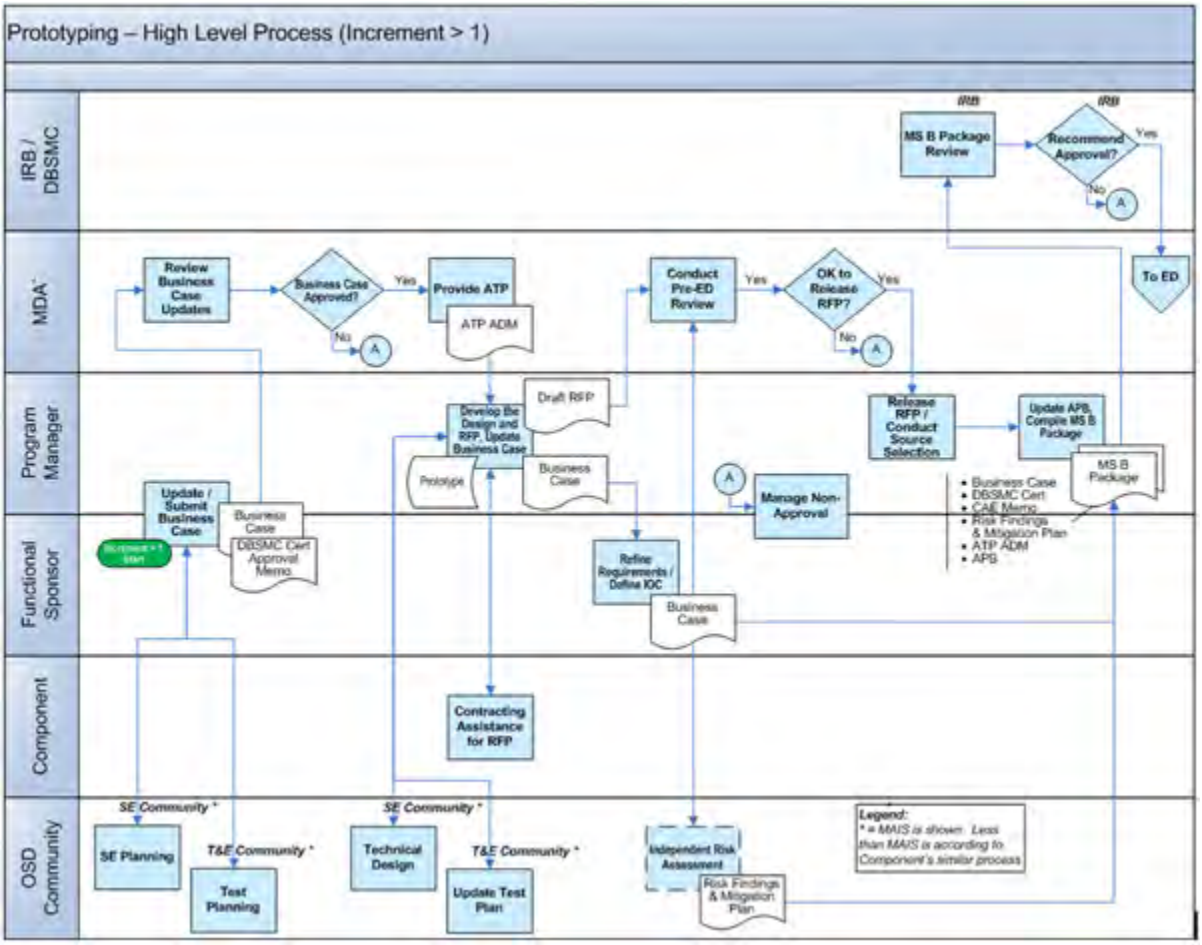


Figure 12.3.2.2.F2 - Prototyping Phase High Level Process Flow (Increment 2-n)



The Prototyping Phase begins when the MDA approves entry into the phase after conducting either a MS A review (for the initial DBS increment) or Authorization to Proceed (ATP) review (for the DBS increments 2-n). In other words, there is one MS A for each DBS and there is an ATP for each follow-on increment. ***Note:*** Multiple increments can be executed concurrently. It's important to note that the ATP is the starting point for obligation of funds for the increment.

During the Prototyping Phase, the Functional Sponsor and PM will perform the necessary activities to install and configure the solution in a relevant environment, perform detail design and requirements trade-offs, summarize updated plans in the Business Case, and develop a draft RFP for a Pre-Engineering Development (Pre-ED) Review. After the Pre-ED Review a draft APB will be developed for the increment and submitted for the MS B review. During this phase, the PM leads all activities pertaining to the materiel portion of the solution while the Functional Sponsor leads activities for the non-materiel or DOT_LPF-P portion of the solution, as outlined in the Program Charter. An independent risk assessment (Enterprise Risk Assessment Methodology (ERAM) for MAIS) will also need to be conducted and a risk mitigation plan developed

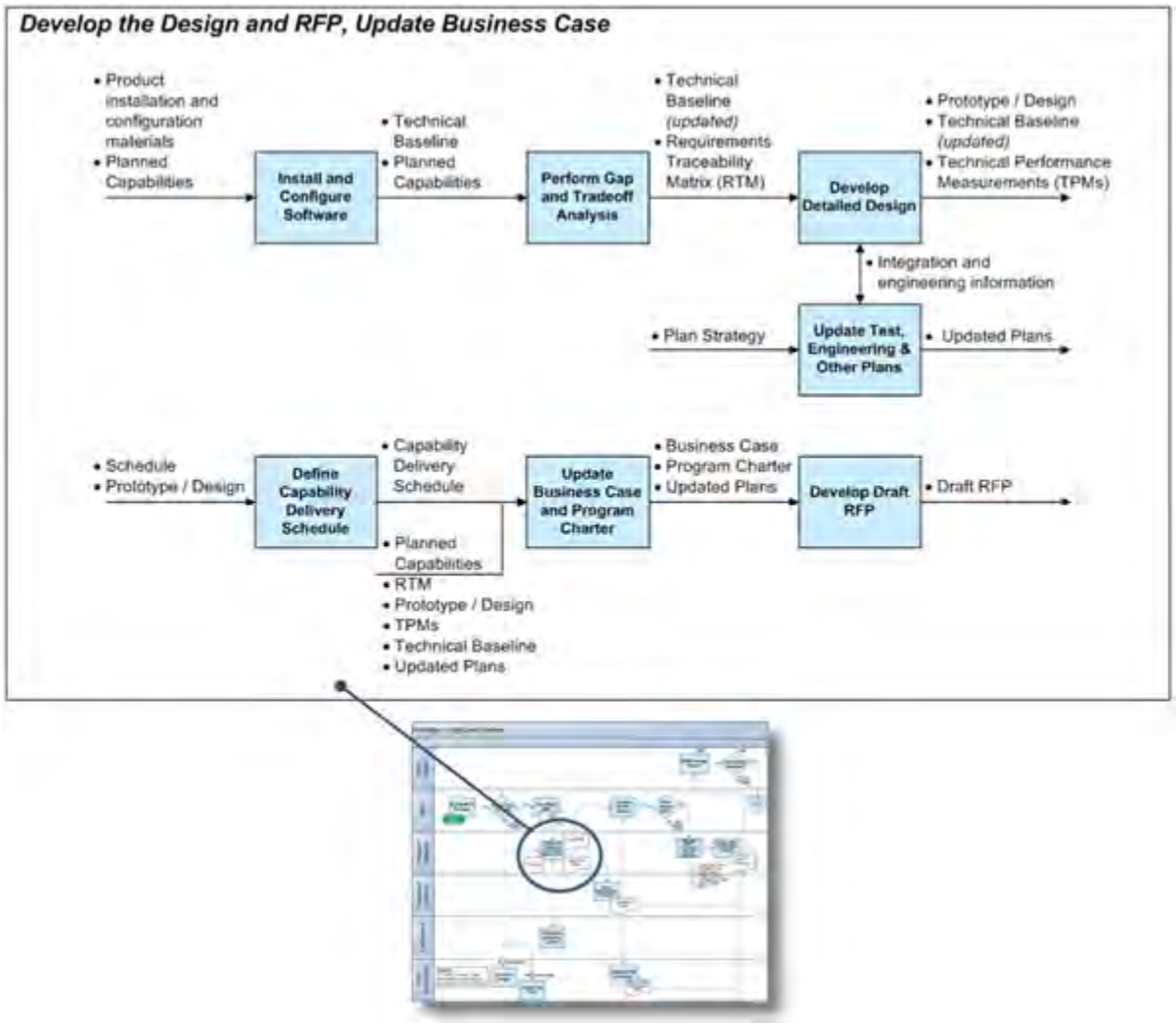
prior to MS B. The PM and the Functional Sponsor must work collectively to ensure the DOTMLPF-P requirements are integrated and will deliver a holistic solution.

Prototyping is a continuous activity, meaning that in a typical program, requirements are constantly being added or changed and must be evaluated, managed, prioritized and queued for development, test and evaluation, and delivery. This requires close collaboration between users, developers, T&E, and the PM who must set expectations, manage risk, and plan what will be delivered for a given increment within the BCL time limitations. This cycle repeats until there are no more development activities to be planned (i.e., there are no more requirements to fulfill).

Prototyping Phase activities end for each increment after the Investment Review Board (IRB) (or Component equivalent) has reviewed the necessary MS B information and the IRB Chair has sent a milestone recommendation to the MDA.

12.3.2.3. Prototyping Phase Activities

Figure 12.3.2.3.F1 - Decomposition of "Develop the Design and RFP, Update Business Case" Process Step



Prototyping Phase activities are conducted in accordance with the approved Business Case, the MS A ADM, and the solution-specific implementation methodology being employed. While conducting Prototyping Phase activities, the PM must work in close collaboration with the Functional Sponsor, functional users, and appropriate Systems Engineering (SE) and Test and Evaluation (T&E) communities as functional, organizational, and user-related activities (such as requirements refinement and implementation of change management / Business Process Re-engineering (BPR) / DOT_LPF-P considerations) occur in tandem with traditional PM responsibilities.

The PM should collaborate with appropriate communities early on to plan the type(s) and amount of design and T&E reviews necessary to facilitate development and validation of the outcomes for the capability to be delivered. More information on

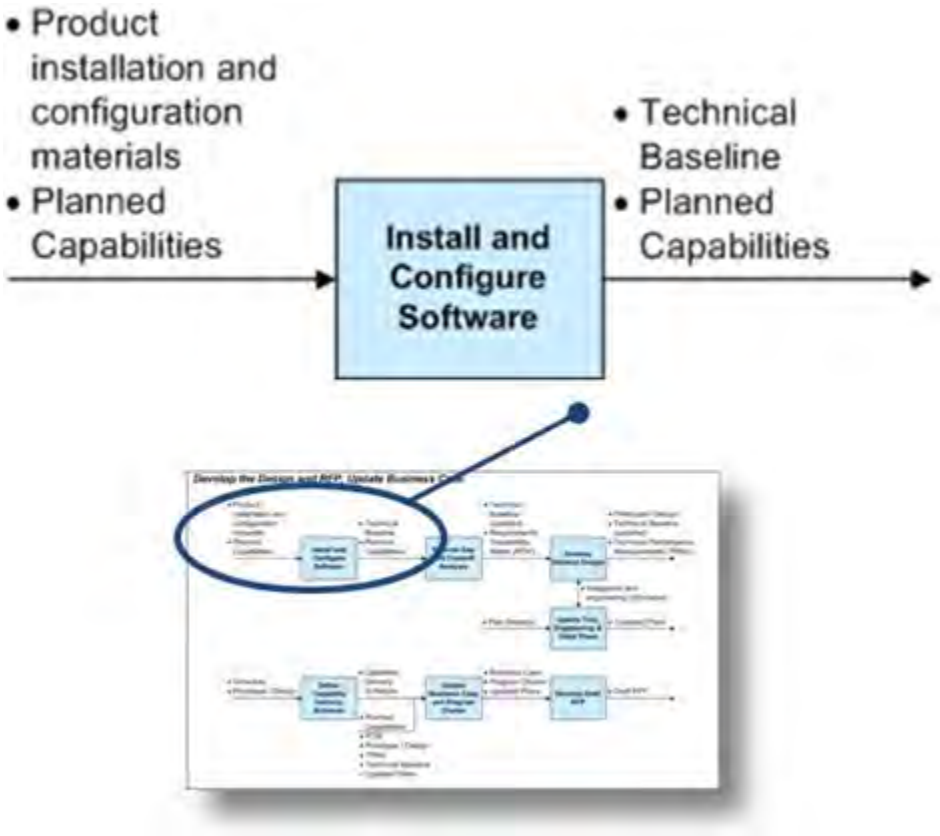
conducting test and engineering reviews is located in DAG Chapter 4, Section 4.2, "Systems Engineering Activities in the System Life Cycle" .

> **TIP:** It is imperative that the Functional Sponsor and the program manager have collective understanding of their roles and responsibilities (and have documented them in the Program Charter) in order to smoothly execute the program going forward.

As mentioned previously, Prototyping Phase activities are continuous and will iterate until the required level of maturity is achieved and prototypes of the system or key system elements are produced, and when there is confidence that the scope defined for the current increment and the cost, schedule, and performance baselines can be maintained throughout the remainder of the increment's planned implementation and sustainment of capability.

Install and Configure Software. This activity involves planning for the installation and configuration of: infrastructure, as necessary (e.g., servers, utilities, services, databases); commercial off-the-shelf (COTS) product(s); backup and recovery procedures; and the initiation of support services necessary to sustain the Technical Baseline. The Technical Baseline includes both the reference assets (e.g., documentation) and technical assets (e.g., software) of the system and acts as a formal baseline for defining subsequent change.

Figure 12.3.2.3.F2 - Install and Configure Software Context



As a result of this activity, the program manager will initiate Configuration Management (CM) to establish and maintain the integrity of work products and to track and control changes. More information on CM can be found in DAG Chapter 4, Section 4.3.7, "Configuration Management".

The following is a summary of the Install and Configure Software activity:

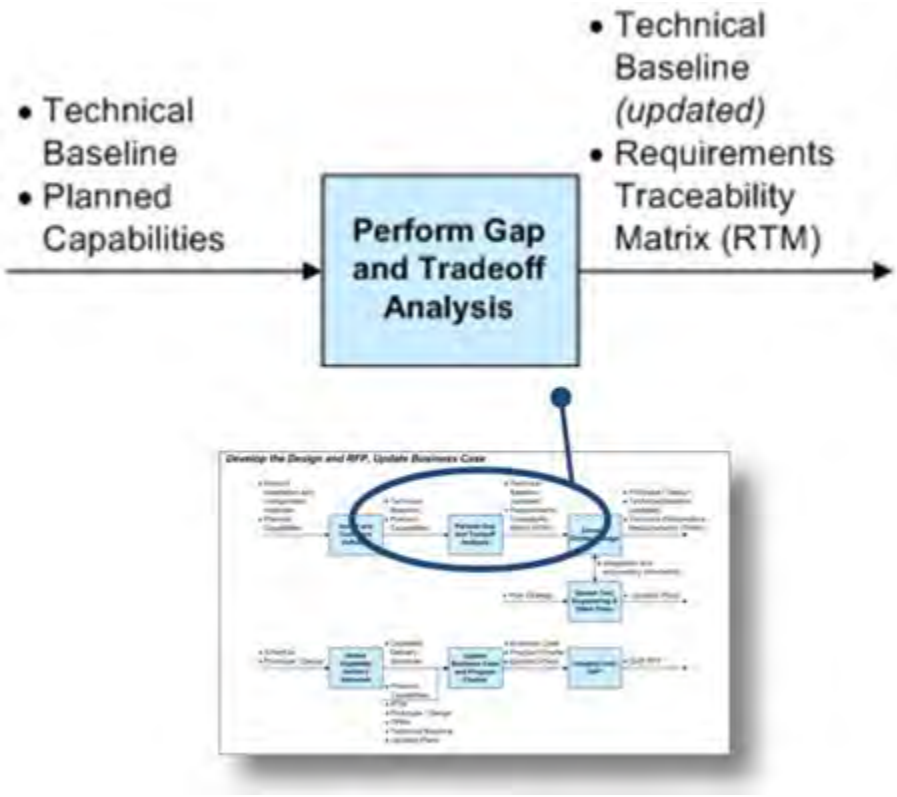
- *Inputs* . Planned outcomes, COTS product and product documentation.
- *Process.* Subject matter experts (SMEs) plan and perform the installation and configuration of COTS product(s) in a relevant environment at the direction of the program manager. The software is demonstrated and evaluated to ensure it performs as expected. The result is the Technical Baseline which is then allocated to and released for follow-on Prototyping Phase activities (e.g., gap and tradeoff analysis, software customization), and the program manager initiates CM.
- *Outputs.* Technical Baseline, planned capabilities.

Perform Gap and Tradeoff Analysis. The purpose of this activity is to: evaluate the installed software's actual performance against the planned capabilities ("To-Be" process, outcomes) defined in the Problem Statement and Business Case; determine

the variance between the capabilities and the software's performance, or "gaps" and; develop alternatives for filling the gaps.

Cost, schedule, and performance may be traded off within the "trade space" between thresholds and objectives documented in the measurement criteria of the Business Case.

Figure 12.3.2.3.F3 - Perform Gap and Tradeoff Analysis Context



The tradeoff analysis may also consider potential exchanges in the trade space, such as re-sequencing capabilities across increments to accelerate high-value capabilities into the early increments, or continued BPR to modify ways of doing business to more closely align with suitable processes that already exist in the COTS products.

The PM and Functional Sponsor engage SMEs, including SE and T&E, who work to determine the gap(s) between the desired business outcomes defined in the Business Case and what the software can deliver, and develop an executable plan for filling the gaps. One goal of this process is to minimize customization of COTS software. Depending on complexity of the materiel solution, adjustment of the "To-Be" business process may be necessary in order to accommodate the way the software was designed to work. Or, it may be discovered that the software has out-of-the-box capabilities superior to those originally planned. Trade-off decisions typically include modifying the way work is traditionally conducted (business processes) versus incurring

the cost and risk of customizing the COTS software. This is why BPR is a continuous refinement effort - where better ways of conducting business are continuously evaluated based on the inherent business capabilities of the selected COTS products.

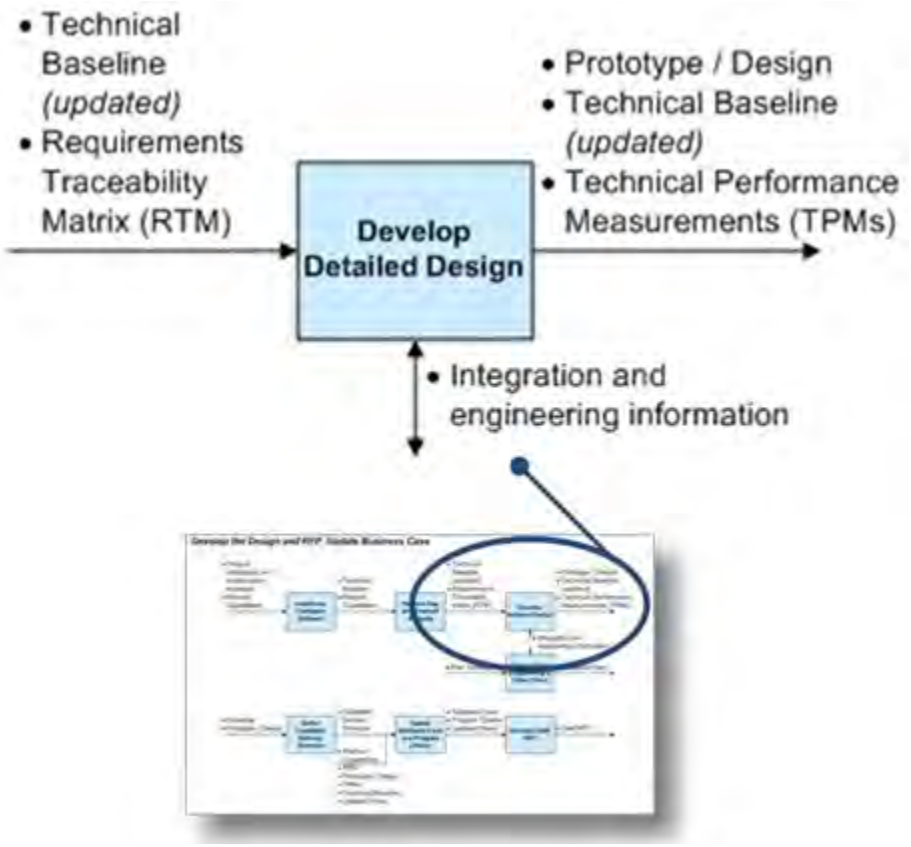
TIP: During these activities, additional requirements or changes to existing requirements are likely to be discovered, particularly when the COTS product is being configured. Potential changes must be balanced against an impact to cost, schedule, and performance and given consideration for deferral to a future increment. The focus should be to execute the current plan and provide capability delivery (and value) to the user and the Department as rapidly as possible.

The following is a summary of the Perform Gap and Tradeoff Analysis activity:

- *Inputs* . Technical Baseline (software and associated documentation) and planned capabilities ("to-be" process and outcomes).
- *Process.* SMEs evaluate installed software against planned capabilities and develop a plan to fill gaps and determine the fastest approach to fielding useful capability, prioritizing requirements, and adjusting business processes as necessary by refining BPR. The outcomes and business capabilities described in the Business Case must be traced to those identified in the Technical Baseline and the plan for filling the gaps using a program-level Requirements Traceability Matrix (RTM). This verifies that all requirements have been allocated to a solution and to help avoid what is known as "gold plating" (i.e., investing in capabilities that are not in scope). The plan for filling the gaps will be used to update the Technical Baseline.
- *Outputs* . Updated Technical Baseline and a RTM.

Develop Detailed Design. The purpose of this activity is to translate planned business capabilities documented in the Business Case into a design specification. To support this, the updated Technical Baseline combined with the initial RTM is used to develop a design to meet the planned business capabilities. As a result, the gaps in the solution will now be closed through design activities by systems integration and software engineering SMEs. More information can be found in DAG Chapter 4, Section 4.3.18, "Systems Engineering Design Considerations" .

Figure 12.3.2.3.F4 - Develop Detailed Design Context



The result of these design activities is a detailed design, which will undergo planned functional and technical reviews to manage the identification of and resolution of design issues (by the PM and Functional Sponsor).

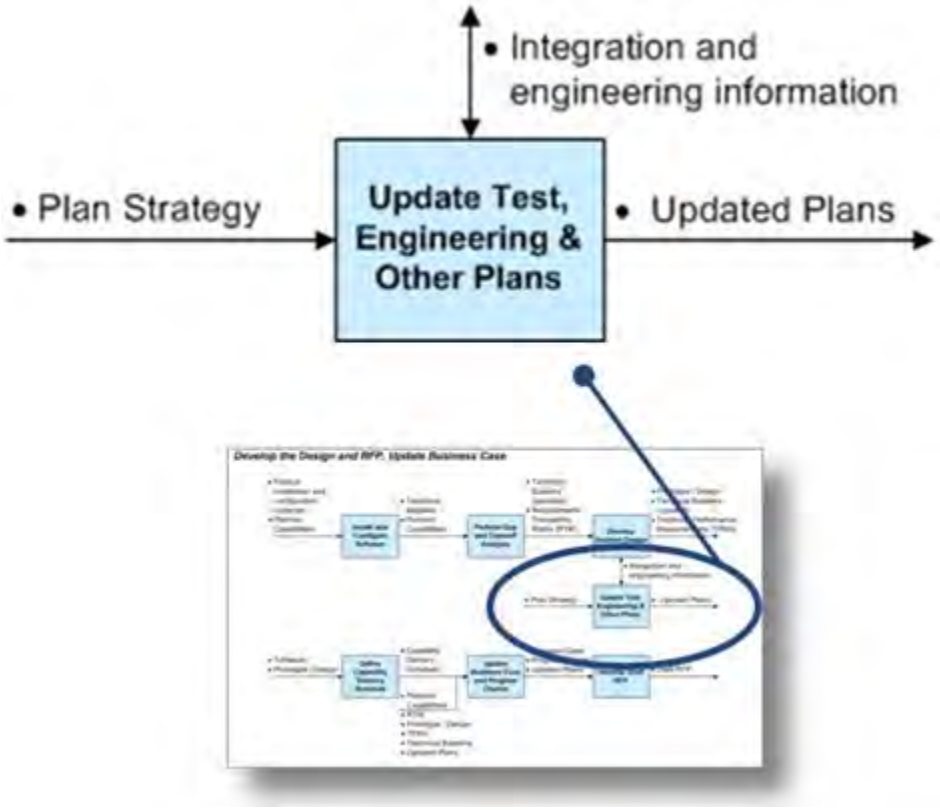
The following is a summary of the Develop Detailed Design activity:

- *Inputs* . Updated Technical Baseline, RTM.
- *Process.* Plan the design activities. Review the existing capabilities of the COTS products that were incorporated into the Technical Baseline. Review the RTM to determine those requirements that will be allocated to the increment being planned. Identify the subset of those requirements that require additional design. Use expert judgment to develop design alternatives and select the "best value" alternative. Verify that the approved cost, schedule and performance parameters of the Business Case will support the proposed design. Further define or update overall performance measures and Technical Performance Measures (TPMs) based on the design and plan appropriate revisions to the Business Case based on the design.
- *Outputs* . Detailed design, Technical Baseline (updated), TPMs.

Update Test, Engineering & Other Plans. The purpose of this activity is to use the knowledge gained from preceding activities in conjunction with the strategies and plans developed during the Investment Management (IM) Phase and enhance the information to convert them into detailed plans during the Prototyping phase for subsequent activities.

Guided by the analyses conducted during the IM Phase combined with the knowledge gained from assessment of the current solution-set now available in the updated Technical Baseline, the program manager and technical teams (e.g., SE, T&E, Systems Integrators) collaborate on integration and engineering needs. Their plans for design, development, test and evaluation, and performance measurement will be refined to yield a comprehensive suite of updated planning information for the remaining phases of Execution.

Figure 12.3.2.3.F5 - Update Test, Engineering and Other Plans Context



The following is a summary of the Update T&E, SE & Other Plans activity:

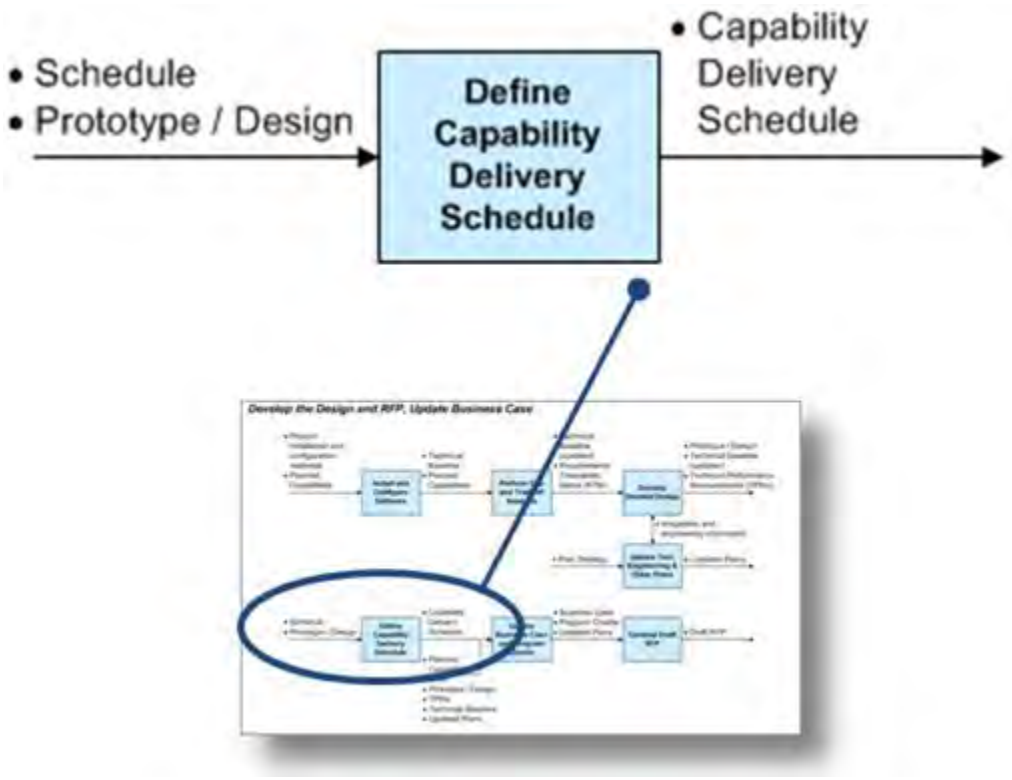
- *Inputs* . Strategies developed during the IM Phase (T&E strategy for the Test Plan, Acquisition Approach).
- *Process.* Update the strategy-level information developed during the IM Phase

with knowledge gained from assessment of the Technical Baseline and design activities to refine to a plan-level of detail that will support subsequent development, test and evaluation, and implementation.

- *Outputs* . Updated plans summarized in the Business Case.

Define Capability Delivery Schedule. Based on the high-level Capability Delivery Plan in the Business Case (developed during the IM Phase), the program manager and Functional Sponsor segment business capabilities into manageable increments based on priority, dependencies, risks, and implementation strategy and prepare a detailed Capability Delivery Schedule for the next planned increment. Changes will likely result in changes to cost estimates, and should be reviewed for such.

Figure 12.3.2.3.F6 - Define Capability Delivery Schedule



The Capability Delivery Schedule includes major reviews and milestone events and depicts releases, etc., as applicable. It is expected that the schedule will be presented at a high level (summary) in the Business Case, but must be maintained and available at a detail level (WBS) for program and stakeholder use since it critical for effective program management. Decision-makers may request the detail-level information for review.

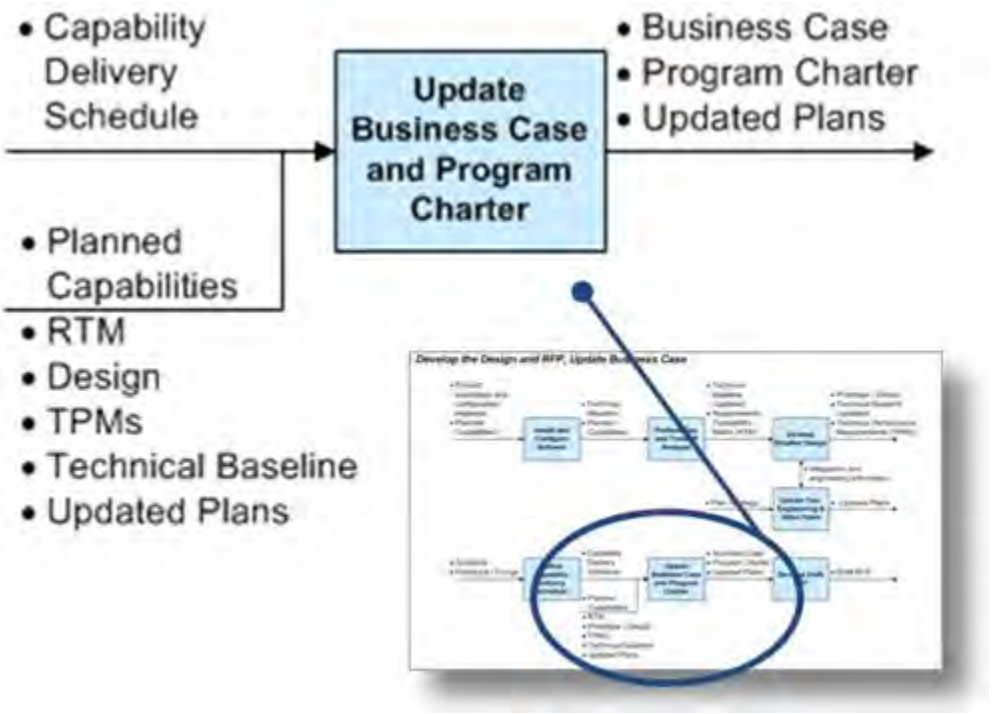
TIP: In the case of an organization-by-organization release of capability, the PM and the users may adjust the capability delivery schedule to accommodate functional/user needs or priorities, consistent with the APB. Such adjustments, however, should not alter the FDD criteria approved by the MDA and documented in the MS B ADM.

The following is a summary of the Define Capability Delivery Schedule activity:

- *Inputs* . Capability Delivery Plan (IM Phase) from the Business Case, design.
- *Process.* Partition business capabilities across multiple increments according to: Functional Sponsor priorities, dependencies, implementation strategy, and other priorities as necessary. Develop a capability delivery schedule. As needed, revise the Work Breakdown Structure (WBS) to indicate consequences of allocating business capabilities across multiple Increments. Verify estimated labor resource requirements, estimated task durations and dependencies based on the new distribution of business capabilities into multiple Increments and modify the Capability Delivery Plan as required.
- *Outputs* . Capability Delivery Schedule.

Update Business Case and Program Charter. Once Prototyping Phase activities are complete, the program manager and Functional Sponsor must update the Business Case and Program Charter as necessary to inform subsequent decision-making.

Figure 12.3.2.3.F7 - Update Business Case and Program Charter Context



TIP: While updating the Business Case, the Functional Sponsor and PM must ensure that the materiel solution is still focused on solving the originally identified business need (from the Problem Statement). If it is not, it may mean that the problem has changed or the right solution has not been chosen.

The following is a summary of the Update Business Case and Program Charter activity:

- *Inputs* . Capability delivery schedule (including the draft APB), planned capabilities, RTM, design, TPMs, Technical Baseline, updated plans (i.e., T&E, SE).
- *Process.* The program manager and Functional Sponsor analyze the outputs from Prototyping Phase activities, such as gaps or changes in business processes resulting from installing and configuring the software, the capability delivery schedule, updated T&E and SE Plans, and update the appropriate sections of the Business Case and Program Charter.
- *Outputs* . Updated Business Case and Program Charter.

Develop Draft RFP. The RFP begins the process of establishing government-industry relationships for acquiring products and services to implement the defined program. The RFP must establish a clear understanding of the government's needs to industry and the resulting proposals help the government understand industry capabilities in their pursuit of "best value".

Based on the Acquisition Approach in the Business Case and the Program Charter's roles, responsibilities and standards for procurement, the program manager initiates the draft RFP in collaboration with a Contracting Officer.

Figure 12.3.2.3.F8 - Develop Draft RFP Context

Contracting specialists provide insight into types of contract and language for the RFP to include such things as data rights and terms and conditions. The content in the RFP is organized in such a manner to clearly define the scope of products and services for the Increment and allow the Government to effectively evaluate proposals; the Business Case and Program Charter are the primary sources for RFP content. The completed draft RFP becomes part of the Pre-ED review package.

The following is a summary of the Develop Draft RFP activity:

- *Inputs* . Business Case, Program Charter, Updated Plans.
- *Process.* The PM follows established procedures within his or her Component to develop an RFP and may replicate applicable sections of the Business Case and Program Charter. The PM collaborates with Contract Specialists to ensure appropriate language is incorporated (e.g., licensing of software and intellectual property, data rights, etc.), in the RFP to protect the Government's interests. The PM also establishes selection criteria for evaluation of proposals.
- *Outputs* . Draft RFP.

Independent Risk Assessment. Prior to MS B, an independent risk assessment must be conducted. For MAIS DBS, the assessment is specifically an Enterprise ERAM assessment and will usually commence 90-120 days before a program is ready for its Pre-ED Review. The PM should notify the risk assessment team as early as possible of knowing the MS B date so preparations can be made. No additional documentation is

created by the program office for the assessment, as it is based on existing program documentation. The PM will work with the assessment team to develop a risk mitigation strategy once the assessment is complete.

Pre-ED Review. The purpose of the Pre-ED Review is to have the MDA review and approve the Business Case and authorize the release of the RFP so source selection can begin while the remaining Prototyping activities are being completed (i.e., APB development). The goal is to complete all of the activities necessary to award a contract or task order immediately after MS B is approved.

In preparation for the Pre-ED Review, the PM compiles a Pre-ED Review Package that includes:

- The updated Business Case signed by the Functional Sponsor, PM, Component Acquisition Executive (CAE), and appropriate sections signed by Deputy Assistant Secretary of Defense, Systems Engineering (DASD(SE)), Deputy Assistant Secretary of Defense, Developmental Test and Evaluation (DASD(DT&E)) and Director, Operational Test & Evaluation (DOT&E);
    - DBS below the MAIS threshold will have a Business Case approved through comparable Component processes and authorities
- Component Acquisition Executive (CAE)-approved Program Charter (MAIS only);
- A presentation that outlines the elements of the Draft RFP.
- A CAE Memorandum (Compliance and Recommendation);
- Any additional information and/or requirements as outlined in previous ADMs; and

The package is submitted to the IRB for review and the IRB Chair will provide a recommendation to the MDA.

The output of the Pre-ED Review is an MDA-approved Business Case and approval to release the RFP and begin source-selection.

MS B Preparation. When the draft APB and independent risk assessment are complete, the PM compiles a MS B Package that includes the following documents:

- The approved Business Case and, if necessary, a memo summarizing any changes since the Pre-ED Review;
- A DBSMC Chair certification approval memorandum to obligate funds;
- The draft APB;
- A CAE Memorandum (Compliance and Recommendation).

The package is submitted to the MDA, who may request an IRB MS B recommendation. For those acquisitions that are not MAIS or designated "special interest" programs, information requirements for a MS B review are submitted for review and approval in accordance with the Component's process and procedures.

12.3.3. Engineering Development

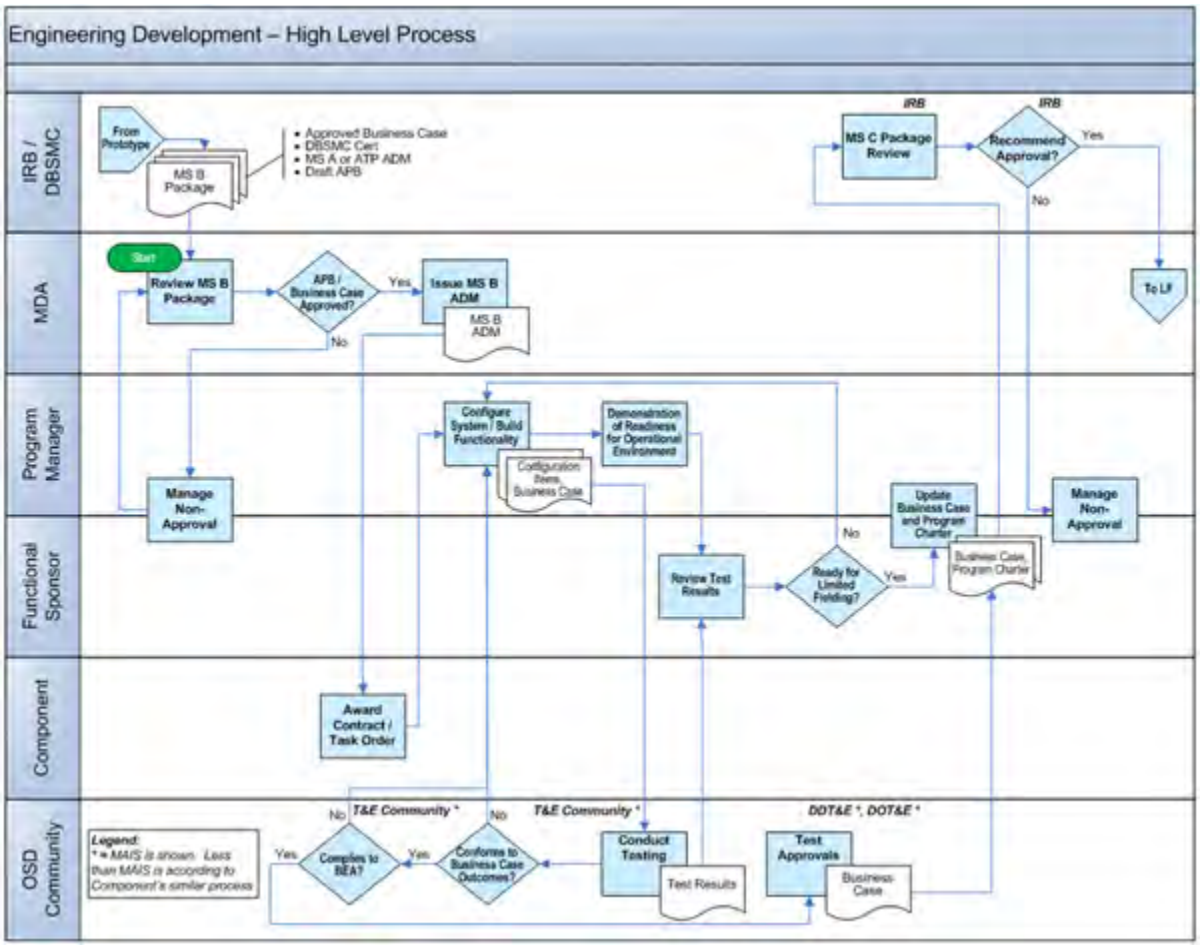
12.3.3.1. Purpose, Outputs, and Outcomes

The purpose of the Engineering Development Phase is to ensure that the materiel solution for the increment has been designed, configured, and developmentally tested in a manner consistent with the approved Business Case and the Program Charter and that it is prepared for limited deployment.

The outputs and outcomes of the Engineering Development Phase is a Business Enterprise Architecture (BEA) -compliant materiel solution ready for limited deployment into an operational environment for testing.

12.3.3.2. Engineering Development Phase Process

Figure 12.3.3.2.F1 - Engineering Development High Level Process Flow



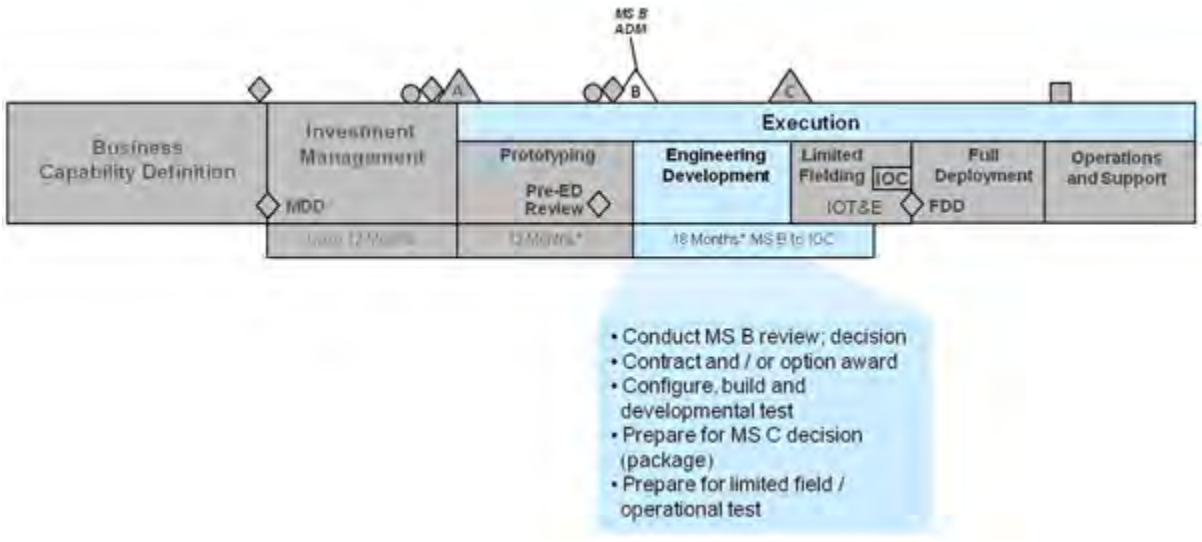
The Engineering Development Phase begins at MS B when the Milestone Decision Authority (MDA) reviews and approves the Acquisition Program Baseline (APB) and documents the decision in an acquisition decision memorandum (ADM). Specific attention shall be given to overall affordability; satisfaction of approved requirements; deployment timelines; risk management; and the basis for the program schedule. Upon approval of MS B, the Contracting Officer can award a contract or have one modified and obligate funds.

During the Engineering Development Phase, the program manager (PM) leads the effort to integrate the solution (increment) in a development / test environment and partners with the Functional Sponsor / user community to ensure functional requirements remain in alignment. The Functional Sponsor continues to solve or implement the Doctrine, Organization, Training, Leadership and education, Personnel, Facilities, and Policy (DOT_LPF-P) aspects of the solution that will accompany the

materiel portion.

12.3.3.3 Engineering Development Phase Activities

Figure 12.3.3.3.F1 - Engineering Development Activities on BCL Model



Engineering Development Phase activities include, but are not limited to:

- Configuring the increment in an developmental / test environment;
- Conducting developmental T&E with the appropriate Component Test Agency / Organization and DOT&E (if appropriate) per the Business Case and Program Charter;
    - Testing and evaluating the capability to be delivered to ensure it achieves the outcomes defined in the Business Case and that it is Business Enterprise Architecture (BEA) -compliant;
    - Planning for operational testing during the Limited Fielding Phase;
- Making preparations for sustaining the increment of capability (continuing solution planning begun in the Investment Management (IM) Phase);
- Minimizing costs, monitoring and mitigating risks, conducting ongoing Business Process Re-engineering (BPR) (as necessary and appropriate);
- Integrating the non-materiel / DOT_LPF-P aspects of the solution, as appropriate;
- Monitoring and managing proposed requirements changes as appropriate to ensure the capabilities are delivered according to the APB for the increment;
- Demonstrating that the capability or increment of capability has been designed, configured, developed, and tested in a manner consistent with the Business Case, Program Charter and the MS B ADM;
- Preparing for MS C review; and
- Preparing the capability for delivery into an operational environment.

The Engineering Development Phase ends when the Functional Sponsor and PM are satisfied that the capability is ready for use and request a MS C / Limited Fielding decision.

MS C Preparation. When the Functional Sponsor and PM have determined that the solution achieves the capabilities described in the Business Case for the increment and the acquisition program baseline (APB), a MS C Package is prepared to request approval to begin Limited Fielding at the MS C decision. Some of the considerations at this phase include:

- User concurrence that the capability satisfies the outcomes specified in the Business Case;
- Associated DOT_LPF-P capability is deployment-ready;
- Performance during developmental and operational testing is acceptable and consistent with the Business Case;
- Interoperability Certifications, Information Assurance Assessment and Authorization (IA A&A), BEA compliance, and any other required certifications have been obtained; and
- Life-cycle support is ready to implement.
- Clinger-Cohen Act (CCA) certification is still valid.

The MS C Package contains:

- The Business Case including any updates resulting from Engineering Phase activities;
- Any additional information / documentation required as directed in previous ADMs; and
- If necessary:
    - An updated APB;
    - A DBSMC Chair Certification approval memorandum; and
    - An updated Program Charter.

12.3.4. Limited Fielding

12.3.4.1. Purpose, Outputs, and Outcomes

12.3.4.2. Limited Fielding Phase Process

12.3.4.3. Limited Fielding Phase Activities

12.3.4. Limited Fielding

12.3.4.1. Purpose, Outputs, and Outcomes

The purpose of the Limited Fielding Phase is to limit risk by having a limited number of users verify that the capability works in an operational environment and to have the Test

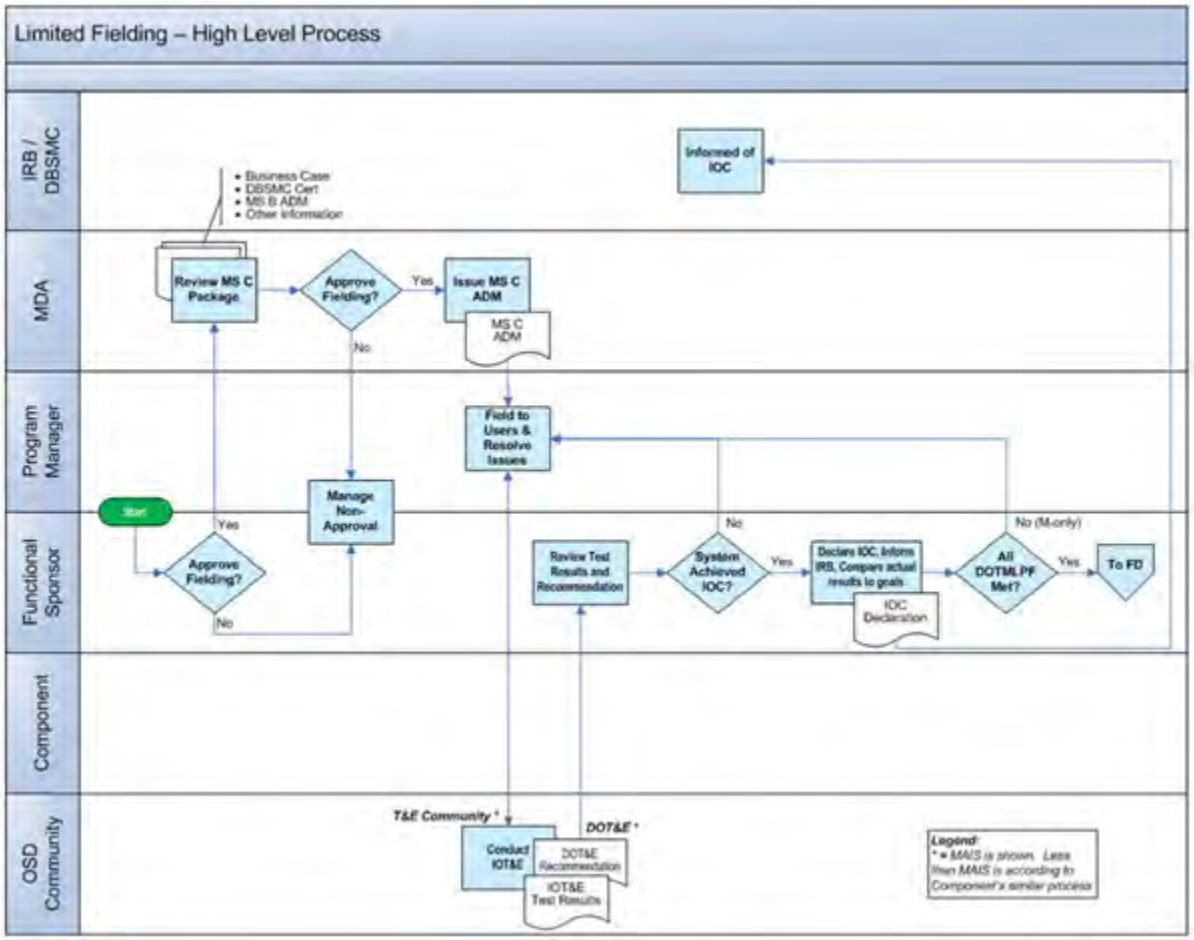
and Evaluation (T&E) community evaluate it against the outcomes (Business Case) and the Test Plan (Business Case).

The outputs and outcomes of the Limited Fielding Phase are:

- An operationally assessed capability that meets the Milestone Decision Authority (MDA)-approved schedule and that includes capabilities that are secure, suitable, operationally useful, and accepted by the user; and
- The Functional Sponsor's written declaration of Initial Operating Capability (IOC).

12.3.4.2. Limited Fielding Phase Process

Figure 12.3.4.2.F1 - Limited Fielding High Level Process Flow



The Limited Fielding Phase begins at MS C when the Milestone Decision Authority (MDA) reviews the updated Business Case and any other required information per previous acquisition decision memorandum (ADMs) and approves the fielding of the capability into an operational environment in accordance with the schedule outlined in

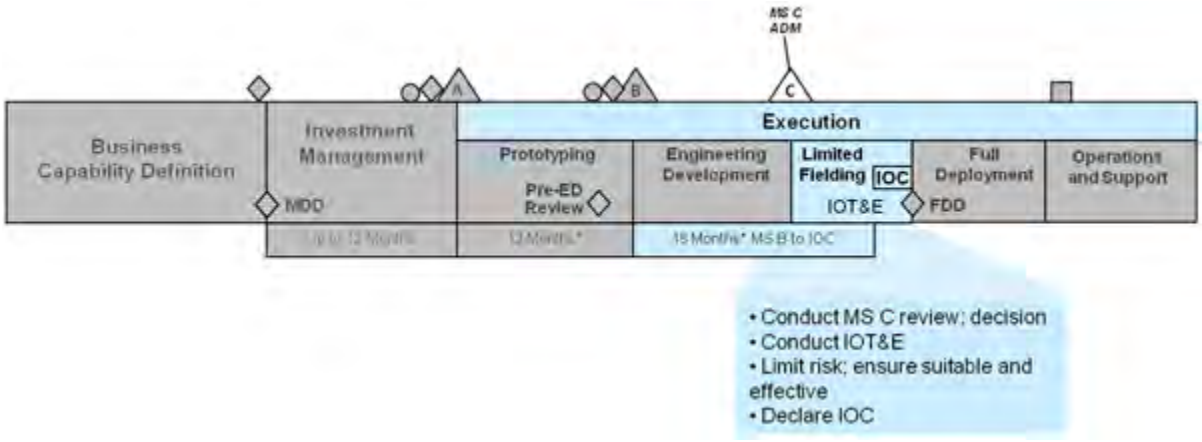
the APB. The MDA's decision is documented in the MS C ADM.

During this Phase, the PM continues to manage the materiel effort and will work closely with users and T&E to resolve issues and execute scheduled initial operational test and evaluation (IOT&E). The Functional Sponsor continues to solve or implement the non-materiel aspects of the solution that will accompany full deployment of the materiel solution. In addition, informed by T&E results and the outcomes defined in the Business Case, the Functional Sponsor will determine whether to declare IOC. For MAIS programs, there are specific test events that may be required to occur; these events and their subsequent processes are discussed in Chapter 9, Section 9.5.8.2 "System Readiness for IOT&E".

At the end of Limited Fielding, the Functional Sponsor will issue a written declaration of IOC and notify the Investment Review Board (IRB). The Functional Sponsor will also determine whether the DOT_LPF-P dependencies have been met sufficiently enough to allow the program to proceed to Full Deployment.

12.3.4.3. Limited Fielding Phase Activities

Figure 12.3.4.3.F1 - Limited Fielding Activities on BCL Model



During Limited Fielding the PM will verify that the materiel solution will support the outcomes (i.e., high-level, business, and program) described in the Business Case and APB for the increment. The operational effectiveness and suitability of the capability is assessed by engaging appropriate T&E communities and collecting end-user feedback. The PM will manage fielding the system to the defined users and manage feedback from users to: identify issues; work with the Functional Sponsor to prioritize issues; and manage priority issues to closure. The PM and Functional Sponsor will identify lessons learned for each increment to help plan subsequent increments.

The PM will also limit risk by working with end-users to ensure they are appropriately trained in using the capability and that issues are identified and addressed expediently. The Functional Sponsor ensures that DOT_LPF-P aspects of the solution have been

integrated as necessary and appropriate and that users have received a complete, usable capability.

When IOT&E results substantially demonstrate that the system is operationally effective, suitable, and survivable, the Functional Sponsor, informed by IOT&E results and DOT&E recommendations (for DBS on the OT&E oversight list), will determine whether IOC has been reached and issue a written IOC declaration to the PM and IRB. The PM will compile a Full Deployment Decision (FDD) review package for the MDA that includes:

- Written declaration of IOC, and
- The updated Business Case.

The Business Case updates may include successive refinement as discovery continues throughout the program life-cycle. At this point updates should include summaries of the revised Life-Cycle Sustainment Plan (LCSP) and Test Plan based on actual IOT&E results.

12.3.5. Full Deployment

12.3.5.1. Purpose, Outputs, and Outcomes

12.3.5.2. Full Deployment Phase Process

12.3.5.3. Full Deployment Phase Activities

12.3.5.3.1. Monitoring Performance Measures

12.3.5.3.2. Conduct Lessons Learned

12.3.5 .Full Deployment

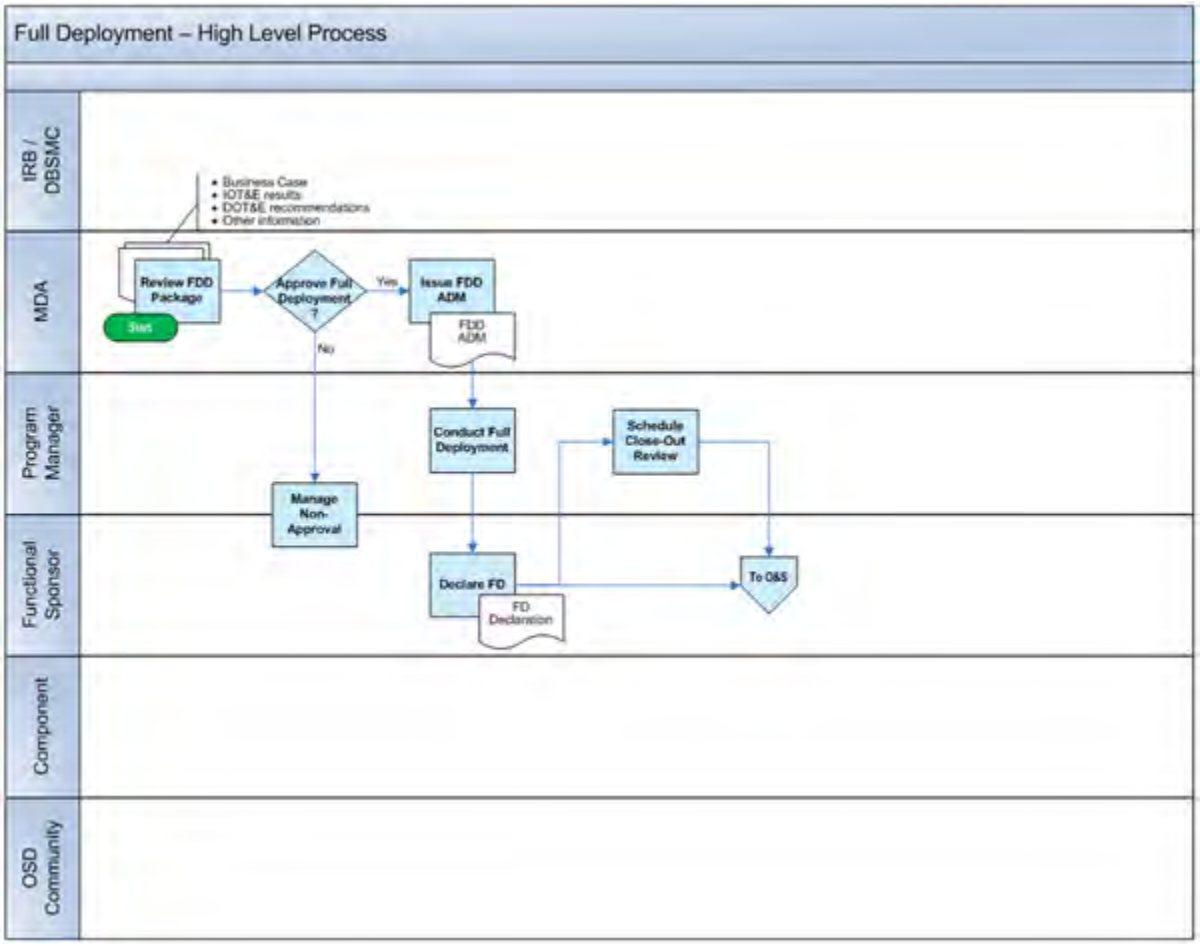
12.3.5.1. Purpose, Outputs, and Outcomes

The purpose of the Full Deployment Phase is to deploy a fully-tested Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) capability to all operational users, in accordance with the acquisition program baseline (APB) and as documented in the approved Business Case.

The outcome of the Full Deployment Phase is to successfully deploy operational capability to users as defined in the Business Case that is secure, suitable, operationally useful, and accepted by the end-user within the milestone decision authority (MDA)-approved schedule.

12.3.5.2. Full Deployment Phase Process

Figure 12.3.5.2.F1 - Full Deployment High Level Process Flow



The Full Deployment Phase begins when the Milestone Decision Authority (MDA) approves the Full Deployment Decision (FDD). Criteria for this decision include:

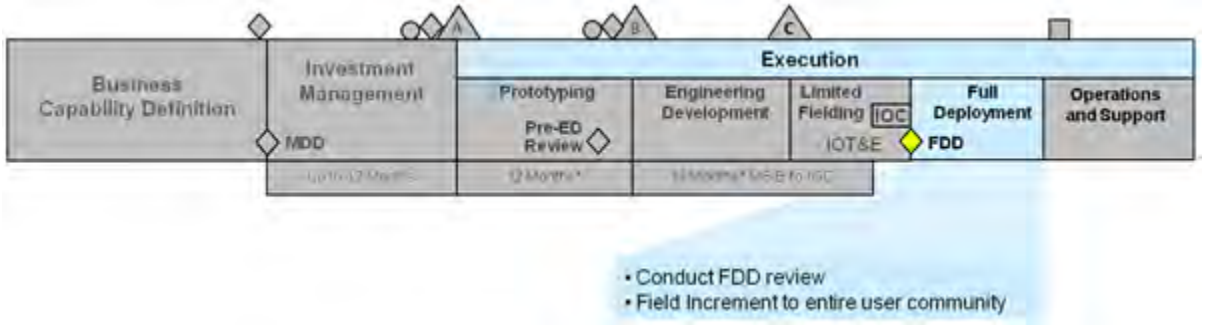
- The Functional Sponsor provided written declaration of Initial Operating Capability (IOC);
- The Functional Sponsor states the associated Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) capability is deployment-ready;
- A low percentage of the total functionality (as documented in the Business Case and the acquisition program baseline (APB)) for the increment remains to be developed. All threshold functionality must have been achieved for IOC. Enhancements, new requirements, and other requirements that are not included as part of the increments APB/Business Case are documented for consideration in a follow-on increment;
- Initial Operational Test and Evaluation (IOT&E) results must indicate that the

system is operationally effective, suitable, and survivable. The final IOT&E report is not a requirement for this decision point;
- Necessary compliance and certifications for deployment have been obtained / achieved;
- Lifecycle support is ready to implement; and
- Insignificant risk remains associated with the technical aspects of the capability, although acceptable fielding risk may remain. The software component of the capability should essentially be risk-free. Deployment risks will exist until they are addressed in the users operational environment.

During this phase, the increment of capability that was successfully deployed and tested during Limited Fielding is deployed to the rest of user community defined in the business case. The activities end when Full Deployment (FD) is declared by the Functional Sponsor and a Close Out Review is scheduled with the Investment Review Board (IRB).

12.3.5.3. Full Deployment Phase Activities

Figure 12.3.5.3.F1 - Full Deployment Activities on BCL Model



Full Deployment activities consist of bringing together change management, training, and technical support to implement the capability to the entire user community described in the Business Case.

The Functional Sponsor is responsible for ensuring the non-materiel components of the DOTMLPF-P solution for the increment have been satisfied and meet the defined outcomes outlined in the Business Case and the cost, schedule, and performance parameters in the APB.

12.3.5.3.1. Monitoring Performance Measures

The program manager and Functional Sponsor must pay close attention to the performance measures during fielding, as these should be an indicator of potential issues. Failure to implement a single aspect of the DOTMLPF-P solution may skew one or more performance measures. For example, if an organization fails to change an underlying business process (to align with a capability's fundamental business process)

and instead continues to use their current business process, the timeliness and efficiencies expected with automation will be diminished. These types of issues will be made visible through performance measures.

12.3.5.3.2. Conduct Lessons Learned

This activity is appropriate in Limited Deployment and / or Full Deployment. The purpose of documenting lessons learned is to understand what worked and what didn't regarding the solutions quality and performance. These lessons can be applied to future efforts, result in general program improvement, reduced risk, increased probability of future successes, and reduce the potential for future failures. Typically, lessons learned will be based on fact and/or perception, both of which should be used as inputs to future DBS activities and archived for use as historical information for future DBS. It may also be beneficial to leverage lessons learned from similar efforts in other organizations.

Full Deployment activities end when the Functional Sponsor declares Full Deployment (FD) and schedules a Close-Out review.

12.3.6. Operations & Support (O&S)

12.3.6.1. Purpose, Outputs, and Outcomes

12.3.6.2. O&S Process

12.3.6.3. O&S Activities

12.3.6.3.1. Stakeholder Feedback

12.3.6.3.2. Lifecycle Sustainment

12.3.6.3.3. Close Out Review

12.3.6. Operations & Support (O&S)

12.3.6.1. Purpose, Outputs, and Outcomes

The purpose of Operations & Support (O&S) is to maintain materiel readiness, provide operational support (e.g., help desk), monitor performance, and sustain the capability in the most cost-effective manner possible over its total lifecycle. The end of this phase is reached with the disposal of the capability when it has reached the end of its useful life.

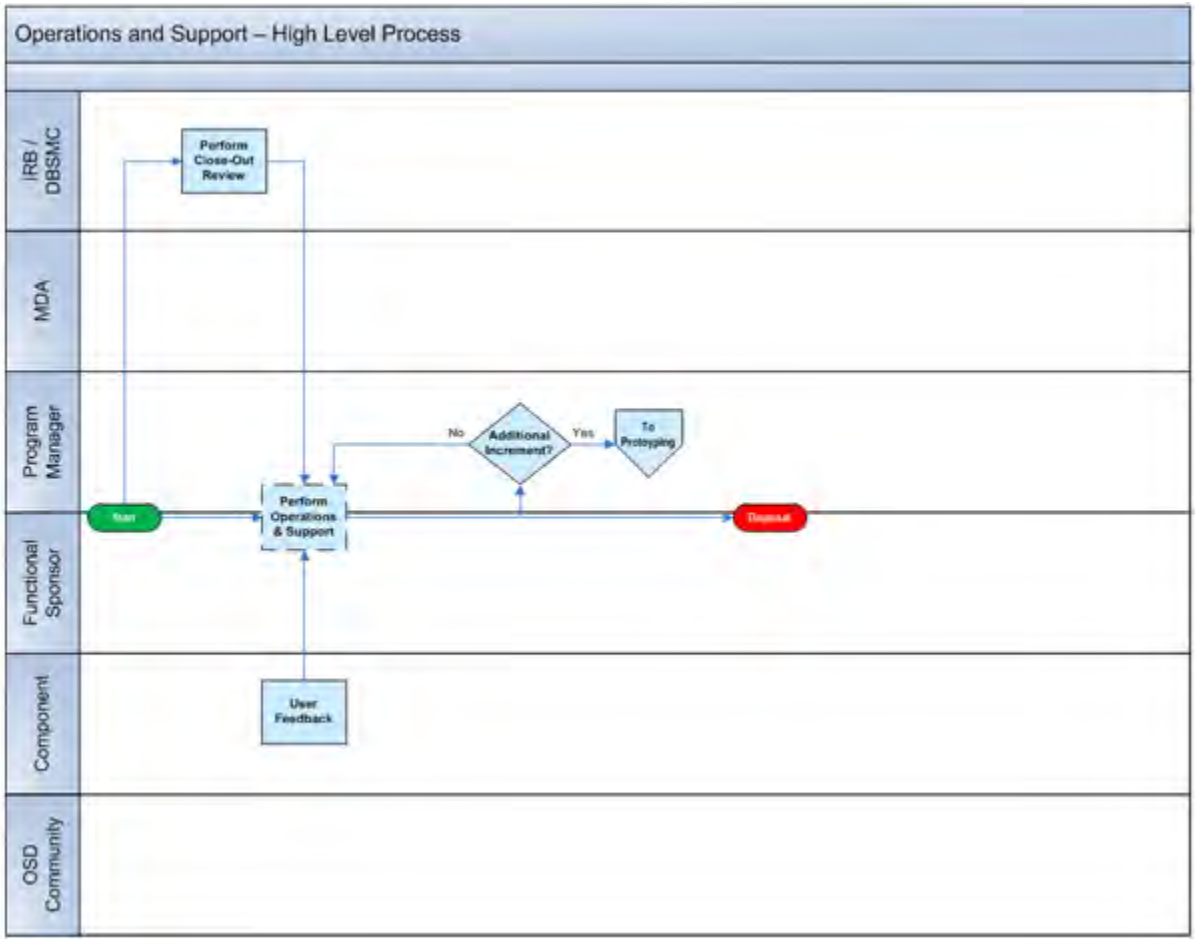
The outputs and outcomes of O&S are:

- Seamless and transparent support to users, until disposal of the capability;
- Requirements inputs for next increment that may impact the Business Case;
- Modifications and upgrades to fielded systems; and

- Updated Systems Engineering planning.

12.3.6.2. O&S Process

Figure 12.3.6.2.F1 - O&S High Level Process Flow

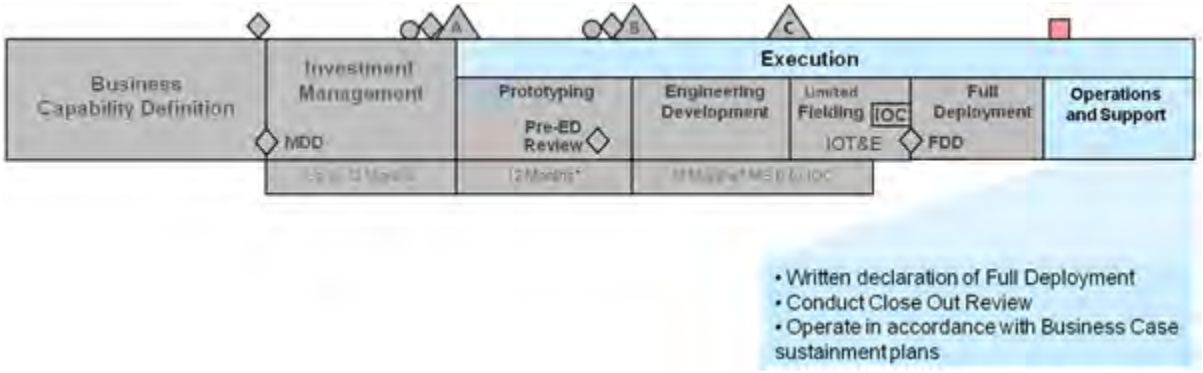


O&S begins when the first increment of a DBS is fully deployed and requires lifecycle sustainment to support users.

While O&S begins with the initial fielding of the capability, the capability fully enters into lifecycle sustainment when the Functional Sponsor decides the capability has been deployed to the full user community and is performing in accordance with the criteria in the Business Case by declaring Full Deployment (FD). Additionally, during O&S, a Close Out Review (which also constitutes the Post-Implementation Review (PIR), traditionally part of Clinger-Cohen) is conducted.

12.3.6.3. O&S Activities

Figure 12.3.6.3.F1 - O&S Activities on BCL Model



12.3.6.3.1. Stakeholder Feedback

One of the major activities during O&S is the evaluation & feedback of the fielded capability by the users, the PM, and the Functional Sponsor. After considering results against the desired outcome for the capability, resourcing, remaining service life, Business Enterprise Architecture (BEA) compliance and technology improvements, this feedback may lead to changes in the software, the product support package, Business Process Re-engineering (BPR), and/or requirements for the next increment. Sustainment is covered by the program's Lifecycle Sustainment Planning and Execution, which seamlessly spans a systems entire life-cycle, from the Analysis of Alternatives (AoA) to disposal. It translates business capability and performance requirements into tailored product support to achieve specified and evolving life cycle product support availability, maintainability, sustainability, scalability, reliability, and affordability parameters. It is flexible and performance-oriented, reflects an evolutionary approach, and accommodates modifications, upgrades, and re-procurement.

12.3.6.3.2. Lifecycle Sustainment

During Lifecycle Sustainment, the program manager (PM) optimizes operational readiness and the Functional Sponsor conducts continuing reviews of sustainment strategies, comparing performance expectations as defined in performance agreements and the Business Case to actual performance results. The Functional Sponsor and PM continuously identify deficiencies in these strategies and update the Business Case as necessary to meet performance requirements.

DAG Chapter 5, Section 5.1.2, "Life-Cycle Sustainment and the DoDI 5000.02 Acquisition Environment" goes into significant depth into sustainment planning. For software development, the following additional guidance is provided:

- Leverage commercial off-the-shelf (COTS) products as much as possible and support them via warranties and Support Agreements to minimize costs.

- Whenever possible, do not customize COTS software. If the software is not customized, the vendor/ developer maintains complete version control of their products, including interoperability, maintainability, and security. This enables modernization of the capability with newer technology without new integration/configuration efforts.
- When COTS products are used in the same manner in the government environment as in the commercial environment (with added physical, information, and operational security), they should be already be covered by organizational standing operating procedures (SOP). When developing the sustainment plans, use existing these SOPs, rather than creating new plans, for both modernization and disposal.
- Due to the nature of DBS capabilities, whenever possible, develop and leverage portfolio sustainment planning (i.e., for those capabilities that utilize the same infrastructure and have similar life-cycle sustainment requirements),), rather than developing a separate plan for each capability.

For DBS, life-cycle sustainment planning evolves throughout BCL:

- ***Prior to Milestone A.*** Planning begins with the Analysis of Alternatives (AoA), describing the notional high-level product support and maintenance concepts to be used for each alternative. When the preferred alternative is selected, these concepts are expanded into a strategy for the entire program, based on the technologies used and acquisition approach. Considerations should include optimizing readiness and minimizing total life-cycle costs.
- ***Prototyping Phase.*** Sustainment planning evolves from the strategy for the program to the management plan for the increment. By the end of this phase, planning should include what sustainment efforts are required for the technology selected; the acquisition approach; and achieves the cost, schedule, and performance parameters outlined in the Business Case.
- ***Engineering Development Phase.*** The sustainment plan evolves into a detailed execution plan for how the product support plan is to be implemented and maintained. As part of the acquisition approach, this includes how the life-cycle support is going to be managed, assessed, and modified. Detailed measures should be developed as part of the acquisition approach and utilized from the initial fielding through disposal.
- ***Limited Fielding and Full Deployment Phase and O&S.*** For the rest of the life-cycle, sustainment planning is constantly monitored and modified to adapt to the addition of new capabilities, glitches, and opportunities in order to achieve desired sustainment measures.

DAG Chapter 5, Section 5.1.2.2, "Life-Cycle Sustainment Plan (LCSP)" Figure 5.1.2.2.F1 provides an outline that can be used to document the program manager's plan for implementing the sustainment strategy. This planning should be modified to fit the DBS acquisition and include, at a minimum, the following:

- ***Life-Cycle Support Strategy.*** Who is going to be responsible for what aspect of

support, throughout the product's life-cycle? This responsibility information is normally summarized in the Program Charter.

- ***Life-Cycle Approach.*** In many cases, support will be provided by multiple entities, each specialized in a different area. This includes COTS vendors, enterprise services, software hosting facilities, and other logistics support.
- ***Supportability Test and Evaluation (T&E) Concept.*** Ensure that T&E for supportability is in place prior to the initial fielding and how issues will be mitigated. Re-use (and reference) similar, proven concepts, and modify them to fit this specific acquisition, rather than developing new concepts.
- ***Integrated Logistics Support Planning.*** A large portion of the life-cycle sustainment planning will be addressed in this section. However, most of the information is contained in other program planning documents. The objective is to ensure the information requirements are addressed, not to repeat this information in another plan.
    - *Design Interfaces.* Should be integrated with SE and Information Support Planning / interface documentation. Normally, it is in the form of DoD Architecture Framework (DoDAF) products at the detailed level.
    - *HAZMAT, Human Systems Integration (HSI), & ESOH.* Generally will not need to be addressed, as COTS capabilities will be utilized as in a similar commercial environment.
    - *Quality Assurance (QA).* Address who is responsible for implementing the QA plan and who provides oversight. Responsibilities are to be covered in the Program Charter.
    - *Reliability and Maintainability (R&M).* Reliability is a systems ability to operate and perform it's intended function for a specified interval under stated conditions. Maintainability is the ease and rapidity with which a system or equipment can be restored to operational status following a failure.

Reliability and maintainability parameters relate to the operational environments, scenarios, and the support that will be provided under these conditions. Reliability and maintainability performance parameters are typically defined in the Business Case, along with other capability measures, and assist the Functional Sponsor in the early identification of issues.

DBS are normally COTS-based. This approach provides a reliable and stable foundation that is easily maintainable for the customer developed application. The use of COTS hardware and software products means commercial sources are available to provide maintenance and support. The program management office may maintain hardware and software maintenance contracts with the appropriate vendors to provide support to the development, test, and operation of systems.

- *Failure Modes Effects and Criticality Analysis (FMECA) (or a similar Component process).* Is generally addressed during Information Assurance (IA) planning and should cover what is considered a critical failure, time-limit's for fixing critical failures, and who is responsible.

- *Damage Modes and Effects Analysis (DMEA) (or similar Component process).* Damage modes are errors or defects in a process, design, or item, especially those that affect the intended function of the capability and/or the process (can be potential or actual).). Effects analysis refers to studying the consequences of those failures.

DMEA is a procedure used in the life-cycle for analysis of potential failure modes within a system to classify the severity and likelihood of the failures. A successful DMEA activity helps a team to identify potential failure modes based on past experience with similar products or processes, enabling the team to design those failures out of the system with the minimum of effort and resource expenditure, thereby reducing development time and costs.

- *Risk Management.* Addressed in a Risk Management Plan. The Program Charter should identify who is responsible for risk management.
- *Safety Engineering.* Safety Engineering is defined as "An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk." If this is necessary (normally not for COTS), it should be addressed as part of the IAS.
- *Standardization, Interchangeability & Interoperability (SI&I)* . Refer to the Business Enterprise Architecture (BEA) . Ensure any interface agreements are documented and can be referenced.
- ***Maintenance Concept for Hardware.*** Address responsibilities for installation, maintenance, refresh, or upgrade of the hardware, to include warranties, agreements, and funding.
- ***Maintenance Concept for Software.*** Address responsibilities for all aspects of the software maintenance, throughout the lifecycle. This includes:
    - Ongoing maintenance to correct existing processing, performance and implementation failures or faults. Based on user feedback, if the program manager/product support manager determines that a problem can only be resolved by changing the software baseline, the program manager must determine the extent of the changes required. If such changes are minor, such changes should be included in the next scheduled maintenance release of the baseline affected.
    - Preventive maintenance for software efficiency and to prevent corruption (e.g., anti-virus tools).
    - Identification of new requirements or upgrades to improve performance, maintainability, and add functionality. If the major changes are required, the program manager should discuss with the MDA prior to implementation.
- ***Tech Support.*** Address operations of the "Service Desk" and different tiers of support. Ensure organizational agreements for different support tiers are addressed in the Program Charter (e.g., the program could document this information in their life-cycle support plan and then reference the Program Charter to that plan.)

- ***Manpower and Personnel.*** Addressed in accordance with the Doctrine, Organization, Training, Leadership and education, Personnel, Facilities, and Policy (DOT_LPF-P) analyses and as part of delivering the comprehensive Doctrine, Organization, Training, Materiel Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) capability. There is a high likelihood that this will be effected by the Business Process Re-engineering (BPR), but may fall outside the scope of the PM and/or the Functional Sponsor.
- ***Training and Training Devices.*** Ensure training requirements, strategy, responsibilities, and methods that will be employed to deliver the best possible instruction are covered, in accordance with the DOTMLPF-P capability delivery.
- ***Supply Support.*** Generally will not apply to DBS. Supplies will primarily be satisfied though hardware and software concepts described above. If not, then ensure they are described.
- ***Support and Test Equipment.*** For COTS, maximum use of commercial service warranties and service contracts are normally utilized. No special tools, General Purpose Electronic Test Equipment or Special Purpose Electronic Test Equipment are normally required to support. If special tools are needed, ensure they are described.
- ***Technical Data.*** See DAG Chapter 5, Section 5.1.6, "Data, Software, and Intellectual Property Rights" .
- ***Packaging, Handling, Storage, and Transportation.*** DBS capabilities generally will not have any unique facility, special packaging, handling, or transportation needs. If they do, ensure they are addressed.
- ***Facilities and Installation.*** Generally, no new facilities are required for DBS. If they are, then they should be addressed.
- ***Support Transition Planning.*** Sustainment Transition Plans are developed to support a program (or increment) after the initial operational capability is achieved and the system moves into full operational capacity where it requires operational support. Since DBS uses an evolutionary approach and is developed in Increments with capability releases, the system is constantly and rapidly evolving to provide new capabilities and functional enhancements. As a result, the operation and sustainment period is very brief as the system transitions from release to release. The activities normally associated within O&S of a system (security and performance management, patches, bug fixes, COTS hardware and software updates, usability improvements, and interoperability updates) are addressed during the development of successive increments or as data updates to fielded versions as required.

However, if a capability is scheduled to cease new development (i.e., the final increment, prior to the MS B decision) and move fully into O&S, this transition planning must be planned for and the appropriate agreements put into place.

- ***Support Resource Funds.*** Ensure funding aspects are adequately addressed. Normally this is for funding that is outside the purview of the program manager. Examples would include hardware replacement and licensing costs while in O&S, development of new capabilities after a Program Office has been deactivated,

and organizational O&M costs.

- ***Configuration Management.*** Although CM is normally captured in a program's CM plan (and considered to be part of the SE discipline) it is crucial for life-cycle support, as different support options may be needed for the different version of the software or technologies that have been released.
- ***Demilitarization, Reutilization and Disposal (DR& D) Strategy.*** At the end of its useful life, a DBS or one or more increments of a DBS is disposed of in accordance with all statutory and regulatory requirements and policy relating to safety, security, and the environment. During the design process, the program manager should estimate and plan for safe disposal. Hardware no longer needed should be disposed of according to each organization equipment disposal procedures or be transferred to another program for reutilization. Software produced or purchased will be maintained in the configuration management library and will be available for reutilization as needed.

12.3.6.3.3. Close Out Review

In O&S, the program manager and Functional Sponsor conduct a Close Out Review, which also serves as the Post Implementation Review (PIR) and fulfills the requirements of such, with the Investment Review Board (IRB) to determine whether or not the delivered capability achieved the outcomes defined in the business case. The Close Out Review is an important vehicle for lessons-learned since it incorporates user feedback and to enable understanding of how well a recently-completed increment meets the needs of users before finalizing the requirements for a subsequent increment. It also informs the IRB of how well an investment performed against expectations and how future increments of capability can be expected to perform.

12.4. DBS-specific Criteria

12.4.1. Time-Limited Development

12.4.2. BCL Governance

12.4.3. Roles and Responsibilities

12.4. DBS-specific Criteria

12.4.1. Time-Limited Development

The reasons for Time-Limited Phases in the Business Capability Lifecycle (BCL) are that:

- Technical capabilities and software development are strongly related to Moore's law, roughly doubling in ability every 18 months (or less); and
- User requirements almost always change as soon as a capability is fielded - as more users take advantage of the solution, new ideas for enhancement or

additional capability tend to increase.

Unlike a traditional "waterfall" acquisition, where requirements and technologies can be defined much earlier in the acquisition process, information technology (IT) acquisitions (specifically in this chapter, defense business systems (DBS)) are characterized by fluid requirements and rapidly changing technology.

The key to successfully fielding IT is to quickly get capability into the hands of users. Too often, users and developers spend years trying to specify requirements in this dynamic environment and never field any capability. Instead, the functional stakeholders should define the business outcomes they want to achieve, how they are going to measure achievement, and acknowledge that things will change.

The success of the BCL approach depends on end-users' prioritization of requirements, the subsequent scoping of each increment, and focusing on fielding useable capability as rapidly as possible. The key is to prioritize requirements and divide them into small, useful capabilities by performing technology trades against cost and requirements to achieve delivery within Milestone Decision Authority (MDA)-approved timelines.

Time-limiting considerations, by phase, are as follows:

- ***Business Capability Definition (BCD) Phase.*** Although this phase is not time limited, it is critical to the success of all the other phases; it defines the problem to be solved and frames the scope of the acquisition. In this Phase, the Functional Sponsor (representing the needs of the end user) defines:
    - What the need / gap / problem is (the Problem Statement);
    - How they will know when the problem is fixed (the high-level outcome(s)); and,
    - How they are going to measure progress towards those outcomes.

Although there are other relevant tasks to be accomplished (see a complete discussion of the Business Capability Definition (BCD) Phase in Section **12.1** , *Business Capability Definition (BCD) Phase*), these have the highest impact on time-limited development (if these are not adequately articulated and agreed to by the Functional Sponsor, it will be unclear what constitutes success and will likely be revisited / redefined).

- ***Investment Management (IM) Phase.*** The time-limit for the IM Phase is 12 months or less. At the start of this Phase, the optimal "To-Be" Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) process should have already been selected, though it is not yet complete. A materiel need is identified, but the specific solution to fulfill it is undefined. Using the Problem Statement, an Analysis of Alternatives (AoA) is conducted to select the best materiel *approach* to solve the problem, or a scoped portion of the problem (i.e., a single problem statement could spawn multiple programs.) Keys for success within the time-limitation are:
    - Define the approach to the materiel solution (e.g., an ERP or Web 2.0

technologies). Ensure assumptions, scope, boundaries and constraints are well-articulated (you may not be able to solve the entire problem with the selected technical solution *today* . Tomorrow brings new technologies, new versions of more-capable software, and updated requirements.)
    - Understanding assumptions, scope, boundaries and constraints. Determine which are statutory and which are "artificial" (an AoA is mandatory, but a subordinate 75-day sub-process may be artificial.) Agreements made with Functional Sponsor(s) and/or the MDA can mitigate artificial constraints.
    - Keep planning at the strategic level. Do not over-plan, because in this environment the plan is going to change. At this stage, the users desired outcomes will be at a very high level. (i.e., "full auditability"). There is no way to address all of the issues that are encountered this early in the process and, even so, requirements would change before completing the associated plans. The result would be an endless do-loop of changing your plans to fulfill new requirements. A key to success is to be able to clearly articulate the approach to solving the problem using the preferred materiel solution (and over-time, the preferred materiel solution is going to change.).
- ***Prototyping Phase.*** BCL mandates completion of Prototyping within 12 months or less of contract/option award. This time-limit also to each subsequent Increment (after Authorization to Proceed (ATP) is granted) as well. The key to completing Prototyping within 12 months is to limit the scope of activities to those absolutely necessary, such as the following:
    - It is critical to obtain the preferred materiel solution as rapidly as possible.
    - Ensure the Functional Sponsor has prioritized requirements (business outcomes) before the MS A decision. Expect this prioritized list to be more requirements than can be fulfilled in 18 months. Part of this phase's activities is scoping the requirements for the Increment to achieve a useful capability that can be delivered in less than 18 months. Multiple prototype or pilot demonstrations may be necessary to reach agreement on an acceptable, operationally useful, and affordable increment of capability that can be delivered within this timeframe.
    - Significant emphasis must be placed on leveraging enterprise services and existing infrastructures. These are known entities and will significantly reduce engineering development and testing risks in the next phase.
    - Develop a reasonable plan to build and deploy. Also, set user expectations. The objective is not to maximize the number of requirements that can be incorporated into an 18 month schedule; rather it is to get the useful capabilities out to the user as rapidly as possible. When the program manager and the Functional Sponsor have agreed which requirements are going to be satisfied and the technologies to be used for the Increment, the Business Case must be updated and the Functional Sponsor must provide a description of what will constitute IOC.
- ***Engineering Development (ED) and Limited Fielding Phases.*** After the Engineering Development Phase contract is awarded (post-MS B) the a MAIS

DBS program has 18 months to obtain a Full Deployment Decision (FDD) to include achieving Initial Operating Capability (IOC). This should be the focus of all of the program's efforts. When achieving IOC appears imminent, focus can be shifted to the next goal(s) - the Full-Deployment Decision (FDD) and possibly the next increment.

- ***Full Deployment Phase and O&S.*** These phases are not time-limited.

The timelines for the phases of BCL must be taken into consideration during program planning, scoping, and Business Case development. Violations of these timelines require re-validation of the Business Case by the Investment Review Board (IRB) (and the MDA, as required), and can potentially slow down the delivery of capability to the user. Table **12.4.1.T1** outlines BCL timelines.

Table 12.4.1.T1 - BCL Timelines

Decision Period	Time Allotted
Materiel Development Decision (MDD) to Milestone (MS) A	12 months
MS A to IOC*	Within 5 years
MS A to Full Deployment Decision (FDD)	Within 5 years (or if no MS A, from when the preferred alternative was selected by the MDA)
MS A (contract / option award) to MS B	12 months or less***
ATP** (contract / option award) to MS B	12 months or less***
MS B (contract / option award) to FDD	18 months or less***

- *IOC is a Functional Sponsor written declaration; though the MDA will generally not grant a MS A if it is not clear that IOC is achievable within 5 years of MS A.
- **Authority to Proceed (ATP) is for follow-on increments. There is one MS A for the overall program, but there may be multiple ATPs (if there are multiple increments). ATP will "kick off" an increment.
- ***If activities can be conducted in time periods much less than the maximum time allotted, reflecting this in schedules and plans promotes visibility, and rapid capability delivery.

12.4.2. BCL Governance

The Business Capability Lifecycle (BCL) aligns defense business system (DBS) requirements, investment, and acquisition processes into a single, tiered integrated decision-making framework that provides oversight commensurate with program complexity and risk. The Functional Sponsor is a key focal point at the Component level in the earliest stages of the capability and partners with the program manager (PM) throughout the process as the capability matures. This integrated model of governance is depicted in Figure **12.4.2.F1** :

Figure 12.4.2.F1 - Governance

Each Investment Review Board (IRB) assesses investments in its portfolio relative to their functional needs, as well as the impact on end-to-end business process improvements as guided by the Business Enterprise Architecture (BEA) , articulated in the DoD Enterprise Transition Plan (ETP), the DoD Strategic Management Plan (SMP), and/or described in Component architectures and transition plans. These products provide both the end-state and the roadmap to deliver more robust business capabilities.

For MAIS, the IRBs review requirement changes and technical configuration changes during the development process that have the potential to result in cost and schedule impacts to the program. Such changes will generally be disapproved or deferred to future increments and will not be approved unless funds are identified and schedule

impacts mitigated.

The Defense Business Systems Management Committee (DBSMC) guides the Department in developing and implementing integrated business functions and capabilities. The DBSMC is the final approval authority for all certification decisions.

The MDA is responsible for making DBS acquisition decisions and relies on the IRB's advice in its role as OIPT and information provided by the Component to include: functional requirements; the Business Case; appropriate Business Process Re-engineering (BPR) and BEA compliance (as determined by the Pre-Certifying Authority (PCA));and a DBSMC-approved investment decision.

12.4.3. Roles and Responsibilities

DoD officials and organizations have specific investment and acquisition-related roles and responsibilities throughout the Business Capability Lifecycle (BCL), as outlined in Table **12.4.3.T1.** and **T2** .

Table 12.4.3.T1 - DoD Component-Level Roles and Responsibilities

DoD Component	Role and Responsibility
Chief Management Officer (CMO)	Responsible for determining those DBS investments within their area of responsibility have adequately performed BPR activities and complies with the Business Enterprise Architecture (BEA)
Component Acquisition Executive (CAE)	Responsible for all acquisition functions within their Component. This includes both the Service Acquisition Executives (SAEs) for the Military Departments and acquisition executives in other DoD Components. The CAE designates the MDA for DBSs other than MAIS (or as otherwise delegated).
Pre-Certification Authority (PCA)	Generally, assesses and pre-certifies compliance with the BEA and BPR. Also ensures required documentation is available for IRB review prior to the IRB meeting.

Functional Sponsor	Represents the end-user / user community. Responsible for activities of the BCD Phase, defining the business need (problem / gap), desired outcomes, and acceptance criteria, remaining actively engaged in the program throughout its lifecycle in order to achieve the complete Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) solution, and for declaring IOC and the criteria for declaring Full Deployment (FD). Works with the program manager to complete the Program Charter. Generally, the Functional Sponsor establishes and continues a strong working relationship with the program manager throughout the lifecycle of the DBS beginning early in IM.
Program Manager (PM)	Designated early during IM and is accountable for the successful development and deployment of the DBS to deliver on the outcomes defined by the Functional Sponsor. The program manager develops the APB for each increment and manages the program to meet cost, schedule, and performance objectives. program managers shall have requisite experience and competency in delivering IT solutions, including the ability to build and manage multi-disciplinary integrated teams and in identifying and mitigating risk. The program manager also establishes and continues a strong working relationship with the Functional Sponsor throughout the lifecycle of the DBS beginning early in IM.

Table 12.4.3.T2 -OSD-Level Roles and Responsibilities

OSD Component	Role and Responsibility
Assistant Secretary of Defense, Research and Engineering ASD(R&E)	If the MDA determines that a Technology Readiness Assessments (TRA) is required, the ASD(R&E) coordinates with DoD Component representatives to accomplish.
Certification Authorities (CA) (Approval Authorities, per 10 U.S.C., 2222)	Via the IRBs, provides oversight of investment review processes and procedures for DBSs supporting their area(s) of responsibility to certify investments and make recommendations to the DBSMC. CA's also advise the MDA on acquisition matters. CAs may serve as IRB Chairs, or may designate an IRB Chair.

Defense Business Systems Management Committee (DBSMC)	Per sections 186 and 2222 of Title 10, U.S.C., provides investment oversight for DBS and guides the transformation activities of the business areas of the DoD. The DBSMC approves IRB Certifications and CMO/DCMO BPR determinations, and is the final authority for DBS requirements.
Director, Cost Assessment and Program Evaluation (DCAPE)	Provides independent analysis and advice to inform decision-making. Responsible for developing and approving Analysis of Alternatives (AoA) Study Guidance for MAIS DBS. May also review, assess and / or conduct independent cost estimates, cost analyses, and economic analyses, as appropriate.
Deputy Assistant Secretary of Defense, Developmental Test and Evaluation DASD(DT&E)	Ensures that developmental test and evaluation is effectively addressed throughout the entire lifecycle of the DBS. DASD(DT&E) works in partnership with the DOT&E) to review and approve the Test Plan section(s) for MAIS described in the Business Case and to collaborate on an integrated testing approach.
Director, Operational Test and Evaluation (DOT&E)	Responsible for the test and evaluation of each DBS. Works with the Functional Sponsor and program manager to ensure that roles and responsibilities, along with required test resources, are adequately addressed with mutual agreement early on in the testing process. The DOT&E also works with the DASD(DT&E) to approve the Test Plan section(s) for MAIS described in the Business Case and to collaborate on an integrated testing approach.
Deputy Assistant Secretary of Defense, Systems Engineering DASD(SE)	Reviews and approves the systems engineering sections of the Business Case for MAIS.
DoD Chief Information Officer (CIO)	Works with DoD Components, the IRBs, the DBSMC, and other stakeholders to ensure that DBSs develop in compliance with applicable statute (i.e., the Clinger-Cohen Act (CCA)), regulations, and in accordance with DoD policy on architecture, design, interoperability, security, and information assurance (IA).
Deputy Chief Management Officer (DCMO)	Responsible for determining BPR efforts have been undertaken as appropriate and for determining BEA compliance for non-military department and joint DBS. The DCMO may also hold delegated MDA authority for certain DBS and may also serve as the Chair of governance forums for review and decision making purposes.

Enterprise Risk Assessment Methodology (ERAM) Team	Conducts independent assessments to identify risk, recommend risk mitigations to the program manager, and provide insight to decision-makers as part of BCL.
Information Review Board (IRB)	Advise the IRB Chair and the MDA and provide cross-functional expertise and oversight for DBS. The IRBs serve as the OIPT for the MDA for DBS. The IRBs review Problem Statements (for all potential DBS), Business Cases, and requirements changes / technical configuration changes for MAIS in development that have the potential to impact program cost and schedule. The IRBs also work to ensure that investments are aligned with the BEA to ensure that DBS support enterprise priorities.
IRB Chair	In addition to reviewing all information mentioned above as a member of the IRB, the IRB Chair has decision authority, and will therefore decide on Problem Statement approvals, make acquisition-related recommendations to the MDA, serve as the validation authority for DBS requirements, and hold specific duties regarding IRB Certification actions.
Milestone Decision Authority (MDA)	Responsible for making DBS acquisition decisions as well as determining the appropriate BCL entry / acquisition phases and the extent to which regulatory and other non-statutory documentation can be tailored. The MDA is also advised by the IRB Chairs during the review process.

12.5. Tools and Methods

12.5.1. Business Case

12.5.1.1. Content Updates

12.5.1.2. General Guidance

12.5.1.3. Evaluation

12.5.2. DOTMLPF-P Analysis

12.5.3. Outcomes and Measures Development

12.5. Tools and Methods

12.5.1. Business Case

The Business Case is a summarization of the Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) solution

performed for a point in time. It is a brief, high-level document, with input from the Functional Sponsor and program manager, which outlines the program/increment and typically does not provide the detail data that the program office produces.

The principal purposes of the Business Case are to:

- Facilitate a way of thinking that causes Components to consider a business capability's value, risk and relative priority as fundamental elements of submission;
- Require those proposing a solution to justify its value and to self-eliminate any proposals that are not of demonstrable value;
- Enable DoD leadership to rapidly determine if a concept or proposed solution is of value to the enterprise and is achievable compared to the relative merits of alternative proposals; and
- Enable DoD leadership to objectively measure the subsequent achievement of the capability's benefit's.

The Business Case provides a compelling, defendable and credible justification for the DOTMLPF-P solution to the defined problem, with corresponding outcomes and performance measures for use throughout the capability's lifecycle. It is an evolving document, with the intent of providing an overview of the current program status in a condensed format. It is structured to best support the program and does not have a mandatory format, but it must cover all of the statutory and regulatory information requirements.

Supporting the Business Case is program documentation. This documentation is what the Component feels is necessary to successfully implement the capability. Each Component has approval processes for documentation and normally does not require Office of the Secretary of Defense (OSD) approval (the DoDI 5000.02 directs the Heads of the DoD Components to keep the issuance of any additional guidance necessary to implement the mandatory procedures to a minimum). Programs still need to make this documentation available to oversight bodies: It just does not require their approval. In select cases, the applicable office with statutory authority (e.g., DASD(DT), DOT&E, etc...) sign-off on the appropriate section of the Business Case to agree that the program plans are adequately addressed.

The Business Case provides a template to ensure that a problem, it's root cause and DOTMLPF-P issues are thoroughly analyzed; that all options have been considered; that risks are identified; risk mitigation plans are sufficient; and that there is a high degree of confidence the expenditure of resources and funds are justified and value-added. It provides leadership with sufficient information to make informed investment decisions within the context of enterprise priorities and available resources. Components are responsible for the development and maintenance of the Business Case.

12.5.1.1. Content Updates

In coordination with the Functional Sponsor, the Component Acquisition Executive (CAE), and the Investment Review Board (IRB), the program manager (PM) must review and, when necessary, update the Business Case to incorporate any changes driven by an increment to ensure that:

- The problem to be solved remains valid;
- The selected solution is still appropriate to achieve the desired outcomes;
- The materiel solution can continue to be executed within the established cost, schedule and performance parameters; and
- The expected benefit's will be realized.

Additionally, the PM must update and/or revise the Business Case if changes occur to the problem scope, context or the requirements for additional modernization funding.

For follow-on increments, it is recommended that an "addendum" be added to the existing Business Case to preserve all program-level information, to reduce rewrites, and to show history and continuity of the program.

If the Business Case is deemed no longer valid, but the capability is still needed, the Functional Sponsor, along with the CAE, must notify the IRB and the MDA immediately to determine how to proceed. If the Business Case is deemed no longer valid and the capability no longer needed, the Functional Sponsor, along with the CAE, must immediately notify the IRB and the Milestone Decision Authority (MDA) of their intention to discontinue the program.

12.5.1.2. General Guidance

- The Business Case is not a technical proposal, though it will contain technical information.
- Utilize tables to summarize information as much as logically possible.
- Up front, explain the decision or action being sought (i.e., seeking a MS A decision in order to do X, Y, and Z.).
- Do not write the Executive Summary until the rest of the content is finished. The Executive Summary should be updated each time a decision is being sought (**Note:** after the first Executive Summary is written, it may only require cursory updates in the future).
- The Executive Summary should be concise and focused on the issue at hand. Do not discuss "general knowledge" data or information (such as, the history of ERPs in the Department, the largesse of the DoD, the challenges of the DoD IT environment, easily "Google-able" information, etc.).
- Clarify between usage of increments or releases, what operational business capability will be delivered in a specific increment or release, and how each works toward achieving the overall outcome from a measures perspective (is it 25% of the overall capability?)

- Measures should not focus on compliance - rather, what compliance will a Law, Regulation, Policy enable (i.e., compliance with SFIS requirements will enable _____.) or conversely, if required compliance with an L, R, or P introduces risk or additional requirements.
- As a general guideline, the complete Problem Statement analysis section for a (projected) MAIS solution should be less than 7 pages in total length and, depending on the number of alternatives considered, the total Business Case may vary from 15 to 40 pages.
- A Problem Statement should never be more than 3-4 sentences in length.
- The Business Case will always be judged on the quality of information it contains, not on the length of the content.

12.5.1.3. Evaluation

A Business Case will be evaluated to ensure:

- The investment has value to the enterprise and aligns with enterprise priorities;
- A materiel solution has not been selected too early in the process, and evidence that robust analysis has been conducted;
- Proper management and support of senior officials for the proposed solution;
- Definition of the scope for the proposed solution and measurable desired outcomes;
- Clear evidence that BPR has been done or is being completed;
- Ability of the Component to deliver the benefits; and
- Dedicated resources are working on the highest value opportunities.

12.5.2. DOTMLPF-P Analysis

Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) is an analytical approach and method for defining the operational context of a perceived problem. There are many options for how to approach a DOTMLPF-P analysis; however, it may be valuable to establish an internal or DoD Component standard. A valuable reference are the JCIDS materials .

Doctrine.

- Is there existing doctrine that addresses or relates to the business need? Is it Joint? Service? Agency?
- Are there operating procedures in place that are NOT being followed which contribute to the identified need?
- If no doctrine is in place which pertains to the defined need, does new doctrine need to be developed and implemented that will provide a total or partial solution to the need?

Organization.

- Where is the problem occurring? What organizations is the problem occurring in?
- What are the primary and secondary mission / management focus of those organizations?
- What are the organizational values and priorities?
- Is the organization properly staffed and funded to deal with the issue?
- Are commanding officers / senior management aware of the issues?
- Is the issue already in some type of organizational issue list?
- If so, why isn't the issue being resolved?
- Who exactly is aware of / being impacted by the issue?

Training.

- Is the issue caused, at least in part, by a complete lack of or inadequate training?
- Does training exist which addresses the issue?
- Is the training being delivered effectively?
- How are training results being measured and monitored?
- Is the issue caused by a lack of competency or proficiency on existing systems and equipment?
- Was the issue discovered in an exercise or during training?
- Do personnel affected by the issue have access to training?
- Is the training effort supported by leadership?
- Is training properly staffed and funded?

Materiel.

- Is the issue caused, at least in part, by inadequate systems or equipment?
- What legacy systems exist where the problem is occurring?
- What functionality would a new system provide that currently does not exist?
- What increases in operational performance are needed to resolve the issue?
- Is the issue caused by a lack of competency or proficiency on existing systems and equipment?
- Can increases in performance be achieved without development of a new system?
- Who would be the primary and secondary users of the proposed systems or equipment?
- Is interoperability either a driver or barrier in issue resolution?

Leadership and education.

- Is the issue caused, at least in part, by inability or decreased ability to cooperate/coordinate / communicate with external organizations?
- Does leadership understand the scope of the problem?
- Does leadership have resources at its disposal to correct the issue?
- Has leadership been trained on effective change management principles?

- Has leadership properly assessed the level of criticality, threat, urgency, risk, etc. of the operational impact(s) of the issue?
- Is leadership aware of the drivers and barriers to resolving the issue within her / his own organization?
- Has leadership identified inter-service / agency cultural drivers and barriers which hinder issue resolution?

Personnel.

- Is the issue caused, at least in part, by inability or decreased ability to place qualified and trained personnel in the correct occupational specialties?
- If issue resolution is likely to involve new materiel, systems, or equipment, are different occupational specialty codes needed to properly staff new systems?
- Do new personnel have support to onboard to their jobs?
- Are the right personnel in the right positions (skill set match)?

Facilities.

- Is the problem caused, at least in part, by inadequate infrastructure?
    - Is physical distance of equipment, etc. leading to other problems?
- Are there proper environmental controls?
- Is there a lack of operations and maintenance?

Policy.

- Is there existing policy that addresses or relates to the business need? Is it Joint? Service? Agency?
- If no policy exists which pertains to the defined need, does new policy need be developed and implemented that will provide a total or partial solution to the need?
    - Can policy be developed and signed at the Component level? Will policy require OSD-level sponsorship, coordination and / or signature?

12.5.3. Outcomes and Measures Development

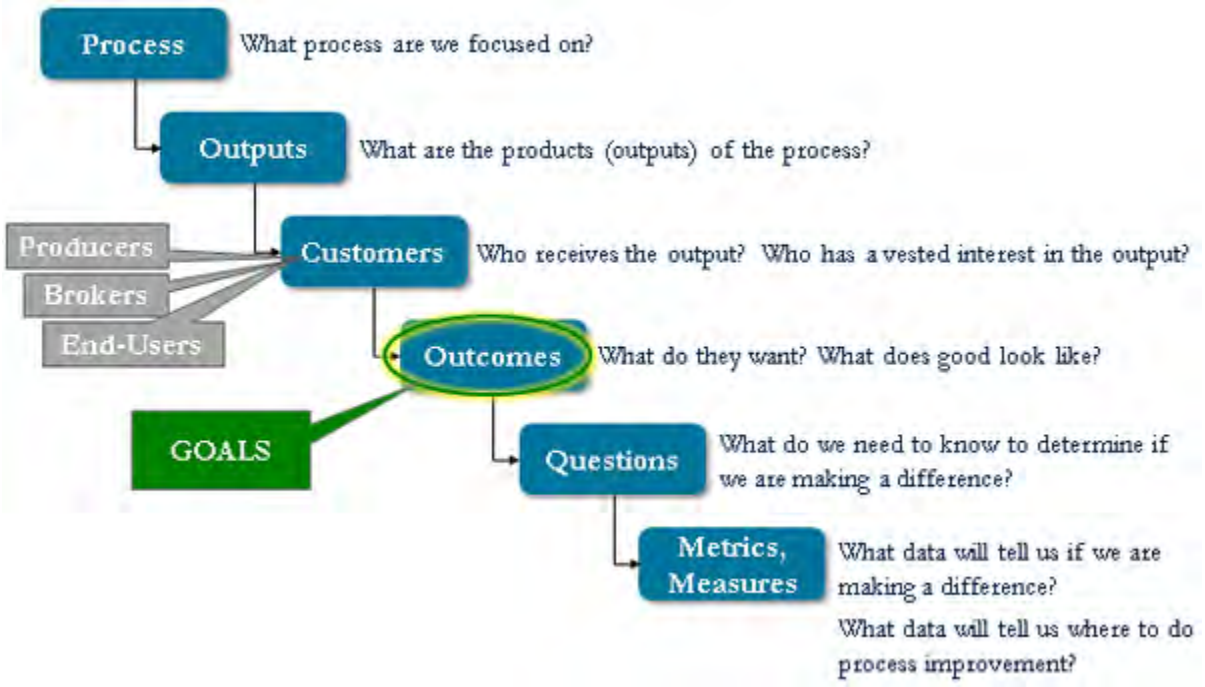
Outcomes and measures development begins during the Business Capability Definition Phase (BCD), helping to scope the effort and identify outcomes that will be used at a future point for testing. During subsequent Business Capability Lifecycle (BCL) activities, outcomes and measures are refined and the Functional Sponsor works closely with the acquisition and testing communities in order to ensure the information is appropriate and relevant to the program at applicable lifecycle points.

The outcome should explicitly state the business value of the resources to be invested and to allow management to prioritize and weigh investments. The outcome provides strategic alignment and clear criterion against which to evaluate potential approaches. It always starts with the desired functional result and is used to focus behaviors and

results by answering the "what's in it for me?" question. Corresponding measures must be specific, actionable, measureable, relevant, and timely operational capabilities that can be achieved against their corresponding outcomes.

Figure **12.5.3.F1** depicts a logical manner of thought in which a process can be decomposed into goals, and finally into metrics and / or measures:

Figure 12.5.3.F1 - Developing Measures and Metrics



Correspondingly, Figure **12.5.3.F2** portrays an example hierarchy of outcomes and metrics / measures in BCL. They decompose from a strategic level to an execution (operational) level of specificity.

Figure 12.5.3.F2 - Outcome Hierarchy

High-Level Outcomes (HLOs). HLOs are developed during BCD as part of the "To-Be" Analysis, support one or more Strategic Management Plan (SMP) goals/objectives, and constrain business outcomes. They address the strategic alignment principle - programs must enable effective portfolio management by aligning individual investments to SMP goals and objectives - that is central to BCL.

HLO measures are developed at the same strategic level as HLOs. They define measurements for strategic purpose and priority and address how the investment will meet enterprise-level expectations in finite terms.

Business Outcomes . Business outcomes are developed during BCD when the "To-Be" Analysis is refined as a result of BPR. Business outcomes should align to specific end-to-end (E2E) business processes defined in the Business Enterprise Architecture (BEA) and describe the functional users intended result of fulfilling an identified business capability gap. They are the HLOs decomposed into observable and measureable business results or changes in business performance.

Business outcome measures, like HLO measures, should address how the investment will meet enterprise-level expectations. They should also add increasing level of detail to determine how the investment will meet the business results outlined in the business outcomes.

Program Outcomes. Program outcomes support business outcomes and are

developed during IM based on the preferred solution. Program outcomes are scoped to the preferred solution and should include specific business rules that explicitly define the "To-Be" state and should address expectations of how the preferred solution will address business outcomes and HLOs.

Program outcome measures must demonstrate the value of the preferred solution to the Department and should provide cost and period of performance expectations for each business capability to be delivered as part of the preferred solution, taking into account the Better Buying Power affordability target.

System Requirements. System requirements fulfill program outcomes and are developed throughout Execution as the chosen solution is built and realized against the HLOs and capability levels are added; they represent the capability delivery aspects of a chosen solution.

TIP: System-level requirements are generally NOT included in the Business Case; but are critical for the operation of the program.

System requirements measures, like their outcomes counterparts, gain increasing level of detail as a chosen solution matures through building, testing, and deployment.

- During Prototyping, system requirements address solution design and program plan tracking and are tied to a work breakdown structure and schedule.
- During Engineering Development, system requirements address developing the solution by executing the plan, include development testing results, and should join the cost, schedule, and performance measures of program realization to support a MS C decision.
- During Limited Fielding, system requirements should include technical quality criteria and cost, schedule, and performance measures. They should focus on displaying added detail to support end-user testing and the results of initial operational test and evaluation (IOT&E) to support initial operating capability (IOC) and a Full Deployment Decision (FDD).
- During Full Deployment, system requirements should reflect program execution details and sustainment activities (help desk, operations) to coincide with transitioning from execution to O&S.

12.5.4. BEA and BCL

12.5.4. BEA and BCL

The Business Enterprise Architecture (BEA) is the enterprise architecture for all DoD defense business systems (DBS) and capabilities and reflects the DoD business transformation priorities; the business capabilities required to support those priorities; and the combinations of enterprise systems and initiatives that enable those capabilities. It also supports use of this information within an end-to-end (E2E) Framework. BCL investment decisions require this Departmental perspective provided

by the E2Es to compare investment opportunities across the Department and to allow effective portfolio management of DBS . Access to the BEAs contents is provided on the DCMOs BEA webpage.

The E2E Business Flows that comprise the Departments E2E Framework play a critical role in how DoD builds business capabilities, as business processes actually span, rather than operate within, functional areas. Each E2E Business Flow represents the life-cycle of business processes that are executed in order to fulfill a business requirement/need of organizations throughout DoD. In order to achieve business process optimization, specific DoD organizations need to identify and decompose the E2E Business Flows across the functional silos of the organization.

Decomposing the E2E flows first requires each organization to identify those E2E Business Flows that apply to them. Next, the organization can break down the E2E Business Flow reference model into a representation of the specific Business Processes they perform, identify Business Process inefficiencies both within and across functional silos, and optimize the organizations E2E Business Flows accordingly.

For more detailed information on BEA Compliance, decomposing E2E Business Flows, and more general information on both the BEA and the E2Es, refer to the DCMOs BEA webpage .

DEFENSE ACQUISITION GUIDEBOOK
Chapter 13 - Program Protection

13.0. Overview

13.0. Overview

Program Protection is the integrating process for mitigating and managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability, or supply chain exploitation/insertion, battlefield loss, and unauthorized or inadvertent disclosure throughout the acquisition lifecycle.

At its core, Program Protection protects technology, components, and information from compromise through the cost-effective application of countermeasures to mitigate risks posed by threats and vulnerabilities. In a simple sense, Program Protection seeks to defend warfighting capability by keeping secret things from getting out and keeping malicious things from getting in. Where the capability is derived from advanced or leading-edge technology, Program Protection mitigates the risk that the technology will be lost to an adversary; where the capability is derived from integration of commercially available or developed components, Program Protection mitigates the risk that design vulnerabilities or supply chains will be exploited to degrade system performance. The Program Protection Plan (PPP) is the milestone acquisition document that describes the plan, responsibilities, and decisions for all Program Protection activities.

13.0.1. Purpose

This chapter provides guidance and expectations for the major activities associated with Program Protection.

13.0.2. Contents

Chapter 13 addresses the following topics:

The Program Protection Process

The Program Protection Plan (PPP)

Critical Program Information (CPI) and Mission-Critical Functions and Components

Intelligence and Counterintelligence (CI) Support

Vulnerability Assessment

Risk Assessment

Countermeasures

Horizontal Protection

Foreign Involvement

Managing and Implementing Program Protection Plans (PPP)

Compromises

Costs

Contracting

Detailed Systems Security Engineering (SSE)

Program Protection Plan (PPP) Review/Approval

Program Protection Plan (PPP) Classification Guidance

13.1. The Program Protection Process

Program Protection is an iterative risk management process within system design and acquisition, composed of the following activities:

- Critical Program Information (CPI) Identification and Criticality Analysis (Section 13.3)
- Threat Analysis (Section 13.4)
- Vulnerability Assessment (Section 13.5)
- Risk Assessment (Section 13.6)
- Countermeasure Implementation (Section 13.7)
- Horizontal Protection (Section 13.8)
- Foreign Involvement (Section 13.9)

Additional considerations (Defense Exportability Features, Program Protection Plan (PPP) Approval, etc.) are covered in subsequent sections.

Commanders, Program Executive Officers, S&T Project Site Directors, Program Managers (PMs) (used throughout this chapter to include program/project leaders prior to official PM designation), systems engineering, system security, information assurance, Test and Evaluation (T&E), and acquisition personnel should be aware of the Program Protection process and should be engaged in supporting it. Program Managers are responsible with complying with this process holistically such that protection decisions are made in the context and trade space of other cost, schedule, and performance considerations. It is important to implement this process across the full acquisition lifecycle in order to build security into the system. The process is repeated at each of the following points in the lifecycle, building on the growing system maturity:

- Systems Engineering Technical Reviews (SETR) (see Section 13.10.2 for further elaboration on specific Systems Engineering Technical Reviews event expectations), starting Pre-Milestone A with the Alternative Systems Review (ASR)

- Systems Engineering (SE) analyses that support preparation for each Acquisition Milestone (see Sections 13.7.6 and 13.14 for further elaboration on how this process is tied to lifecycle phase-related Systems Security Engineering (SSE)
- Development and release of each Request for Proposal (RFP) (see Section 13.13.1 for further details on what should be incorporated in the Request for Proposal (RFP) package)

At each of these points, the process is iterated several times to achieve comprehensive results that are integrated into the system design and acquisition. This process applies to all programs and projects regardless of acquisition category (ACAT) or status (i.e., all acquisition categories (ACATs), Quick Reaction Capability (QRC), Request for Information (RFI), Joint Capability Technology Demonstration (JCTD), Science and Technology (S&T) or Authority to Operate (ATO)), or whether the technology is meant for Government and or military use.

13.2. The Program Protection Plan (PPP)

Program Protection is the Department's holistic approach for delivering trusted systems and ensures that programs adequately protect their technology, components, and information. The purpose of the Program Protection Plan (PPP) is to ensure that programs adequately protect their technology, components, and information throughout the acquisition process during design, development, delivery and sustainment. The scope of information includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, compromise or defeat warfighting capability.

The process of preparing a PPP is intended to help program offices consciously think through what needs to be protected and to develop a plan to provide that protection. Once a PPP is in place, it should guide program office security measures and be updated as threats and vulnerabilities change or are better understood.

It is important that an end-to-end system view be taken when developing and executing the PPP. External, interdependent, or government furnished components that may be outside a program managers' control must be considered.

The PPP is the focal point for documentation of the program protection analysis, plans and implementation within the program for understanding and managing the full spectrum of the program throughout the acquisition lifecycle. The PPP is a plan, not a treatise; it should contain the information someone working on the program needs to carry out his or her Program Protection responsibilities and it should be generated as part of the program planning process.

The Program Protection Plan Outline and Guidance , established as expected business practice through a July 18, 2011 Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) policy memo, can be found at: http://www.acq.osd.mil/se/docs/PDUSD-ATLMemo-Expected-Bus-Practice-PPP-

18Jul11.pdf .

13.3. Critical Program Information (CPI) and Mission-Critical Functions and Components

Critical Program Information (CPI) and mission-critical functions and components are the foundations of Program Protection. They are the technology, components, and information that provide mission-essential capability to our defense acquisition programs, and Program Protection is the process of managing the risks that they will be compromised.

13.3.1. Critical Program Information (CPI)

DoDI 5200.39 defines Critical Program Information (CPI) as Elements or components of a research, development, and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes, and end-items. Includes elements or components critical to a military system or network mission effectiveness. Includes technology that would reduce the US technological advantage if it came under foreign control.

Metaphorically, CPI should be thought of as the technological crown jewels of the program. The United States gains military advantages from maintaining technology leads in key areas, so we must protect them from compromise in the development environment and on fielded systems.

CPI may include classified military information that is considered a national security asset that will be protected and shared with foreign governments only when there is a clearly defined benefit to the United States (see DoD Instruction 5200.39). It may also include Controlled Unclassified Information (CUI), which is official unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations such as the International Traffic in Arms Regulations for U.S. Munitions List items and the Export Administration Regulations for commerce controlled dual-use items. In some cases (dependent on the PM's

determination) a commercial-off-the shelf (COTS) technology can be designated CPI if the COTS element is determined to fulfill a critical function within the system and the risk of manipulation needs mitigation.

CPI requires protection to prevent unauthorized or inadvertent disclosure, destruction, transfer, alteration, reverse engineering, or loss (often referred to as "compromise").

CPI identified during research and development or Science and Technology should be safeguarded to sustain or advance the DoD technological lead in the warfighter's battlespace or joint operational arena.

The CPI, if compromised, will significantly alter program direction; result in unauthorized or inadvertent disclosure of the program or system capabilities; shorten the combat effective life of the system; or require additional research, development, test, and evaluation resources to counter the impact of its loss.

The theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents, directly threatens the economic competitiveness of the U.S. economy. Increasingly, foreign governments, through a variety of means, actively target U.S. businesses, academic centers, and scientific developments to obtain critical technologies and thereby provide their own economies with an advantage. Industrial espionage, by both traditionally friendly nations and recognized adversaries, proliferated in the 1990s and has intensified with computer network attacks today.

Information that may be restricted and protected is identified, marked, and controlled in accordance with DoD Directives 5230.24 and 5230.25 or applicable national-level policy and is limited to the following:

- Information that is classified in accordance with Executive Order 13526, and
- Unclassified information that has restrictions placed on its distribution by:
- U.S. Statutes (e.g., Arms Export Control Act , Export Administration Act);
- Statute-driven national regulations (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR)); and
- Related national policy (e.g., Executive Order 13526, National Security Decision Directive 189).
- 13.3.1.1 Critical Program Information (CPI) Identification

CPI determination is done with decision aids and Subject Matter Experts (SMEs). As general guidance, PMs should identify an element or component as CPI if:

- Critical technology components will endure over its lifecycle
- A critical component which supports the warfighter is difficult to replace
- A capability depends on technology that was adjusted/adapted/calibrated during testing and there is no other way to extrapolate usage/function/application
- The component / element was identified as CPI previously and the technology

has been improved or has been adapted for a new application
- The component / element contains a unique attribute that provides a clear warfighting advantage (i.e. automation, decreased response time, a force multiplier)
- The component / element involves a unique method, technique, application that cannot be achieved using alternate methods and techniques
- The component / elements performance depends on a specific production process or procedure
- The component / element affords significant operational savings and/or lower operational risks over prior doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) methods
- The Technology Protection and/or Systems Engineering (SE) Team recommends that the component/element is identified as CPI
- The component / element will be exported through Foreign Military Sales (FMS)/Direct Commercial Sales (DCS) or International Cooperation

PMs should contact their Component research and development acquisition protection community for assistance in identifying CPI.

13.3.2. Mission-Critical Functions and Components

Mission-critical functions are those functions of the system being acquired that, if corrupted or disabled, would likely lead to mission failure or degradation. Mission-critical components are primarily the elements of the system (hardware, software, and firmware) that implement critical functions. In addition, the system components which implement protections of those inherently critical components, and other components with unmediated access to those inherently critical components, may themselves be mission-critical.

Mission-critical functions and components are equal in importance to Critical Program Information (CPI) with respect to their inclusion in comprehensive program protection, it's planning (documented in the Program Protection Plan (PPP)), and it's execution, including:

- Trade-space considerations (including cost/benefit analyses)
- Resource allocations (staffing and budget)
- Countermeasures planning and implementation
- Adjustment of countermeasures, as appropriate, for variations in the planned use or environment of inherited critical components
- Summary of consequences if compromised
- Residual risk identification after countermeasures are implemented, including follow-up mitigation plans and actions

Efforts to identify mission-critical functions and components and their protection must begin early in the lifecycle and be revised as system designs evolve and mature.

13.3.2.1. Criticality Analysis (CA)

What is a Criticality Analysis (CA)? CA is the primary method by which mission-critical functions and components are identified and prioritized. It is an end-to-end functional decomposition of the system which involves:

- Identifying and prioritizing system mission threads;
- Decomposing the mission threads into their mission-critical functions; and
- Identifying the system components (hardware, software, and firmware) that implement those functions; i.e., components that are critical to the mission effectiveness of the system or an interfaced network.

Also included are components that defend or have unmediated access to mission-critical components.

The identified functions and components are assigned levels of criticality commensurate with the consequence of their failure on the system's ability to perform its mission, as shown in Table 13.3.2.1.T1 .

Table 13.3.2.1.T1. Protection Failure Criticality Levels

Level I Total Mission Failure	Program protection failure that results in total compromise of mission capability
Level II Significant/Unacceptable Degradation	Program protection failure that results in unacceptable compromise of mission capability or significant mission degradation
Level III Partial/Acceptable	Program protection failure that results in partial compromise of mission capability or partial mission degradation
Level IV Negligible	Program protection failure that results in little or no compromise of mission capability

When to perform a CA? The CA is an iterative process. To be effective, many CAs must be executed across the acquisition lifecycle, building on the growing system maturity, knowledge gained from prior CAs, updated risk assessment information, and updated threat and vulnerability data.

At each key decision point, system design changes may result in adding or removing specific items from the list of critical system functions and components. Guidance for the iterative performance of CAs includes:

- Prior to Milestone A: Evaluate mission-threads, identify system functions, and analyze notional system architectures to identify mission-critical functions.
- Prior to Milestone B: Refine the critical function list and identify critical system components and candidate subcomponents (hardware, software, and firmware).
- Prior to CDR: Analyze the detailed design/architecture and update the list to

identify all critical system components and subcomponents.

Who performs the CAs? The Government program office should perform an initial CA early in the lifecycle (pre-Milestone A). When contracts are awarded, the DoD contracting office should develop Requests for Proposals (RFPs) that require contractors to perform updated CAs periodically, based on earlier CAs (see Section 13.13.1.2 for guidance on what to include in the Statement of Work (SOW) requirements).

The CA should be led by systems engineers and mission/operator representatives; however, it is a team effort and mission-critical functions and components must be identified by a multi-disciplined group.

How is a CA performed? What is the process? While the Government should perform an initial CA during the Materiel Solution Analysis (MSA) phase, realize that it may only be possible to execute some of the steps in the CA process given below and/or to execute them at a high level. As noted previously, to be effective, Criticality Analyses (CAs) must be executed iteratively across the acquisition lifecycle, building on the growing system maturity, knowledge gained from prior CAs, updated risk assessment information, and updated threat and vulnerability data.

For example, the first pass through the CA process, together with assessments of vulnerabilities, threats, risks, and countermeasures, might take just a few days and provide a 30% solution. This CA might only involve Subject Matter Expert (SME) input during several work sessions (to address system and architecture), as opposed to detailed information collected from numerous program documents. For an early iteration, precision is not possible, as it takes several iterations to complete the initial Criticality Analysis (CA).

The detailed procedural steps in performing a CA are:

Identify Missions and Mission-Essential Functions	**Sources of Information**
1. Identify mission threads and principle system functions. • Derived first during pre-Milestone A and revised as needed for successive development milestones.	Joint Capabilities Integration Development System (JCIDS) Documents: Initial Capabilities Documents (ICD), Capability Development Documents (CDD), Capability Production Documents (CPD) Concept of Operations

2. If possible or necessary, group the mission capabilities by relative importance. Training or reporting functions may not be as important as core mission capabilities.	Operational Representative Subject Matter Expertise (Integration Experts, Chief Engineers)
3. Identify the systems mission-critical functions based on mission threads and the likelihood of mission failure if the function is corrupted or disabled. (Mission-critical functions may include navigating, targeting, fire control, etc.).	Activity Diagrams Use Cases Functional Decomposition Potential Department of Defense Architecture Framework (DODAF) Sources • OV-5 (Operational Activity Model) • SV-4 (System Functionality Description) Subject Matter Expertise
Identify Critical Subsystems, Configuration Items, and Components	
4. Map the mission threads and functions to the system architecture and identify critical subsystems, Configuration Items, and sub-Cis (components). Note : Focus on Configuration Items and components containing Information and Communications Technologies (ICT). Logic-bearing components have been singled out as often implementing critical functions and as susceptible to lifecycle corruption.	System/Segment Design Document Architecture Description Document Requirements Traceability/Verify. Matrix Potential Department of Defense Architecture Framework (DODAF) Sources • SV-5a (Operational Activity to System Function Traceability Matrix)

5. Assign levels of criticality (I, II, III, IV) to the identified Configuration Items or components. Factors or criteria may include: • Frequency of component use across mission threads • Presence of redundancy triple-redundant designs can indicate critical functions. • Subject matter expertise	Subject Matter Expertise • Systems Engineer • Operators Representative • Program Office
6. Identify any Configuration Items or components that do not directly implement critical functions, but either have unmediated communications access (i.e., an open access channel) to one or more critical functions or protect a critical function. • Which components give or receive information to/from this the critical components? Note : a non-critical component may communicate with a critical function in a way that exposes the critical function to attack. In some cases, the architecture may need to include defensive functions or other countermeasures to protect the critical functions.	Architecture Diagrams Subject Matter Expertise Data Flow Diagram
Initial Start Conditions	
7. Identify critical conditions/information required to initialize the system to complete mission-essential functions. a. What information is needed to successfully execute capabilities? How is this information obtained, provided, or accessed by the system? b. How quickly must information be received to be useful? c. Does the sequence in which the system initializes itself (power, software load, etc.) have an impact on performance?	Data Flow Diagram Information Support Plan
8. Based on the answers to the questions above, identify these functions or components to be included in Program Protection risk management.	
Operating Environment	

9. Identify the system functions or components required to support operations in the intended environment. This may include propulsion (the system has to roll, float, fly, etc.), thermal regulation (keep warm in space, keep cool in other places, etc.) or other environmentally relevant subsystems that must be operational before the system can perform it's missions.	Architecture Diagrams
10. Identify the Information and Communications Technologies (ICT) implementing those system functions and any associated vulnerabilities with the design and implementation of that Information and Communications Technologies (ICT).	
Critical Suppliers	
11. Identify suppliers of critical configuration items or Information and Communications Technologies (ICT) components.	Manufacturing Lead
Note: Repeat this process as the system architecture is refined or modified, such as at SETRs and major acquisition milestone decision points • Design changes may result in adding or removing specific Configuration Items and sub-Configuration Items from the list of critical functions and components	

Important considerations in carrying out the CA process described above include:

- Document the results of each step
  - Include rationale
- Use SE tools to support the analysis; for example:
  - Fault-tree analysis can be useful in determining critical components (see Section 13.7.6 for further details)
  - What information is needed to successfully execute capabilities?
  - How is this information obtained, provided, or accessed by the system?
  - How quickly must information be received to be useful?
  - Does the sequence in which the system initializes itself (power, software load, etc.) have an impact on performance?
  - Example: These may include propulsion (the system has to roll, float, fly, etc.), thermal regulation (keep warm in space, keep cool in other places, etc.), or other environmentally relevant subsystems that must be operational before the system can perform it's missions.
- Use available artifacts to inform the CA; for example:
  - SE artifacts such as architectures/designs and requirements traceability matrices
  - Available threat and vulnerability information

    - Residual vulnerability risk assessments to inform follow-up CAs

- In isolating critical functions/components, identify critical conditions/information required to initialize the system to complete mission-critical functions

- Identify the subsystems or components required to support operations in the intended environment

What is the CA output? The expected output of an effective CA process is:

- A complete list of mission-critical functions and components
- Criticality Level assignments for all items in the list
- Rationale for inclusion or exclusion from the list
- Supplier information for each critical component
- Identification of critical elements for inclusion in a Defense Intelligence Agency (DIA) Threat Assessment Center (TAC) Request (See Section 13.4)

The identification of critical functions and components and the assessment of system impact if compromised is documented in the Program Protection Plan (PPP) as discussed in Appendix C (Table C-1) of the PPP Outline.

The prioritization of Level I and Level II components for expending resources and attention will be documented in the PPP as discussed in Appendix C (Table C-2) of the PPP Outline.

Why is the CA performed? The level I and selected level II components from the CA are used as inputs to the threat assessment, vulnerability assessment, risk assessment, and countermeasure selection. The following sections describe these activities.

13.4. Intelligence and Counterintelligence (CI) Support

13.4.1. Defense Intelligence Agency Supply Chain Risk Management Threat Assessment Center (DIA SCRM TAC)

13.4.1.1. Threat Assessments

13.4.1.2. Criticality Analysis to Inform TAC Requests

13.4.2. Counterintelligence Support

13.4.2.1. Requesting Counterintelligence (CI) Analytical Support

13.4.2.2. Preliminary Counterintelligence (CI) Analytical Product

13.4.2.3. Final Counterintelligence (CI) Analytical Product

13.4. Intelligence and Counterintelligence (CI) Support

13.4.1. Defense Intelligence Agency Supply Chain Risk Management Threat Assessment Center (DIA SCRM TAC)

DoD has designated the Defense Intelligence Agency (DIA) to be the DoD enterprise focal point for threat assessments needed by the DoD acquisition community to assess supplier risks. DIA established the Threat Assessment Center (TAC) for this purpose. The Threat Assessment Center (TAC) provides the enterprise management and interface to resources within the National Counterintelligence Executive (NCIX), and coordinates with the Defense Intelligence and Defense Counterintelligence Components to provide standardized all-source intelligence assessments to support acquisition risk management efforts. This enterprise integration role of the DoD Threat Assessment Center (TAC) was designed and organized to achieve comprehensive and consistent engagements with the United States Government (USG) across all of the Military Departments (MILDEPs) and Defense Agencies needs for supplier threat assessments and to ensure the efficiency and coherent use of the results provided to the acquisition community.

13.4.1.1. Threat Assessments

Defense Intelligence Agency (DIA) Threat Assessments provide specific and timely threat characterization of the identified suppliers to inform program management. Threat Assessment Center (TAC) reports are used by the Program Manager and the engineering team to assist in selecting supplier and/or architecture alternatives and developing appropriate mitigations for supply chain risks. For the policy and procedures regarding the request, receipts, and handling of Threat Assessment Center (TAC) reports, refer to DoD Instruction O-5240.24.

Supplier threat assessment requests are developed based on the criticality analysis. An annotated work breakdown structure (WBS) or system breakdown structure (SBS) that identifies the suppliers of the critical functions components may be used to assist with the creation of the Threat Assessment Center (TAC) requests. Supplier threat assessment requests may be submitted as soon as sources of critical capability are identifiable. Near the end of the Materiel Solution Analysis (MSA) Phase, as some threat information is available from the capstone threat assessment (CTA) and

technologies and potential suppliers are identified, Supply Chain Risk Management (SCRM) Threat Assessments may be used to assist in defining lowest risk architectures, based on suppliers for particular architecture alternatives. Note that early in the system lifecycle the threat requests may be more focused on suppliers in general technology areas to inform architecture choices, while later in the system lifecycle they may be more focused on critical components defined in the criticality analysis.

13.4.1.2. Criticality Analysis to Inform TAC Requests

Engineering activities related to Supply Chain Risk Management (SCRM) begin as architecture alternatives are considered and continue throughout the acquisition lifecycle. As the systems engineering team develops the initial view of system requirements and system design concepts, a criticality analysis is performed to define critical technology elements. Criticality analysis produces a list of critical components and suppliers that are used to generate Threat Assessment Center (TAC) requests and supplier risk mitigation.

The criticality analysis begins early in the system acquisition lifecycle and continues to be updated and enhanced through Milestone C, becoming more specific as architecture decisions are made and the system boundaries are fully defined. The engineering team may at any point, beginning prior to Milestone A, identify technology elements and potential manufacturers and request supplier threat assessments. It is expected that the number of supplier threat assessment requests will grow as the criticality analysis becomes more specific and the system architecture and boundaries are fully specified, i.e., the greatest number of Threat Assessment Center (TAC) requests will typically occur between Milestones B and C (i.e., Preliminary Design Review (PDR) and Critical Design Review (CDR)). See Section 13.3.2 for more information.

13.4.2. Counterintelligence Support

[This section will be updated to reflect implementation guidance for DoD Instruction O-5240.24, but content was not ready by the submission deadline for this major update.]

When an acquisition program containing Critical Program Information (CPI) is initiated, the Program Manager (PM) should request a counterintelligence (CI) analysis of CPI from the servicing CI organization. The CI analysis focuses on how the opposition sees the program and on how to counter the opposition's collection efforts. The CI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of the U.S. program. Therefore, CI organizations need information that describes the CPI and its projected use to determine the foreign collection threat to an acquisition program.

The CI analytical product that results from the analysis will provide the PM with an evaluation of foreign collection threats to specific program or project technologies, the impact if that technology is compromised, and the identification of related foreign technologies that could impact program or project success. The CI analytical product is

updated as necessary (usually prior to each major milestone decision) throughout the acquisition process. Changes are briefed to the Program or PM within 60 days.

13.4.2.1. Requesting Counterintelligence (CI) Analytical Support

The PM's request to the counterintelligence organization for an analytical product normally contains the following information and is classified according to content:

- Program office, designator, and address;
- PM's name and telephone number;
- Point of contact's (POCs) name, address, and telephone number;
- Supporting or supported programs' or projects' names and locations;
- Operational employment role, if any;
- List of CPI;
- Relationship to key technologies or other controlled technology lists of the Departments of Defense, Commerce, and/or State;
- CPI technical description, including distinguishing characteristics (e.g., emissions; sight or sensor sensitivities) and methods of CPI transmittal, usage, storage, and testing;
- Use of foreign equipment or technology during testing (if known);
- Anticipated foreign involvement in the development, testing, or production of the U.S. system;
- Contractor names, locations, Points of Contact (POCs), and telephone numbers, as well as the identification of each CPI used at each location; and
- Reports of known or suspected compromise of CPI.

13.4.2.2. Preliminary Counterintelligence (CI) Analytical Product

After the request is submitted, the DoD Component CI organization provides a preliminary CI analytical product to the program manager within 90 days. A preliminary analytical product is more generic and less detailed than the final product. It is limited in use since it only provides an indication of which countries have the capability to collect intelligence on the U.S. system or technology as well as the possible interest and/or intention to collect it. The preliminary CI analytical product may serve as the basis for the draft Program Protection Plan.

13.4.2.3. Final Counterintelligence (CI) Analytical Product

The program manager approves the Program Protection Plan only after the final CI analysis of Critical Program Information (CPI) has been received from the applicable DoD Component CI and/or intelligence support activity. Normally, the CI analysis of CPI is returned to the requesting program office within 180 days of the CI and/or intelligence organization receiving the request.

The CI analysis of CPI answers the following questions about CPI:

- Which foreign interests might be targeting the CPI and why?
- What capabilities does each foreign interest have to collect information on the CPI at each location identified by the program office?
- Does evidence exist to indicate that a program CPI has been targeted?
- Has any CPI been compromised?

13.5. Vulnerability Assessment

This section briefly describes a process for identifying vulnerabilities in systems. A vulnerability is any weakness in system design, development, production, or operation that can be exploited by a threat to defeat a systems mission objectives or significantly degrade it's performance. Decisions about which vulnerabilities need to be addressed and which countermeasures or mitigation approaches should be applied will be based on an overall understanding of threats, risks, and program priorities. Vulnerability assessment is a step in the overall risk assessment process, as described in Section 13.5 .

Vulnerability assessments should focus first on the mission-critical functions and components identified by a Criticality Analysis (see Section 13.3.2) and the Critical Program Information (CPI) identified (see Section 13.3.1). The search for vulnerabilities should begin with these critical functions, associated components and CPI.

13.5.1. Approaches to Identifying Vulnerabilities

Potential malicious activities that could interfere with a systems operation should be considered throughout a systems design, development testing, production, and maintenance. Vulnerabilities identified early in a systems design can often be eliminated with simple design changes at lower cost. Vulnerabilities found later may require add-on protection measures or operating constraints that may be less effective and more expensive.

The principal vulnerabilities to watch for in an overall review of system engineering processes are:

- Access paths within the supply chain that would allow threats to introduce components that could cause the system to fail at some later time (components here include hardware, software, and firmware); and
- Access paths that would allow threats to trigger a component malfunction or failure at a time of their choosing.

Supply chain here means any point in a systems design, engineering and manufacturing development, production, configuration in the field, updates, and maintenance. Access opportunities may be for extended or brief periods (but potentially exploitable).

Two design processes that have proven effective in identifying vulnerabilities are Fault

Tree Analysis (FTA) and Failure Modes, Effects, and Criticality Analysis (FMECA). An important twist in applying these techniques is that the potential sources of failures are malicious actors, not random device failures. Malicious actors invalidate many assumptions made about randomness and event independence in reliability analysis. Both FTA and FMECA assume hypothetical system or mission failures have occurred, and trace back through the system to determine contributing component malfunctions or failures. For a vulnerability assessment, the possible access paths and opportunities a threat would have to exercise to introduce the vulnerability or trigger the failure must also be considered.

For software, a number of software tools are available that will identify common vulnerabilities. These tools apply different criteria and often find different flaws. It is therefore beneficial to run code through multiple tools.

Controls on access to software during development and in the field are critical to limiting opportunities for exploitation. One approach to testing access controls and software vulnerabilities in general is Red Teaming. Red teams typically subject a system under test to a series of attacks, simulating the tactics of an actual threat. (See further discussion of software tools and access controls in Section 13.7.3, Software Assurance .)

13.5.2. Rating Vulnerability Severity

The consequences of exploiting a vulnerability should be levels on the same scale as criticality (catastrophic, critical, marginal, and negligible). Vulnerability levels however, may not be the same as the criticality levels. For example, a vulnerability may expose a critical function in a way that has only a marginal consequence. At the same time, another vulnerability may expose several critical functions that taken together could lead to a catastrophic system failure.

Additional factors that should be rated include the ease or difficulty of exploiting a vulnerability, the developers or maintainers ability to detect access used to introduce or trigger a vulnerability, and any other deterrents to threats such as the consequences of being caught. A summary table of the vulnerability assessment is illustrated in Table 13.5.2.T1 .

Table 13.5.2.T1. Sample summary vulnerability assessment table

Critical Components (Hardware, Software, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)	Exposure

Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II	Low
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I	High
SW Algorithm A	None	Very Low	II	Very Low
FPGA 123	Vulnerability 1 Vulnerability 23	Low	I	Low

13.5.3. Identifying Vulnerability Mitigations or Countermeasures

There are multiple countermeasures available to mitigate a wide range of possible vulnerability risks. Design changes may either 1) eliminate an exploitation, 2) reduce the consequences of exploitation, or 3) block the access necessary for introduction or exploitation. Add-on protection mechanisms may block the access required to trigger an exploitation. An effective update process, particularly for software, can correct or counteract vulnerabilities discovered after fielding.

As a result of globalization, commercial off-the-shelf (COTS) components are designed and manufactured anywhere in the world, and it may be difficult or impossible to trace all opportunities for malicious access. If the source of a particular component might be compromised, it may be possible to substitute a comparable component from another, more dependable source. Anonymous purchases (Blind Buys) may prevent an untrustworthy supplier from knowing where the component is being used. More extensive testing may be required for critical components from unverified or less dependable sources. A variety of different countermeasures should be identified to inform and provide options for the program managers risk-mitigation decisions.

13.5.4. Interactions with Other Program Protection Processes

Investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality levels of functions and components identified in earlier criticality analyses. Investigation of vulnerabilities may also identify additional threats, or opportunities for threats, that were not considered risks in earlier vulnerability assessments. Vulnerabilities inform the risk assessment and the countermeasure cost-risk-benefit trade-off.

Discovery of a potentially malicious source from the threat assessment may warrant additional checks for vulnerabilities in other (less-critical) products procured from that

source. Therefore, threat assessments can inform vulnerability assessments.

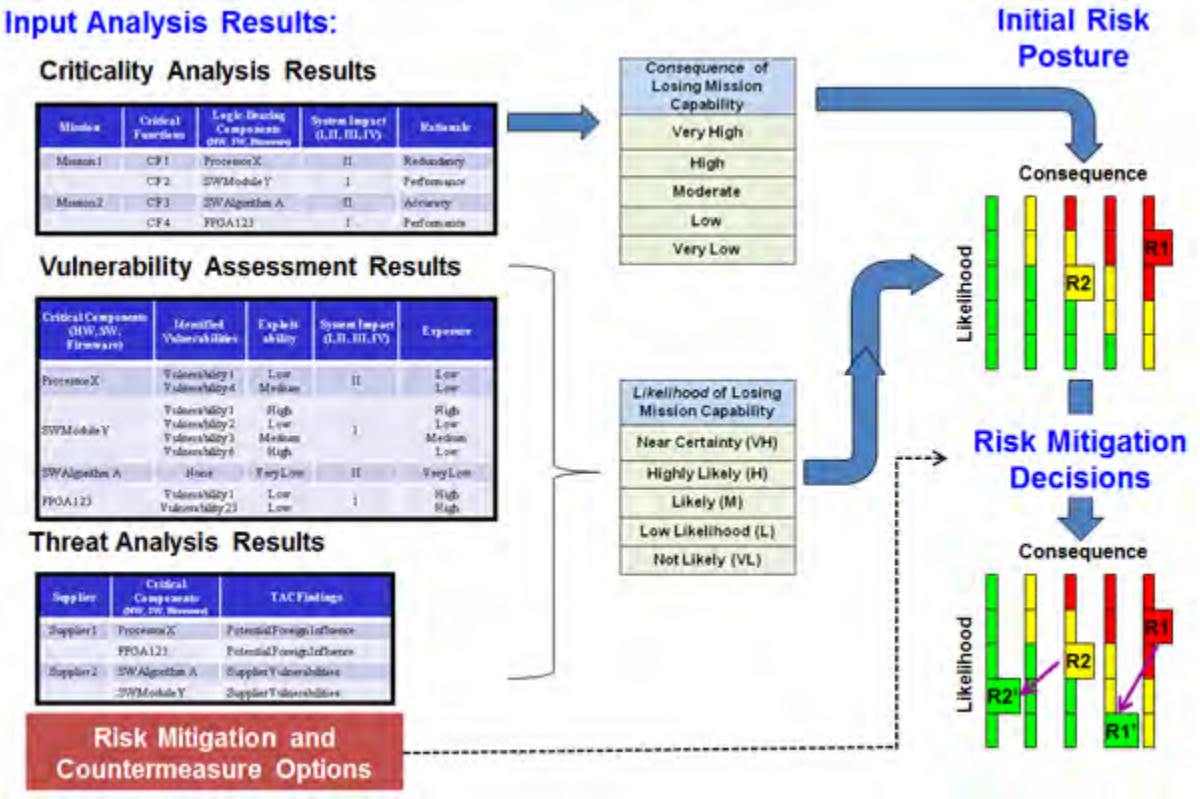
In the Program Protection Plan (PPP) the vulnerability process should be documented at a high level along with the person responsible for the process. The date of the vulnerability assessment, the results of the vulnerability assessment and the planned dates or period of future vulnerability assessments is also recorded in the PPP.

13.6. Risk Assessment

13.6. Risk Assessment

For each Level I and Level II critical function or component the program performs a risk assessment. Figure 13.6.F1 shows the overall risk assessment methodology.

Figure 13.6.F1. Risk Assessment Methodology



The system impact level from the criticality analysis is used to determine the risk consequence. The risk likelihood is based upon the vulnerability assessment and the knowledge or suspicion of threats within the supply chain and potential vulnerabilities within supplied hardware, software, and firmware products. Each Service and program may have specific guidance on how to use the threat assessment and vulnerability assessment to develop the risk likelihood. A basic method which may be used in the

absence of program or service specific guidance is described in this section.

One way to translate the threat assessments and vulnerability assessments into risk likelihood or probability is to develop specific questions for supply chain and software assurance. The following paragraphs list two sets of sample Yes/No vulnerability questions that a program can use to establish the risk likelihood. The first set of vulnerability questions applies to supply chain considerations.

- **Does the Contractor:**
  - Have visibility into lower-level suppliers that provide sub-components used in constructing or assembling critical components?
  - Vet suppliers of critical function components (hardware / software / firmware) based upon the security of their processes?
  - Have processes to verify critical function components received from suppliers to ensure that components are free from malicious insertion (e.g. seals, inspection, secure shipping, testing, etc.)?
  - Have controls in place to ensure technical manuals are printed by a trusted supplier who limit's access to the technical material?
  - Have a process to establish trusted suppliers of critical components?
  - Require suppliers to have similar processes for the above questions?
  - Have processes to limit access to critical components? Can the contractor identify everyone that has access to critical components?
- **Are Blind Buys Used to Contract for Critical Function Components?**
- **Are Specific Test Requirements Established for Critical Components?**
- **Does the Developer Require Secure Design and Fabrication or Manufacturing Standards for Critical Components?**
- **Are Critical Program Information (CPI) and Critical Functions stored, maintained, transported, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, modem) securely?**

The second set of sample Yes / No questions apply to software/ firmware assurance considerations.

- **Does the Developer have:**
  - A design and code inspection process that requires specific secure design and coding standards as part of the inspection criteria?
  - Secure design and coding standards that consider Common Weakness Enumeration (CWE), Software Engineering Institute (SEI) *Top 10* secure coding practices, and other sources when defining the standards?
  - From Common Weakness Enumeration (CWE)
  - Common Vulnerabilities and Exposures (Common Vulnerabilities and Exposures (CVE)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
- **Have software vulnerabilities derived from these three sources been mitigated?**
  - From Common Weakness Enumeration (CWE)

    - Common Vulnerabilities and Exposures (Common Vulnerabilities and Exposures (CVE))
    - Common Attack Pattern Enumeration and Classification (CAPEC)
- **Are static analysis tools used to identify and mitigate vulnerabilities?**
- **Does the software contain Fault Detection/Fault Isolation (FDFI) and tracking or logging of faults?**
- **Do the software interfaces contain input checking and validation?**
- **Is access to the development environment controlled with limited authorities and does it enable tracing all code changes to specific individuals?**
- **Are specific code test-coverage metrics used to ensure adequate testing?**
- **Are regression tests routinely run following changes to code?**

No responses to the questions provide points where a countermeasure may be considered for risk mitigation. A simple way of translating the No responses into a risk likelihood is to map the percentage of No responses to a risk likelihood, such as is shown in Table 13.6.T1 .

Table 13.6.T1 Sample Risk Likelihood Mapping

Number of No Responses	Risk Likelihood
All NO	Near Certainty (VH)
>=75% NO	High Likelihood (H)
>= 25% No	Likely (M)
<= 25% No	Low Likelihood (L)
<= 10% No	Not Likely (NL)

Table 13.6.T2 provides an example of a table that summarizes the vulnerability and threat assessment results used to develop the risk likelihood. A table similar to this is beneficial to the program in understanding the rationale and should be documented in the Risk section of the Program Protection Plan (PPP). The overall likelihood is derived from the supply chain risk likelihood, the software assurance risk likelihood and the threat assessment. The Overall Risk Likelihood may be derived by using a weighted average of the three inputs or using the highest risk. In the example shown in Table 13.6.T2 , the overall risk likelihood of High was derived by applying equal weights for the Supply Chain and Software Assurance Risk Likelihood and the Threat Assessment Risk. The program or service may develop their own specific weightings based upon their program and domain specific knowledge.

Table 13.6.T2 Risk Likelihood Derived From Vulnerability and Threat Assessments

Critical Function Component	Mission Impact	Supply Chain Risk Likelihood	Software Assurance Risk Likelihood	Threat Assessment Risk	Overall Risk Likelihood
Component 1	I	High - No blind buys - No Supply Chain visibility - No supplier qualification process - No receiving verification - No trusted suppliers	Very High - No fault logging - No secure design standard - No static analysis - No Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC) - No input validation - No dev envir ctrl - No Regression test - Low test coverage	Medium	High
Component 2	II	Low - No Supply Chain visibility - No supplier qualification	Not Likely	Medium	Low

The No responses to the questions help to determine the possible countermeasures to be considered for risk mitigation. A similar table may be created which records the countermeasures planned and the new risk probability as a result of the planned mitigations. Table 13.6.T3 provides an example worksheet for planning the countermeasures and the resulting Risk Likelihood.

Table 13.6.T3. Risk Likelihood After Mitigations

Critical Function Component	Mission Impact	Supply chain mitigations	Software assurance mitigations	Threat assessment risk	Overall Risk Likelihood
Component 1	I	- Blind buys - Supply Chain (SC) visibility included in Statement of Work (SOW) - Supplier verification and test of Commercial off-the-shelf (COTS) - Requirement to flow down Statement of Work (SOW) requirements to sub-tier suppliers	- Secure design and coding std included in SOW - Fault logging added - Static analysis added - Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC) used to establish and update secure design standards - Input validation added to interfaces - Development environment control added to limit access and record all access - Regression testing added - Test coverage increased to 60% - Penetration testing added	Medium	Low to Medium

The risk is then incorporated into the program technical risks. The risk entry may look similar to the following example:

Software Assurance Technical Risks		Mitigation Activities
R1. Field-programmable gate array (FPGA) 123 has high exposure to software vulnerabilities with potential foreign influence		Establishing a wrapper to implement secure design standards and fault logging, static analysis, increased test coverage, and penetration testing
Technical Issues		
1. May impact performance, cost, and schedule		
Opportunities		
O1. Low investment, great benefit for program and overall for Missile Programs		Low cost, benefit for program and command

Ensure that the top program protection risks (very high and high) have a risk cube and mitigation plans.

13.7. Countermeasures

13.7.1. Anti-Tamper

13.7.1.1. Critical Technologies (CT)

13.7.1.2. Anti-Tamper Considerations

13.7.1.3. Anti-Tamper Execution

13.7.1.3.1. Process

13.7.1.3.2. Sustainment

13.7.1.3.3. Packaging

13.7.1.4. Anti-Tamper Disclosure Guidelines

13.7.1.5. DoD Anti-Tamper Executive Agent (ATEA) Office

13.7.1.6. Anti-Tamper Verification and Validation (V&V)

13.7.1.7. Anti-Tamper and Verification and Validation (V&V) Plan Approval

13.7.2. Information Assurance (IA)

13.7.2.1. Critical Program Information (CPI) in DoD Information Systems

13.7. Countermeasures

This section describes the guidance and expectations for Program Protection countermeasures. Countermeasures are cost-effective activities and attributes to manage risks to Critical Program Information (CPI) and critical functions and components. They vary from process activities (e.g., using a blind buying strategy to obscure end use of a critical component) to design attributes (e.g., Anti-Tamper design

to defeat Critical Program Information (CPI) reverse engineering attempts) and should be selected to mitigate a particular threat. For each countermeasure being implemented, the program should identify someone responsible for its execution and a time- or event-phased plan for implementation.

Many countermeasures may have to be partially or completely implemented by prime and subcontractors on the program. See Section 13.13 for guidance on contracting for the implementation of Program Protection.

13.7.1. Anti-Tamper

Anti-Tamper (AT) is the Systems Engineering activities intended to deter and/or delay exploitation of critical technologies in U.S. defense systems in order to impede countermeasure development, unintended technology transfer, or alteration of a system. (DoDI 5200.39) Properly fielded Anti-Tamper (AT) should:

- Deter countermeasure development that would decrease U.S. warfighting capabilities
- Prevent the unauthorized or out of baseline augmentation or change of capabilities in Direct Commercial Sales (DCS), Foreign Military Sales (FMS), and International Cooperative Development Programs
- Prevent unauthorized technology changes on Critical Program Information (CPI) or any released capability
- Protect U.S. critical design knowledge and manufacturing processes from unauthorized transfer
- Protect U.S. investment in weapon system capabilities, and avoid additional unplanned investment to regain the U.S. advantage

13.7.1.1. Critical Technologies (CT)

A subset of Critical Program Information (CPI) that specifically resides within a weapon system, training or its support equipment, must be considered for protection by Anti-Tamper (AT) techniques to delay or prevent Reverse Engineering (RE). Critical Technologies can be found in: System hardware, embedded software, application software, and data. Critical Technologies should not be confused or associated with Critical Technology Elements (CTE), in other words, Critical Technologies (CTs) as it apply to Anti-Tamper (AT) is not a matter of maturity or integration level.

13.7.1.2. Anti-Tamper Considerations

Anti-Tamper (AT) is more cost effective when implemented at program onset. Therefore, Anti-Tamper (AT) considerations and techniques should be initiated prior to MS A, during program development, preferably in the program material solution analysis phases:

- The PM should include both Anti-Tamper (AT) requirements and costs in

capability development, acquisition and Planning, Programming, Budgeting and Execution (PPBE) process planning cycles.

- Anti-Tamper (AT) requirements may affect other aspects of a program, such as associated maintenance and training devices, and should include end item assessment of cost, schedule and performance if not considered at program onset.
- Anti-Tamper (AT) requirements should be included (but not limited to) in the following documents; Request for Proposal (RFP), SOO, Statement of Work (SOW), Initial Capabilities Document (ICD), Capability Production Documents (CPD), Capability Development Documents (CPD), Acquisition Strategy (AS), Work Breakdown Structure (WBS), Test and Evaluation Master Plan (TEMP) , Information Assurance Strategy (IAS), Systems Engineering Plan (SEP) , and Systems Engineering Management Plan (SEMP) should be included in the DoD Acquisition systems review process (i.e., Systems Engineering Technical Reviews (SETRs)). Refer to DoD Anti-Tamper (AT) Desk Reference for sample language and further guidance.
- Anti-Tamper (AT) is also applicable to DoD systems during Pre-Planned Product Improvement (P^3I) upgrades as new Critical Technologies (CT) may be added to the system. Additionally, Anti-Tamper (AT) should be specifically addressed in export sales (direct commercial sales, foreign military sales) and international cooperative programs if those systems have Critical Technologies (CT) to protect.
- Anti-Tamper (AT) also involves risk management. The level of Anti-Tamper (AT) should be based on the risk of the loss of U.S. control on the asset containing Critical Program Information (CPI) (level of exposure) and the operational impact (criticality and consequence) if the Critical Program Information (CPI) is lost or compromised. Refer to DoD Anti-Tamper (AT) Guidelines for further guidance.

13.7.1.3. Anti-Tamper Execution

The DoD Anti-Tamper Executive Agent (ATEA) provides support to the PM by helping to determine whether or not to implement Anti-Tamper (AT), per DODI 5200.39. The decision to use or not to use Anti-Tamper (AT) will be documented in a classified annex to the Program Protection Plan (PPP), referred to as the Anti-Tamper (AT) Plan. The Anti-Tamper (AT) Plan includes, but is not limited to, the following information:

- The Program Manager (PM) recommendation and the Milestone Decision Authority (MDA) decision on Anti-Tamper (AT);
- Identification of the Critical Technology (CT) being protected and a description of its criticality to system performance;
- Foreign Teaming and foreign countries / companies participating;
- Threat assessment and countermeasure attack tree;
- Anti-Tamper (AT) system level techniques and subsystem Anti-Tamper (AT) techniques investigated;
- System maintenance plan with respect to Anti-Tamper (AT);
- Recommended Anti-Tamper (AT) solution set to include system, subsystem and

component level;
- Determination of how long Anti-Tamper (AT) is intended to delay hostile, or foreign exploitation or reverse-engineering efforts;
- The effect that compromise would have on the acquisition program if Anti-Tamper (AT) were not implemented;
- The estimated time and cost required for system or component redesign if a compromise occurs and;
- Key Management Plan.

13.7.1.3.1. Process

The Anti-Tamper (AT) Process consists of fifteen steps:

1. Identify critical program information
2. Refine results from Step 1 to determine Critical Technologies (CT)
3. Evaluate Critical Technologies (Critical Technologies (CT)) exposure level
4. Evaluate criticality and consequence of compromise of Critical Technologies (CT)
5. Identify Anti-Tamper (AT) protection level requirements
6. Identify potential Anti-Tamper (AT) solution sets considered
7. Describe Critical Program Information (CPI)/Critical Technologies (CT) engineering solution analysis
8. Select initial architecture technique(s) and solution set(s)
9. Identify Anti-Tamper (AT) requirements in the System Functional Baseline
10. Develop Anti-Tamper (AT) architecture
11. Identify Anti-Tamper (AT) implementations in allocated baseline
12. Finalize Anti-Tamper (AT) architecture
13. Implement Anti-Tamper (AT) Architecture and identify residual vulnerabilities
14. Fabricate system and Test (Verification &Validation)
15. Verification and Validation (V&V) results published 60 days prior to deployment

(Consult the DoD Anti-Tamper (AT) Desk reference for further guidance.)

Note: It is highly recommended that the program contact the Component Anti-Tamper (AT) Office of Primary Responsibility (OPR) to obtain a name of a Verification and Validation (V&V) lead. This Verification and Validation (V&V) lead and his team will follow the progress of the Anti-Tamper (AT) Plan implementation and provide consultation. This Verification and Validation (V&V) lead will also determine if the Anti-Tamper (AT) Plan meets the protection level and provide whether the Component Anti-Tamper (AT) Office of Primary Responsibility (OPR) should concur/non-concur with the Anti-Tamper (AT) Plan. This Verification and Validation (V&V) lead will also be the witness to the actual testing of the Anti-Tamper (AT) Plan and provide a memo back to the program as to whether it did complete the Anti-Tamper (AT) testing. The Verification and Validation (V&V) lead and team will be provided to the program at no cost but only as consultants. They will not develop the Anti-Tamper (AT) Plan. That is for the program office/contractor.

13.7.1.3.2. Sustainment

Anti-Tamper (AT) is not limited to development and fielding of a system. It is equally important during life-cycle management of the system, particularly during maintenance. Maintenance instructions and technical orders should clearly indicate the level at which maintenance is authorized; and include warnings that damage may occur if improper or unauthorized maintenance is attempted.

To protect Critical Technologies (CT) during maintenance, it may be necessary, as prescribed by the Delegation of Disclosure Authority Letter, to limit the level and extent of maintenance an export customer may perform. This may mean that maintenance involving the Anti-Tamper (AT) measures will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions may be no different than those imposed on U.S. Government users of Anti-Tamper (AT) protected systems. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents should state such maintenance and logistics restrictions. The contract terms and conditions should establish that unauthorized maintenance or other unauthorized activities:

- Should be regarded as hostile attempts to exploit or reverse engineer the weapon system or the Anti-Tamper (AT) measure itself; and
- Should void the warranty or performance guarantee.

Note: The U.S. Government and U.S. industry should be protected against warranty and performance claims in the event Anti-Tamper (AT) measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities are regarded as hostile attempts to exploit or reverse engineer the system or the Anti-Tamper (AT) measures.

Note: Programs should also plan and budget for Anti-Tamper (AT) maintenance to include government/contractor investigations of tamper events.

13.7.1.3.3. Packaging

Anti-Tamper (AT) affected equipment may need specially designed and approved shipping containers ready upon delivery. The containers should provide the same level of protection from exploitation as the protected Critical Technologies (CT) within the container while in the supply chain or have the Anti-Tamper (AT) equipment active while shipping.

13.7.1.4. Anti-Tamper Disclosure Guidelines

Anti-Tamper (AT) processes and techniques cannot be discussed or revealed to non-U.S. or unauthorized U.S. persons:

- The fact that Anti-Tamper (AT) has been implemented on a specific system is

classified as Unclassified/FOUO (For Official Use Only) unless otherwise directed (e.g. specific direction requiring system Anti-Tamper (AT) be handled at a higher classification level, system security classifying system Anti-Tamper (AT) higher)
- The fact that Anti-Tamper (AT) has been implemented on a specific sub-system or even a component of a sub-system is classified SECRET. Refer to the DoD Anti-Tamper (AT) Security Classification Guide (SCG) for further clarification.

13.7.1.5. DoD Anti-Tamper Executive Agent (ATEA) Office

The DoD Anti-Tamper Executive Agent (ATEA) is responsible for all Anti-Tamper (AT) policy consistent with the DoDI 5000.02 and DoDI 5200.39 . The office has established a network of DoD Component Anti-Tamper (AT) points of contacts (POCs) to assist program managers in responding to Anti-Tamper (AT) technology and/or implementation questions. Additionally, the Acquisition Security Database (ASDB) has been developed as a common shared database of Anti-Tamper (AT) related information.

13.7.1.6. Anti-Tamper Verification and Validation (V&V)

Anti-Tamper (AT) implementation is tested and verified during developmental test and evaluation and operational test and evaluation.

The PM develops the validation plan and provides the necessary funding for the Anti-Tamper (AT) Verification and Validation (V&V) on actual or representative system components. The Verification and Validation (V&V) plan, which is developed to support Milestone C, is reviewed and approved by the DoD Anti-Tamper (AT) Executive Agent , or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR), prior to milestone decision. The program office conducts the Verification and Validation (V&V) of the implemented Anti-Tamper (AT) plan. The Anti-Tamper (AT) Verification and Validation (V&V) team witnesses these activities and verifies that the Anti-Tamper (AT) techniques described in the Anti-Tamper (AT) Plan are implemented into the system and performs according to the Anti-Tamper (AT) plan. The validation results are reported to the Milestone Decision Authority.

13.7.1.7. Anti-Tamper and Verification and Validation (V&V) Plan Approval

The DoD Anti-Tamper Executive Agent (ATEA) has published a DoD Anti-Tamper (AT) and Verification and Validation (V&V) Plan Templates to assist program managers and contractors with the required content for approval. The latest Templates can be downloaded by registered users at https://www.at.dod.mil/ .

There is a two-step approval process for all Anti-Tamper (AT) plans:

Domestic cases:

The Anti-Tamper (AT) Plans (Initial and Final) are to be created by the government or government contractor and approved first by the program manager. Then, they are submitted to the Component Anti-Tamper (AT) Office of Primary Responsibility (OPR) 60 days prior to PDR for initial plans and 60 days prior to Critical Design Review (CDR) for final Anti-Tamper (AT) Plans. The same approval timeline holds true for the verification and validation plans (Initial and Final) if separated from the Anti-Tamper (AT) Plan.

After the program manager has approved the Anti-Tamper (AT) Plan, the Anti-Tamper (AT) Executive Agent or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR), provides an evaluation of the Anti-Tamper (AT) Plan and a letter of concurrence to the program office and Milestone Decision Authority.

Export cases:

1. An Initial Anti-Tamper (AT) Plan MUST be submitted to the DoD Anti-Tamper Executive Agent (ATEA) (or designee) NLT 60 days prior to submission of a Letter of Offer and Acceptance (LOA) or contract signature, whichever comes first. Written DoD Anti-Tamper Executive Agent (ATEA) (or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR)) approval of the Initial Anti-Tamper (AT) Plan must be obtained prior to release of the Letter of Agreement (LOA) or contract signature. As a minimum, the plan should include:
    a. A description of the architecture
    b. The Critical Program Information (CPI) and proviso limit's requiring protection
    c. Level of Anti-Tamper (AT) required for each Critical Program Information (CPI) (1-5)
    d. Top-level solution w/core Anti-Tamper (AT) technology being implemented
    e. Penalty/Response initial thoughts
    f. Support and tamper event reporting concept
    g. Cost and Schedule Rough Order of Magnitude (ROM) for Anti-Tamper (AT) implementation
    h. Risk to implementation
2. An update to the Initial Anti-Tamper (AT) Plan must be provided to the DoD Anti-Tamper Executive Agent (ATEA) (or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR)) within 60 days after contract award.
3. A Final Anti-Tamper (AT) Plan must be submitted to the DoD Anti-Tamper Executive Agent (ATEA) (or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR)) NLT 60 days prior to Critical Design Review (CDR). Written DoD Anti-Tamper Executive Agent (ATEA) (or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR)) approval of the Final Anti-Tamper (AT) Plan must be obtained prior to Critical Design Review (CDR) closure.
4. Verification and Validation (V&V) testing must be completed NLT 60 days prior to system export. Written DoD Anti-Tamper Executive Agent (ATEA) (or Component Anti-Tamper (AT) Office of Primary Responsibility (OPR)) concurrence of satisfactory Verification and Validation (V&V) completion must be

obtained prior to system export.

13.7.2. Information Assurance (IA)

Information Assurance (IA) is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

All mission critical functions and components, and information systems storing, processing, or transmitting Critical Program Information (CPI) must be appropriately protected, regardless of whether the information systems are owned and controlled by the Department of Defense or by external entities. Programs with identified Critical Program Information (CPI) need to ensure that the Critical Program Information (CPI) is protected in every computing environment that hosts it, or over which it is transmitted. With the requirement to identify system critical functions and associated components, Information Assurance (IA) needs to determine the Information Assurance (IA) controls needed for their protection. (See Chapter 7 for further details on Information Assurance (IA) Implementation.)

13.7.2.1. Critical Program Information (CPI) in DoD Information Systems

DoDD 8500.01E and DoDI 8500.2 detail the policy, process, and procedures for implementing appropriate Information Assurance (IA) into DoD information systems. They mandate a controls-based approach, which considers a systems assigned Mission Assurance Category (MAC) and Confidentiality Level (CL) in determining the required robustness of Information Assurance (IA) controls to be implemented. DoD information systems with Critical Program Information (CPI) must be accredited in accordance with DoDI 8510.01 (DIACAP). The DoD Information Assurance Certification and Accreditation Process (DIACAP) establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit information systems throughout the system lifecycle. The DoD Information Assurance Certification and Accreditation Process (DIACAP) provides an independent validation process that verifies that appropriate protection measures have been implemented, tested, and maintained, and that any residual risk is at an acceptable level for system operation.

It is important to differentiate between the implementation of Information Assurance (IA) in program support information systems (U.S. Government or contractor) for the protection of Critical Program Information (CPI) as opposed to the implementation of Information Assurance (IA) in the system being acquired. For example, an acquisition program office acquiring a new weapons system may utilize a DoD information system that hosts Critical Program Information (CPI). Similarly, that same program may have Critical Program Information (CPI) being processed or transmitted on the prime contractor or systems integrators design, development, or support systems. The Information Assurance (IA) requirements and certification and accreditation process for each of these support systems are totally separate and distinct from those of the

weapons system being acquired, which may also contain Critical Program Information (CPI).

In practice, the implementation of Information Assurance (IA) to protect Critical Program Information (CPI) is no different from the implementation to protect any other information type. DoD information systems with Critical Program Information (CPI) must have both a Mission Assurance Category (MAC) and Confidentiality Level (CL) designated in accordance with DoDD 8500.01E. The presence of Critical Program Information (CPI) may be a factor in the Confidentiality Level (CL) assigned (public, sensitive, or classified), if the Critical Program Information (CPI) sensitivity drives the assignment to a higher level.

13.7.2.2. Critical Program Information (CPI) in Other Than DoD Information Systems

As previously noted, adequate security must be provided to all Critical Program Information (CPI) released to or developed by and in the possession of offeror's, DoD contractors, grantees, or other sharing partners, to include when it is stored or processed on information systems and networks that are not owned by or operated on behalf of the Department. This may be a very diverse group, and may include prime and subcontractors, system integrators, program management support contractors, Federally Funded Research and Development Centers (FFRDC), and independent test organizations. Critical Program Information (CPI) that is classified must be protected in contractor facilities with Defense Security Service (DSS) accredited information systems in accordance with the National Industrial Security Program Operating Manual (NISPOM). Unclassified Critical Program Information (CPI) that resides on unclassified non-DoD systems must be protected in accordance with Directive-Type Memorandum (DTM) 08-027, Security of Unclassified DoD Information on Non-DoD Information Systems. These requirements should be incorporated as clauses in contracts or change orders, or as appropriate language in sharing agreements and grants.

13.7.2.3. Indicators of Achieving Baseline Information Assurance (IA) Protection of Critical Program Information (CPI)

For DoD information systems containing Critical Program Information (CPI):

- Confidentiality Level (CL) appropriate to the Critical Program Information (CPI) sensitivity and/or classification, and applicable baseline Information Assurance (IA) controls is implemented.
- Authorization to Operate (ATO) or Interim Authorization to Operate (IATO) issued by the hosting systems designated accrediting authority (DAA) is current.
- Information Technology (IT) security plan of action and milestones (POA&M) does not identify any security weaknesses impacting Critical Program Information (CPI) that are not sufficiently mitigated; Information Technology (IT) security plan of action and milestones (POA&M) indicates appropriate level of follow-up actions.

- Inventory of Critical Program Information (CPI) (item, site, system hosting, and Information Assurance (IA) Point of Contact (POC)) is complete.
- Any supplemental Information Assurance (IA) controls specified to protect Critical Program Information (CPI) are incorporated into the DoD Information Assurance Certification and Accreditation Process (DIACAP) implementation plan or equivalent security requirements traceability matrix.

For non-DoD information systems containing Critical Program Information (CPI):

- Required Information Assurance (IA) protection measures are negotiated and agreed to in contract or sharing agreement. Protection requirements flow down through prime to subcontractors, as appropriate.
- For DoD contractor systems accredited under the National Industrial Security Program Operating Manual (NISPOM), accreditation decision issued by the Defense Security Service (DSS) Designated Approving Authority (DAA) is current.
- Reports of Information Assurance (IA) protection self-assessments are submitted to the program office periodically. Reports include appropriate levels of follow-up activity to clear discrepancies. Defense Security Service (DSS) will notify the Government Contracting Agency (GCA) of security compromises or serious security violations involving such systems and of a marginal or unsatisfactory security review rating for the facility.
- Inventory of Critical Program Information (CPI) (item, site, system hosting, and Information Assurance (IA) Point of Contact (POC)) is complete.

The details of the programs Information Assurance (IA) approach to protecting all Critical Program Information (CPI) and system critical functions and components should be documented in the Countermeasures subsections of the Program Protection Plan (PPP), and should address the content of Sections 13.7.2.1 and 13.7.2.2 , as applicable.

13.7.3. Software Assurance

The extensive use of Commercial off-the-shelf (COTS), Government off-the-shelf (GOTS), open source, and other off the shelf software as well as developmental software in DoD systems necessitates early planning for and design of software security protections that address the threats to those systems and the types of attacks those threats can orchestrate against the systems. Systems must be securely supplied, designed and tested to assure mission success as well as the protection of critical functions, associated components, and Critical Program Information (CPI). Of particular interest are the protection and assurance activities that are undertaken during the COTS integration and development processes, those aimed at mitigating attacks against the operational system (the fielded system), and those that address threats to the development environment. The purpose of this section is to develop a plan and statement of requirements for software assurance early in the acquisition lifecycle and incorporate the requirements into the request for proposal (RFP). Then use that plan to

track software assurance protections throughout the acquisition. The progress toward achieving the plan is measured by actual accomplishments/results that are reported at each of the Systems Engineering Technical Reviews (SETRs) and recorded as part of the Program Protection Plan.

The Program Protection Plan (PPP) Outline and Guidance requires acquisition programs to address software assurance responsibilities for the planning and implementation of program protection countermeasures. Such countermeasures address the anticipated attacks a system may experience from the threats it will face by eliminating or reducing vulnerabilities. The countermeasures are selected with an understanding of which parts of the software are the most critical to the success of the mission. The plan includes a sample Software Assurance Countermeasures Table, which summarizes the planned and current state of a programs software assurance activities. The table is also used as part of a vulnerability assessment to identify operational, developmental, design, COTS and software tool vulnerabilities that that can be addressed by planning and implementing software assurance countermeasures.

The table in the PPP is divided into 3 sections that provide different vulnerability and countermeasure perspectives on software assurance plans and implementation:

- Development Process assurance activities conducted during the development process to mitigate and minimize attacks (e.g., threat assessment and modeling, attack surface analysis, architecture and design reviews, application of static and dynamic code assessment tools and services, penetration testing, and red teaming) that the developed system is likely to face when deployed into operation
- Operational System attack countermeasures and other assurance activities applied within the operational environment (e.g., failover, fault isolation, encryption, application firewalls, least privilege, and secure exception handling) to mitigate attacks against the delivered system and software interfaces, which may include COTS, GOTS, open source, and other off the shelf software
- Development Environment assurance activities and controls (e.g., access controls, configuration management, and release testing) applied to tools and activities (e.g., compilers, linkers, integrated development environments, run-time libraries, and test harnesses) used to develop and sustain software to mitigate attacks

Given the constraints of cost, schedule, and performance, fully comprehensive assessment and testing is often not feasible. Thus SwA planning should reflect priorities chosen to mitigate risk and deliver mission capability with acceptable levels of assurance. The coding language, source of code (i.e. custom, COTS, GOTS, open source), platform (i.e. web based, mobile, embedded, etc.) as well as the results of criticality analysis (see 13.3.2.1) will be used to prioritize software assurance activities when planning for SwA.

13.7.3.1. Development Process

The purpose of this section of the table is to measure and explicitly capture the assurance activities conducted during software development and the integration of off-the-shelf components. As appropriate to the risk of compromise and criticality of the software in question, PMs are to analyze the development activities for:

- potential introduction of vulnerabilities and risks based on the anticipated threat and the attacks the threats are capable of making against the system;
- development of a plan for the assurance process as well as the technical disciplines and knowledge needed for Integrated Project Teams (IPTs);
- how IPTs address the architecture, design, code, and implementation choices to include the appropriate mitigations necessary to address the anticipated attacks and assure the critical function software components; and
- review points to track/assess the progress at the milestones in the Program Protection Plan.

Not all software will require the same level of software assurance activities and mitigation planning and implementation in programs with millions of lines of code, there may be some functions (perhaps a monthly reporting feature) that are less mission-critical than other (perhaps a satellite station-keeping module). It may also be difficult to perform some types of assessment and mitigation activities on COTS software for which the source code is not available. Note that in such cases software related risks still exists and may be unmitigated. The software assurance table in the PPP recognizes these varying types of software and allows for differing plans/implementation of assurance as needed.

13.7.3.1.1 Static Analysis

Programs should investigate the applicability of automated static analysis tools to review source and/or binary copies of their software and, where advantageous, apply both static source code and static binary analysis to assist in identifying latent weaknesses that would manifest as operational system vulnerabilities and allow attackers to interfere, manipulate, or otherwise suborn the systems mission capabilities. The use of these types of tools within the development activity (i.e., as an add-on to the developers Integrated Development Environment (IDE)) as well as in the Independent Test and Evaluation (IT&E) activities are both valuable and useful. Approaches that integrate such forms of continuous assessment into the developers activities should be emphasized and encouraged.

13.7.3.1.2 Design Inspection

The establishment and update of secure design and code standards by the program should address the potential types of attacks the system would face and draw upon DoD, Government, Federally Funded Research and Development Centers (FFRDC), academia, commercial web sites and industry sources for mitigation approaches and

methods to address those that could impact the systems mission capabilities. The list of attack patterns captured in the Common Attack Pattern Enumeration and Classification (CAPEC) collection can be used to help consistently analyze a system for potential types of attacks they may face and to bring consistency into the validation activities when the program is verifying that the design and coding standards are being followed.

13.7.3.1.3 Code Inspection

Due to the subtle nature of most weaknesses in code that lead to unreliable, insecure, and brittle applications that are easily influenced by attackers it is important that code inspections utilizing tools be part of the approach used to minimize these weaknesses. There are over 700 documented types of weaknesses in code, design, architecture, and implementation captured in the Common Weakness Enumeration (CWE) catalog but not all of them are equal threats to any specific application or system. Programs may wish to draw upon secure design and coding approaches defined on websites such as top 10 secure coding practices (https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices) and the Common Weakness Enumeration (CWE)/ SysAdmin, Audit, Network, Security (SANS) top 25 most dangerous software errors (http://cwe.mitre.org/top25/index.html) to establish and update their secure design and coding standards. As a minimum the code inspection is used to inspect for conformance to the secure design and coding standards established for the program.

An important part of the code inspection is to identify the subset of the overall CWE collection to focus on initially. Alternate approaches to focusing in on a subset of the weaknesses are described in the CWE paragraph below (13.7.3.1.6.) and the CAPEC paragraph (13.7.3.1.5.) . These approaches can be used independently or in combination if desired.

Because of the dynamic nature of the threat environment and information about how systems can be compromised through software weaknesses, the program should have a methodology to periodically update their secure design and coding standards so that reviews using them address new types of attacks and types of weaknesses.

The next three sections of this document describe the middle three columns of the PPP Software Assurance Table, which are meant to capture how the established vulnerability (CVE), weakness (CWE), and attack pattern (CAPEC) collections are being used by the project team to identify and mitigate the most dangerous types of vulnerabilities in the software. These columns are further defined below but the most critical part of completing these three columns is the analysis of which CVEs, CWEs, and CAPECs should be used as the denominator of these percentage calculations and the documentation within the project team of the rationale and methodology followed in determining those lists and keeping them current throughout the project as the system design, development and testing progresses and the threat environment and other factors change.

13.7.3.1.4. Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) information is used to identify, track, and coordinate mitigation activities of the publicly known vulnerabilities in commercial (COTS) and open source software which are often used by threats actors/agents to attack systems. Programs that incorporate COTS software into their systems should perform regular searches of the CVE lists before purchase and throughout the software lifecycle to understand vulnerabilities in those COTS software components and assess potential threat to mission success.

The CVE list is a compilation of publicly known information about security vulnerabilities and exposures. The list is international in scope, free for public use, and referenced in most commercial tools that scan operational systems and networks for vulnerabilities. The CVE list can be used to identify publicly known software vulnerabilities that could:

- Allow an attacker to execute unauthorized code or commands;
- Allow an attacker to gain privileges or assume identities;
- Allow an attacker to access and/or manipulate data that is contrary to the specified access restrictions for that data;
- Bypass protection mechanisms:
- Allow an attacker to hide their activities; and
- Allow an attacker to conduct denial of service attacks.

CVE is intended for use by security experts, so it assumes a certain level of knowledge. Programs should use a tool during incremental software testing of their commercial and open source packages that scans those operational components and matches the results with the CVE dictionary. Alternately, a scan of the affected software packages on the CVE list can be used to review the list for any publicly known vulnerabilities for the software packages being used by a DoD program. A list of CVE compatible tools is available at http://cve.mitre.org/compatible/product.html .

The CVE column in the Program Protection Plan Software Assurance table reports the planned and actual percentages of software components that incorporate COTS or open source that have been analyzed and acceptably remediated against the CVEs from the CVE list that apply to those COTS and open source packages.

Supportive analysis by the project team must record the CVEs found, the remediation applied, and the residual risk to the mission of any unresolved CVEs. To identify which CVEs should be included in the analysis the list of CVEs for each COTS product and open source should be tracked and those that were remediated documented as such. For each COTS and open source package utilized as part of the system, the project staff should determine whether an explicit vulnerability advisory/alert activity is provided/offered by the provider/developer of those packages.

For those that do not provide publicly available advisories/alerts about security issues that need to be resolved the project staff should carefully consider the risk they are

inheriting from that developer by not providing patch information in a manner that CVE identifiers can be assigned. Without CVE identifiers it is much harder to track and manage the state of deployed software within the DoD's vulnerability management practice and the automation tooling deployed within the DoD. 100% of developmental Critical Program Information (CPI) software and developmental critical-function software packages, whether COTS or open source, must be evaluated using CVE, to surface exposures inherited by incorporating open source or COTS libraries or products.

Guidance on searching the CVE is located at http://cve.mitre.org/about/faqs.html#c . An important aspect of applying CVE tools and reviews to a collection of COTS and open source is to apply the Common Vulnerability Scoring System (CVSS) to the determination of which CVEs to mitigate first and to understand the severity of the remaining CVEs.

If the selected tool outputs any CVE with a CVSS score above medium (4), programs should mitigate the vulnerability with highest priority first and then work through the next highest priority issue until the residual risk represented by the remaining vulnerabilities is acceptable to the mission owner. CVEs that are included in any DoD Information Assurance Vulnerability Management (IAVM) alerts and advisories should be addressed in accordance to the priorities and timeframe included in the IAVM from DISA.

The CVE web site is at http://cve.mitre.org

13.7.3.1.5. Common Attack Pattern Enumeration and Classification (CAPEC)

Common Attack Pattern Enumeration and Classification (CAPEC) is meant to be used for the analysis of common patterns of attacks against systems, whether for understanding how attacks are done, scoping of relevant threats, templates for malicious testing, or as a foil for thinking about the susceptibility of systems architecture, design, and technical implementation to specific attacks.

CAPEC is international in scope, free for public use, catalog of attack patterns outlining information such as a comprehensive description of the phases and steps in attacks, the weaknesses they are effective against (using CWEs), and a classification taxonomy that can be used for the analysis of common attack patterns. CAPEC attack patterns cover a wide variety of families of attacks including: data leakage attacks, resource depletion attacks, injection attacks, spoofing attacks, time and state attacks, abuse of functionality attacks, attacks using probabilistic techniques, attacks exploiting authentication, attacks exploiting privilege/trust, attacks exploiting data structure, resource manipulation attacks, network reconnaissance, social engineering attacks, as well as some physical security attacks and supply chain attacks.

The attack patterns in CAPEC can be a powerful mechanism to capture and communicate the attacker's perspective, organize the analysis of a system with respect to attacks, and prioritize weaknesses (CWEs) based on the anticipated attack patterns. They are descriptions of common methods for exploiting software. Identified attack

patterns may influence the selection of the COTS and open source software products, programming languages, and design alternatives. By understanding the attackers perspective and how a programs software is likely to be attacked, programs can directly consider these exploit attempt methods and mitigate them with design, architecture, coding and deployment choices that will lead to more secure software.

Programs should identify the set of attack patterns that pose the most significant risk and leverage them at each stage of the Software Development Lifecycle (SDLC). A discussion of how to use CAPEC in this manner is available on the Engineering for Attack page on the CWE site (http://cwe.mitre.org/community/swa/attacks.html). This is the same basic methodology described in the new *ISO/IEC Technical Report 20004, "Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045"* , which describes an alternate approach for doing a vulnerability analysis of a software-based system under the Common Criteria regime. ISO/IEC 15408 and ISO/IEC 18045 are the two standards that guide and describe the Common Criteria evaluation methodology.

Basically that page describes how an analysis using attack patterns to represent the expected threat and identify the subset of weaknesses that are of most concern, can be used to identify which weaknesses those attacks would be effective at exploiting and that list can be used to influence the choices about design and architecture, considering the planned operational use, the creation of security policies, requirements, and thinking through the risks related to the systems intended use. This list of the weaknesses, the ones that are exploitable by the attack patterns the systems adversary are capable of using against the system can be used to identify the subset of relevant CWE weaknesses to avoid and to vet for during implementation. The lists associated CAPECs can be used to guide the software testing by identifying high priority test cases that should be created for risk-based security testing, penetration testing, and red teaming. [1]

The CAPEC column in the Program Protection Plan Software Assurance table reports the planned and actual percentages of developed software components that have been evaluated utilizing the attack patterns from the CAPEC list to identify the appropriate sub-set of CWEs, to consider alternate design and architectures or implementations, or to drive the creation of appropriate misuse and abuse test cases.

Supportive analysis by the project team must record the CAPECs identified as germane to the system, the CWEs identified as being susceptible to those CAPECs and the remediation applied along with an understanding of the residual risk to the mission of any CWEs that weren't tested by simulating CAPECs against the system. To identify which CWEs should be included in the testing analysis based on CAPEC inspired test cases the list of CWEs reviewed for the static analysis tools/services should be tracked and those that were identified, covered by the analysis tool/service and appropriately remediated should be documented as such. For each CWE that was not covered by a static analysis tool/service, the project staff should determine whether an appropriate CAPEC inspired test case or Red Team activity was conducted without finding an

exploitable CWE.

For those CWEs that were not covered by static analysis or testing, the project staff should carefully consider the risk to the mission from the potential of those weaknesses remaining in the system. Without demonstrable evidence that the CWEs that an attacker could exploit are mitigated there will always be some level of risk but it is incumbent on the project staff to document this residual risk for the end user so they can manage that risk when the system is deployed within the DoD. 100% of developmental Critical Program Information (CPI) software and developmental critical-function software should be evaluated against the CAPEC list.

The CAPEC web site is http://capec.mitre.org. A description of the CAPEC schema is located in the Documentation portion of the CAPEC Documents page at http://capec.mitre.org/about/documents.html .

13.7.3.1.6. Common Weakness Enumeration information (CWE)

The Common Weakness Enumeration (CWE) is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses to enable more effective discussion, description, selection, and use of software security tools and services to find weaknesses in source code and operational systems components as well as to better understand and manage software weaknesses related to architecture and design.

CWE is targeted to developers and security practitioners. Programs should use CWE-compatible tools to scan software for CWE. A list of CWE-compatible products is available at http://cwe.mitre.org/compatible/product.html .

The CWE column in the table reports the planned and actual percentages of developed software components that have been evaluated utilizing the weaknesses from the CWE list to identify the appropriate sub-set of CWEs, to consider alternate design and architectures or alternate coding constructs.

Supportive analysis by the project team must record the subset of CWEs identified as being most germane to the secure operation of the system. The subset of CWEs can be taken from the CWE/SANS Top 25 Most Dangerous Software Errors list or by utilizing the Common Weakness Risk Analysis Framework (CWRAF) to identify the subset of CWEs that are the most dangerous to the systems mission given what the software is doing for the mission. CWRAF allows a project team to create their own list of the most dangerous CWEs based on the specifics of their system and which failure modes are the most important to mitigate/prevent.

The CWE/SANS Top 25 Most Dangerous Software Errors list on the CWE and SANS Web sites provides detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding them.

The CWRAF methodology is described on the CWE web site and numerous examples are provided to help a project team learn how to apply the methodology to their system in combination with the Common Weakness Scoring System (CWSS).

By using the Common Weakness Scoring System (CWSS) a program can also reflect their specific list of dangerous CWEs into their tools so the risk to the mission of the weaknesses found during static and dynamic analysis or penetration testing reflects the relative importance of those impacts.

The CWE web site is at http://cwe.mitre.org and the CWSS web page is at http://cwe.mitre.org/cwss/ .

Additionally, the project team should have a documented understanding of the residual risk to the mission of any CWEs that weren't reviewed for by static analysis tools/services or tested by simulating the CAPECs that would be effective against those CWEs. For CWEs deemed to be dangerous but not covered by a static analysis tool/service, the project staff should determine whether an appropriate CAPEC inspired test case or Red Team activity was conducted without finding an exploitable CWE.

For those CWEs that were not covered by static analysis or testing, the project staff should carefully consider the risk to the mission from the potential of those weaknesses remaining in the system. Without demonstrable evidence that the CWEs that an attacker could exploit are mitigated there will always be some level of risk but it is incumbent on the project staff to document this residual risk for the end user so they can manage that risk when the system is deployed within the DoD. 100% of developmental Critical Program Information (CPI) software and developmental critical-function software should be evaluated against the identified subset of the CWE list.

In addition to the above listed MITRE websites, PMs should consider best practices identified at http://www.safecode.org/index.php .

13.7.3.1.7. Penetration Test

Programs should report what portion of the system will undergo penetration testing. The purpose of penetration testing is to subject the system to an attack exercise to raise awareness of exploitable vulnerabilities in the system and accelerate their remediation. Also the knowledge that a system will undergo penetration testing increases the vigilance of the software engineers responsible for architecting, designing, implementing, and fielding the systems.

The text should support the number with brief an explanation of the penetration testing performed and a reference to any supporting reports generated by that testing.

The unit's used for planned/actual percentages for this metric are at the discretion of the program. They should be explained in the text and be meaningful and provide insight into the completeness of the testing. For example a network that exposes a certain

number of protocols may measure the percentages in the space of protocol states. A system with an API may measure the number of interface functions probed.

13.7.3.1.8 Test Coverage

Programs should report on their planned and actual test coverage. Unit's and metrics for test coverage are at the discretion of the program, but should be meaningful and yield insight into the completeness of the testing regimen.

Possible measure for test coverage include percentage of statements exercises, percentages of API calls and exception conditions exercised, number of function points tested.

13.7.3.2. Operational System

This section refers to the software and firmware on the fielded system. Software assurance countermeasures is a rapidly evolving area. Successful assessments, techniques, applications, and example outcomes are frequently published in papers that can be found at DoD, Government, Funded Research and Development Centers (FFRDC), and commercial web sites. The FFRDC Carnegie Mellon Software Engineering Institute (SEI) and MITRE both have searchable libraries containing information about the approaches to Software Assurance indicated in the *Program Protection Plan Outline &* Guidance , Table 5.3.3-1 Application of Software Assurance Countermeasures.

13.7.3.2.1. Failover Multiple Supplier Redundancy

Identical code for a failed function will most likely suffer the same failure as the original. For redundancy in software, therefore, a completely separate implementation of the function is needed. This independence reduces the probability that the failover code will be susceptible to the same problem.

13.7.3.2.2. Fault Isolation

Design principles applied to software to isolate faults, include functions to trap, log, and otherwise protect element failures from affecting other elements and the larger system. Logs help trace the sources of operational faults. Logs can also be examined to determine whether there was a malicious attack.

Programs reporting a Yes in the table should be prepared elaborate with technical detail on how the fault isolation mechanisms were employed in the architecture and design for the particular component or sub-system. Fail over or fault isolation is also where the logging of the failure event and the capture of relevant data needed to determine root cause of the failover event is best included.

13.7.3.2.3. Least Privilege

Design principle applied to software that limits the number, size, and privileges of system elements. Least privilege includes separate user roles, authentication, and limited access to enable all necessary functions but minimize adverse consequences of inappropriate actions.

Programs reporting a Yes in the table should be prepared elaborate with technical detail on how least privilege principles were employed in the architecture and design for the particular component or sub-system.

13.7.3.2.4. System Element Isolation

Design principles applied to software to allow system element functions to operate without interference from other elements.

Programs reporting a Yes in the table should be prepared elaborate with technical detail on how system element isolation principles were employed in the architecture and design for the particular component or sub-system.

13.7.3.2.5. Input Checking/Validation

The degree to which software element inputs are checked and validated according to defined criteria and functionality. Input checking and validation should ensure that out-of-bounds values are handled without causing failures and the invalid input events are logged

Programs reporting a Yes in the table should be prepared to elaborate on the architectural and design criteria governing the extent of input checking/validation employed.

13.7.3.2.6. Software Encryption and Anti-Tamper Techniques (SW load key)

The degree to which executable software code is encrypted or otherwise protected (e.g., by checksums or cyclic redundancy checks) from corruption, between factory delivery and use in a military mission. Defense Acquisition University (DAU) currently teaches an anti-tamper course, which provides some Anti-Tamper (AT) techniques that can be used for software encryption.

Programs reporting a Yes in the table should be prepared to elaborate on specific anti-tamper techniques are included in the architecture, design, and implementation of the software component or sub-system and what risks they are intended to mitigate.

13.7.3.3. Development Environment

Software tools used in the development environment (as opposed to the actual fielded

software) are another source of risk to warfighting capability and should be considered in the Program Protection Plan (PPP). In particular a compromised development environment could be leveraged by an attacker to insert malicious code, exploitable vulnerabilities, and/or software backdoors into the operational software before it is fielded.

Examples of software development tools include:

- Compilers, assemblers, pre-compilers, and other code generating tools such as design templates
- Structured code editors and pretty printers
- Code static analysis tools
- Debugging and timing analysis tools
- Code configuration management tools
- Accounts and access controls on development computers and networks
- Test management tools, test data generators, test harnesses, automated regression testing tools

Examples of compromising tools to achieve malicious insertion include

- Modify compiler to generate or insert additional functionality into the operational code
- Modifying a math library of routines with malware that then gets incorporated into the operational code.

Programs should tailor the list contents of the SW Product column in this section of the table to enumerate the software tools pertinent to the programs development environment(s). For each SW product listed table entries should address the items enumerated in the following columns.

13.7.3.3.1 Source Code Availability

When source code is available, it becomes easier to answer some questions about the behavior of the tool and detect potential compromise.

Is source code available for the tool? A simple yes or no should suffice. If further information (e.g. coding language, code size, licensing cost constraints) would provide useful insight annotate the entry with a note.

13.7.3.3.2. Release Testing

Software tools are often updated. These updates are a potential path for an attacker to compromise the development environment and thus the operational software.

Indicate whether testing for indications of malicious insertion or tool compromise are performed on each update of the tool before that update is incorporated into the

development environment.

13.7.3.3.3. Generated Code Inspection

Indicate whether/how any generated code for the system is examined for malicious code or exploitable vulnerability potentially inserted by the software tool in question.

In general, the problem of how to effectively inspect generated code for malicious insertion remains an open area of research. From the practical standpoint, it is better to perform some inspection than to ignore the problem entirely. That at least raises the bar for what an attacker needs to do compromise the system undetected.

Potential code inspection countermeasures include:

- Manual inspection of a representative sample of the generated code
- Analysis of the code with reverse engineering tools
- Identification of the libraries compiled into an executable
- A sanity check of components output by the tools against components expected
- Comparison to baselines generated by previous versions of the tool.
- Manual inspection of tool outputs against a known/analyzable test corpus.
- Advanced/experimental techniques such as automated function extraction.

Note that in many instances simple sanity checks can be effective in detecting some injected malware. For example: extracting, comparing and sorting strings might point to a trigger string used to open a backdoor. Decompiling an executable may reveal the presence of OP codes not normally generated by the compiler.

Where generated code inspection is deemed of benefit programs should tailor the form of inspection to the unique aspects of the program and report planned and actual percentages appropriately.

13.7.3.3.4. Additional Countermeasures

Programs should consider adding additional columns to this area of the software assurance table with the rationale for the additions if programs judge them to significantly reduce the risk of malicious insertion.

Additional countermeasures may include:

- Access controls and other controls detect malicious behavior or suspicious artifacts in the development environment?
- Information assurance controls to safeguard technical data in the development environment (networks, computers, test equipment, and configuration systems)?

Controlling and accounting for printing of technical manuals and other documentation.

[1] http://capec.mitre.org/documents/An_Introduction_to_Attack_Patterns_as_a_Software_Assurance_Knowledge_Resource.pdf

13.7.4. Supply Chain Risk Management (SCRM)

This section describes how a program can manage supply chain risks to critical program information and critical functions and components with a variety of risk mitigation activities throughout the entire system lifecycle. The Supply Chain Risk Management (SCRM) guidance in this section identifies references that establish a sample of practices for managing supply chain risks. As Supply Chain Risk Management (SCRM) techniques and practices continue to evolve, additional guidance will be published to refine the Departments understanding and implementation of Supply Chain Risk Management (SCRM). There are a variety of existing resources available to aid in the understanding and implementation Supply Chain Risk Management (SCRM). The following is a list that includes, but is not limited to the following foundational documents:

- DTM 09-016 Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems - Establishes authority for implementing Supply Chain Risk Management (SCRM) throughout DoD and for developing initial operating capabilities.
- DoD Supply Chain Risk Management (SCRM) Key Practices and Implementation Guide Provides a set of practices that organizations acquiring goods and services can implement in order to proactively protect the supply chain against exploitation, subversion, or sabotage throughout the acquisition lifecycle.
- National Defense Industrial Association (NDIA) System Assurance Guidebook Provides guidance on how to build assurance into a system throughout its lifecycle, organized around the Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Life Cycle Management Framework.
- DoD Instruction O-5240.24, Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)

13.7.4.1. Scope of Supply Chain Risk Management (SCRM)

Currently, Program Protection Planning Supply Chain Risk Management pertains to Information and Communications Technology (ICT). In the digital age where supply chains are distributed globally, and design, manufacturing and production often occur internationally, supply chains have a greater exposure to threats and exploitation.

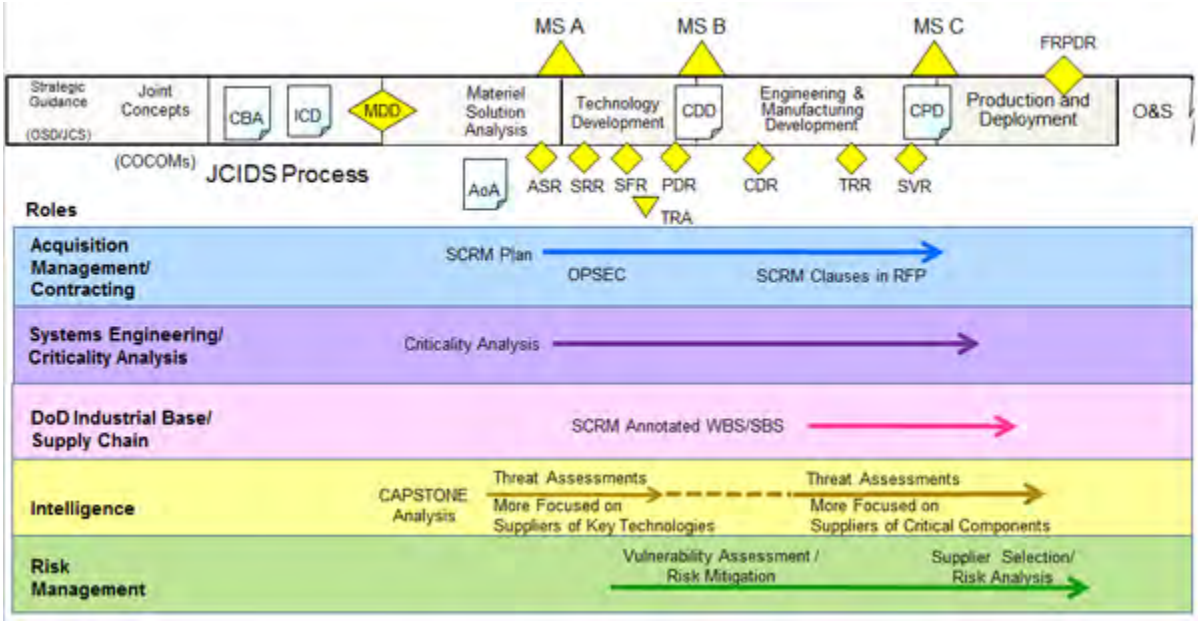
Supply chain risk management provides programs with a framework for analyzing all the risks associated with the supply chain, which enables the determination of what risks may be mitigated, and what risks may be accepted. This determination will vary based on the purpose and mission being performed. Applying Supply Chain Risk Management (SCRM) early in the production lifecycle will allow for earlier mitigations and a more strategic approach for managing risk.

13.7.4.2. Supply Chain Risk Management (SCRM) Throughout the System Lifecycle

The protection of mission-critical systems (including the information technology that compose those systems) must be a priority throughout the entire system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and disposal). This is accomplished through threat awareness and by the identification, management, and potential elimination of vulnerabilities at each phase of the life cycle using complementary, mutually reinforcing strategies to mitigate risk.

Figure 13.7.4.2.F1 illustrates how key Supply Chain Risk Management (SCRM) activities align with the steps in the DoD Acquisition Lifecycle. Activities are organized by the various roles that should perform the indicated functions/procedures. Due to the multidisciplinary nature of Supply Chain Risk Management (SCRM), Program Protection requires careful planning and coordination across multiple stakeholders.

Figure 13.7.4.2.F1. Supply Chain Risk Management (SCRM) Activities throughout the System Lifecycle



Mitigation of supply chain risks is most effective when identification and implementation occur early in a programs acquisition planning and contracting. Generally, mitigation choices narrow and become more expensive the further into the lifecycle they occur. Given the amount of information and supply choices that are present in the marketplace, Operations Security (OPSEC) related to the acquisition process for programs is vital.

13.7.4.2.1. Criticality Analysis

Information on Criticality Analysis can be found in Section 13.3.2.1 .

13.7.4.2.2. Supplier Annotated Work Breakdown Structure (WBS) or System Breakdown Structure (SBS)

A cornerstone for the identification of supply chain risks and the development of supply chain risk management strategies and mitigations for critical components is the criticality analysis. The Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) may be used to annotate the suppliers of the critical components identified by the criticality analysis. A Supplier-Annotated Supply Chain Risk Management (SCRM) Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) is a helpful tool to assist with tracking and managing the supply chain risks. The Supply Chain Risk Management (SCRM) Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) is a detailed breakdown identifying all system assemblies, subassemblies and components and their suppliers for, at a minimum, all critical components identified through criticality analysis. The Supply Chain Risk Management (SCRM) Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) may also include alternative suppliers for all critical components down to the Commercial off-the-shelf (COTS)-item level, with the cost, schedule, and performance impact data for each alternative. Although the Supply Chain Risk Management (SCRM) Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) is not a current requirement, it may be an effective way to record, track and manage the potential suppliers of critical functions as the trade-offs analysis between security, performance, and cost is examined.

The Supply Chain Risk Management (SCRM) System Breakdown Structure (SBS) may provide insight into any teaming arrangements based on an understanding of the defense industrial base and subsequent supply chain. Prior to Milestone B, manufacturers typically develop their supplier lists and enter into teaming agreements. Because of that, programs may consider requiring oversight and input into any supplier teaming arrangements. The program could put controls in place so that supplier lists provide alternatives/alternative suppliers for critical components. Between Preliminary Design Review (PDR) and Critical Design Review (CDR), the Supply Chain Risk Management (SCRM) Work Breakdown Structure (WBS) or System Breakdown Structure (SBS) should be provided by suppliers to the government for review and vulnerability/risk assessment. It is essential that the DoD work with potential Prime Contractors to develop supplier lists and gain insight to potential teaming arrangements. This input is supported by contract clauses such as Consent to Subcontract.

13.7.4.2.3. Securing the Supply Chain Through Maintaining Control Over the Information and Information Flow

OPSEC

Sensitive information must be protected from suppliers and potential suppliers. Operations Security (OPSEC) and appropriate classification guides should be employed to protect system supply chain, design, test and other information from potential adversaries. This includes limiting the sharing of information with suppliers and potential suppliers at multiple tiers sufficient to manage risk. Confidentiality of key information (such as user identities, element uses, suppliers, and their processes, requirements, design, testing, etc.) must be protected when critical to mission success.

Provenance

It is important to establish and maintain the origin, development, delivery path, and mechanisms to protect the integrity of critical components, tools, and processes, as well as their associated changes, throughout the lifecycle. This enables accurate supply chain (SC) risk assessment and mitigation, which requires accurate information on the origin of components, how they are developed, how they are delivered throughout the supply chain. This includes strong system and component configuration management to ensure traceability against unauthorized changes. Selecting suppliers who maintain provenance is the first step to reducing supply chain (SC) risks.

13.7.4.2.4. Design and Engineering Protections

Once critical functions and components have been identified, design and engineering protections can be employed to reduce the attack surface and reduce what is considered critical. These protections should further protect intrinsically critical functions and reduce existing unmediated access to them.

System elements may still have unintentional or intentional vulnerabilities (whether in isolation or when combined) even if they all come from trustworthy suppliers. Defensive Design helps reduce the attack surface and limit the exposure of vulnerabilities. Defensive approaches reduce opportunities to expose or access an element, process, system, or information and to minimize adverse consequences of such exposure or access. In particular, defensive design should be used to protect critical elements and functions by reducing unnecessary or unmediated access within system design.

13.7.4.2.5. Supply Alternatives

Application-specific integrated circuits (ASICs) should be acquired from a trusted supplier because if they are compromised, then unique DoD designs could be exposed and critical system information could become available to adversaries. For information

on trusted suppliers of microelectronics, please refer to Sect ion 13.7.5 .

13.7.4.2.6. Procurement Authorities

Procurement language has been developed and is available for use to help mitigate supply chain risk through contractual requirements in the Statement of Work (SOW). Refer to Section 13.13.1.2 below for suggested language.

Supplier Security Practices

Organizations can help mitigate supply chain risk down the contract stack by requiring and encouraging suppliers and sub-suppliers to use sound security practices and allow transparency into processes and security practices. It is recommended that contract vehicles should require, encourage, or provide incentives for suppliers to deliver up-to-date information on changes that affect supply chain (SC) risk, such as changes in their suppliers, locations, process, and technology.

Use of the acquisition and procurement process early in the system lifecycle is a key way to protect the supply chain by defining and creating supplier requirements and incentives; using procurement carve-outs and controlled delivery path processes; and using all-source intelligence in procurement decisions. Source selection criteria and procedures should be developed in order to encourage suppliers to provide detailed visibility into the organization, elements, services, and processes. Other procurement tools may be available to manage the criticality of components and address risk in acquisition planning and strategy development.

13.7.4.2.7. Enhanced Vulnerability Detection

Due diligence analysis for items of supply is performed to counter unintentional vulnerabilities, intentional vulnerabilities (e.g., malicious wares and processes), and counterfeit's. It may include software static analysis, dynamic analysis (including the use of simulation, white and black box testing), penetration testing, and ensuring that the component or service is genuine (e.g., tag, digital signature, or cryptographic hash verification). Tools can include development, testing and operational tools.

Refer to Section 13.7.3 for more information on Software Assurance.

13.7.5. Trusted Suppliers

In the context of Program Protection, trusted suppliers are specific to microelectronic components and services. The Department is currently developing new policy on the criteria for using trusted suppliers. This content will be updated when that policy is published.

Defense Microelectronics Activity (DMEA) maintains a list of accredited suppliers on its

website at http://www.dmea.osd.mil/trustedic.html .

13.7.6. System Security Engineering

13.7.6.1. Definitions

System Security Engineering (SSE) : An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats. (MIL-HDBK-1785)

System Assurance (SA) : The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. (National Defense Industrial Association (NDIA) Guidebook, *Engineering for System Assurance* , Ver. 1.0)

Therefore, Systems Security Engineering (SSE) comprises the security-related Systems Engineering (SE) processes, activities, products, and artifacts for Systems Analysis (SA). Chapter 4 discusses the need to apply Systems Engineering (SE) early in the acquisition lifecycle. Accordingly, Systems Security Engineering (SSE) must also be considered early (and often).

13.7.6.2. Context of Systems Security Engineering (SSE) Within SE

In order to be cost-efficient and technically effective, Systems Security Engineering (SSE) must be integrated into Systems Engineering (SE) as a key sub-discipline. In fact, Section 5.3.5 of the Program Protection Plan (PPP) Outline indicates that the Program Protection Plan (PPP) should Describe the linkage between system security engineering and the Systems Engineering Plan and answer the question, How will system security design considerations be addressed?

DAG Chapter 4 provides comprehensive guidance for Systems Engineering (SE). In this chapter, Section 13.7.6.3 provides an overview of Systems Security Engineering (SSE) as a key countermeasure and Section 13.14 provides elaboration on how to include Systems Security Engineering (SSE) within Systems Engineering (SE). As a contextual starting point, the evolution of specifications and associated baselines across the acquisition is shown in Table 13.7.6.2.T1 .

Table 13.7.6.2.T1 Evolution of Specifications/Baselines

The	is developed by	and forms the
System Requirements Document (SRD)	the Government	Requirements Baseline
System Specification	the Contractor	Functional Baseline
Lower-level Subsystem Spec	the Contractor	Allocated Baseline
Fully-decomposed Component Spec	the Contractor	Product Baseline

Each of these specifications should baseline the developing system security requirements to be included in system design by applying the methods and tools of good Systems Engineering (SE). For example, as described in Section 13.3.2.1, repeated application of the Criticality Analysis (CA) methodology, reinforced by Systems Engineering (SE) tools such as fault isolation trees and system response analysis, will yield incremental refinements in the determination of what to protect and how to protect it.

Table 13.7.6.2.T2 shows the expected maturity of the baselines across the system lifecycle, according to the Systems Engineering Technical Reviews (SETR) events at which they should be assessed. It is noteworthy that even as early as the Alternative Systems Review (ASR), the preliminary system requirements should be identified. For further details concerning the appropriate system security content of the maturing baselines as they relate to the Systems Engineering (SE) review timeline, see Section 13.10.2 (*Systems Engineering Technical Reviews*).

Table 13.7.6.2.T2. Expected Maturity of Baselines at Each Systems Engineering Technical Reviews (SETR) Event

SETR or Audit	Typical Required Maturity of the Baselines				
	Requirements	Functional	Allocated	Design Release	Product
ASR	Preliminary	--	--	--	--
SRR	Draft	Preliminary	--	--	--
SFR	Approved	Entrance: Draft Exit: Established	Preliminary	Initial Preliminary	--
PDR	Maintained	Approved and Maintained	Entrance: Draft Exit: Established	Preliminary Draft	--
CDR	Maintained	Maintained	Approved and Maintained	Approved	Exit: Initial Baseline Established
FCA	Maintained	Maintained	Maintained	--	Controlled
SVR	Maintained	Maintained	Maintained	--	Controlled

PCA	Maintained	Maintained	Maintained		Finalized; Approved

13.7.6.3. Systems Security Engineering (SSE) Across the Lifecycle

While Systems Security Engineering (SSE) is categorized in this chapter as a countermeasure, it is important to realize that Systems Security Engineering (SSE) is actually an overarching Systems Engineering (SE) sub-discipline, within the context of which a broad array of countermeasures is appropriate. Some of these Systems Security Engineering (SSE)-related countermeasures represent an overlap with other countermeasure categories, such as Software Assurance (see Section 13.7.3) and Supply Chain Risk Management (SCRM) (see Section 13.7.4).

As a countermeasure in its own right, key Systems Security Engineering (SSE) activities are highlighted as follows:

- **Integrate Security into Requirements, Systems Security Engineering (SSE) Processes, and Constructs**
  - Integrate security requirements into the evolving system designs and baselines
  - Use secure design considerations to inform lifecycle trade space decisions
- **Activity Considerations by Phase**
  - Pre-Milestone A: Evaluate mission threads, identify system functions, and analyze notional system architectures to identify mission critical functions
  - Pre-Milestone B: Refine critical function list and identify critical system components and candidate subcomponents (hardware, software, and firmware)
  - Pre-Milestone C: Refine list of critical system components and subcomponents
  - **Note:** Consider rationale for inclusion or exclusion in the list and for priority assignments
- **Identify and implement countermeasures and sub-countermeasures**
  - Assess risks and determine mitigation approaches to minimize process vulnerabilities and design weaknesses
  - Perform cost/benefit trade-offs where necessary

Key Systems Security Engineering (SSE) criteria can be specified for each of the phases leading up to a major program Milestone, and it is important to establish these criteria across the full lifecycle in order to build security into the system. Further details are provided in Section 13.14 .

13.7.7. Security

This section will be updated in the next Defense Acquisition Guidebook (DAG) update.

[1] http://capec.mitre.org/documents/An_Introduction_to_Attack_Patterns_as_a_Software_Assurance_Knowledge_Resource.pdf

13.8. Horizontal Protection

Horizontal protection analysis is the process that determines if critical defense technologies, to include Critical Program Information (CPI), associated with more than one Research, Development, and Acquisition (RDA) program, are protected to the same degree by all involved DoD activities (DoDI 5200.39). DoD horizontal protection requires that all those who develop, process or store the same or similar Critical Program Information (CPI) use the same or equally effective:

- Classification standards
- Export Control guidelines
- Foreign disclosure arrangements
- Anti-tamper protections
- Information Assurance standards
- Physical Security Standards

Horizontal protection is necessary to ensure that an investment made by one program to protect Critical Program Information (CPI) is not diminished due to another program exposing the same Critical Program Information (CPI) or a similar technology with great risk. The goal of the adjudication process is an agreement on a common risk mitigation level among affected programs for the same Critical Program Information (CPI) or similar technologies, not a common protection requirement. The adjudication step in the horizontal protection process will only be necessary in rare cases.

13.8.1. Acquisition Security Database (ASDB)

The Acquisition Security Database (ASDB) is designed to support PMs, Research and Technology Protection (RTP), Anti Tamper (AT), Counterintelligence, Operations Security (OPSEC), and Security personnel supporting Acquisition Programs. It provides automated tools and functionality to enable efficient and cost-effective identification and protection of Critical Technologies (CT) and Critical Program Information (CPI). It offers a federated search capability and facilitates a standardized identification, implementation, and tracking of Critical Program Information (CPI) countermeasures.

The Acquisition Security Database (ASDB) supports program protection and specifically the horizontal protection process by providing a repository for Critical Program Information (CPI) and Countermeasures and offering a collaboration environment for programs, counterintelligence, security Subject Matter Experts (SMEs), and enterprise individuals supporting the program protection planning effort. The use of the Acquisition Security Database (ASDB) by DoD Components was directed by an Acquisition, Technology, and Logistics (AT&L) memo on July 22, 2010 which directed DoDI 5200.39 establishes policy to conduct comparative analysis of defense systems' technologies and align Critical Program Information (CPI) protection activities horizontally throughout the DoD.

The Acquisition Security Database (ASDB) supports the horizontal protection process in three ways. First, the Acquisition Security Database (ASDB) features a federated search that will allow enterprise individuals to search for similar Critical Program Information (CPI) based on name, Military Critical Technology List (MCTL), or technology type. The search results include the names of Program Protection Plans (PPPs) that match the search criteria. The Critical Program Information (CPI) description within the Program Protection Plan (PPP) can be reviewed and the assessment made as to whether or not the two Critical Program Information (CPI) are similar enough to require similar risk mitigation levels. Second, after the same or similar Critical Program Information (CPI) have been identified and determined to require equivalent risk mitigation, the protections lists in the Program Protection Plans (PPPs) can be analyzed for applicability. Third, the Acquisition Security Database (ASDB) provides the collaboration environment for discussions about the comparison of Critical Program Information (CPI), counterintelligence threats, and planned protections.

The program Acquisition Security Database (ASDB) record should be created as soon as Critical Program Information (CPI) is identified and updated periodically, as changes occur, and at each subsequent milestone. Critical Functions/Components are not identified in the Acquisition Security Database (ASDB).

To request access to the Acquisition Security Database (ASDB), please do the following from a SIPRNET Terminal:

1. Navigate to the Acquisition Security Database (ASDB) Public Site: https://asdb.strikenet.navy.smil.mil/default.aspx .

2. Select "Register" (on left menu).
3. Fill out User Information.
4. Click "Submit Information".

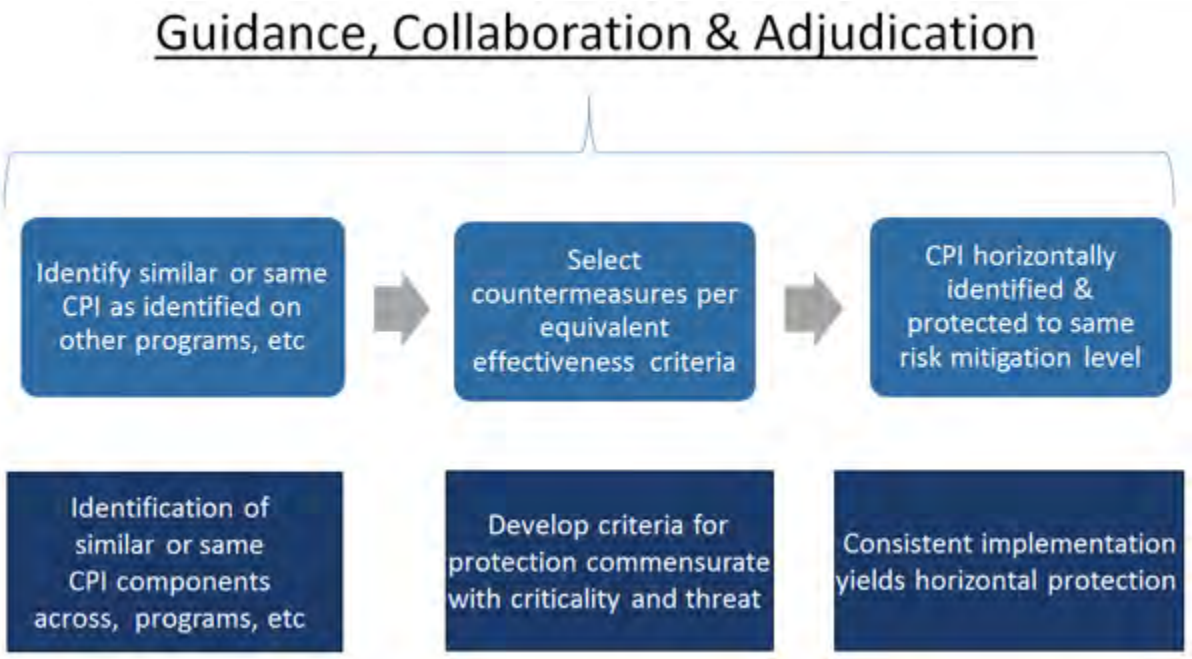
Your access request will be placed into the workflow process for approval. Once approved you will receive a SIPR and NIPR email from the Acquisition Security Database (ASDB) Technical Team.

If you need assistance, please contact the Acquisition Security Database (ASDB) Technical Team at (252) 464-5914 or DSN 451-5914.

13.8.2. Horizontal Protection Process

Programs should be continuously doing horizontal protection as soon as Critical Program Information (CPI) is identified. Below is the high-level horizontal protection process that shows how to protect Critical Program Information (CPI) to the same degree across the Services and programs.

Figure 13.8.2.F1. Horizontal Protection Process



The process for doing horizontal protection during Program Protection Plan (PPP) creation, update, or review is outlined below:

1. Request Acquisition Security Database (ASDB) access at https://asdb.strikenet.navy.smil.mil/default.aspx .
2. Create a record and fill out appropriate fields.
3. Use the search capabilities in the Acquisition Security Database (ASDB) to

identify other programs with potentially similar Critical Program Information (CPI). Consider threat and vulnerability differences between programs.
4. Compare planned countermeasure protection against the similar Critical Program Information (CPI) and consider threat and vulnerability differences between programs.
5. If there are perceived discrepancies or concerns, adjudicate the differences at the lowest organizational level.
6. If the discrepancies are not resolved, escalate to an executive decision making organization as determined by Acquisition, Technology, and Logistics (AT&L).
7. Incorporate the results of adjudication into the Program Protection Plan (PPP).

If you have any questions or need assistance, please contact the Acquisition Security Database (ASDB) Technical Team.

Phone: (252) 464-5914 or DSN 451-5914

NIPR E-Mail: W_SPAWAR_CHRL_SSCLANT_ChPt_TEAM_US@navy.mil

SIPR E-Mail: webmaster@strikenet.navy.smil.mil

13.9. Foreign Involvement

13.9.1. Programs with Foreign Participation

The Department of Defense, by law, is to consider cooperative opportunities with the North Atlantic Treaty Organization (NATO), NATO member nations, NATO organizations, non-NATO major allies, and other friendly countries for major defense acquisition programs. In general, DoD policy encourages foreign participation in DoD acquisition programs. Foreign participation ranges for cooperative research and development through production (i.e. foreign industrial participation), acquisition of the system through direct commercial sales (DCS) or foreign military sales (FMS), and other follow-on support.

When it is likely that there will be foreign involvement or access to the resulting system or related information, the Program Manager must plan for this foreign involvement to assist in identifying vulnerabilities to foreign exposure and developing technology security and foreign disclosure guidance to ensure that foreign access is limited to the intended purpose for that involvement while protecting critical program information and mission-critical functions and components and other sensitive information.

Some considerations to forecast potential foreign involvement includes:

- Cooperative research and development with allied or friendly foreign countries
- An allied system may be adopted
- System will replace/upgrade a system that had been previously sold to allies and friends

- System interoperability will be needed for use in future coalition operations

The Program Manager should consult with their international programs organization and technology security and foreign disclosure offices (i.e. National Disclosure Policy, Low Observable/Counter Low Observable (LO/CLO), Defensive Security Systems (DSS), Anti-Tamper (AT), Communication Security (COMSEC), Intelligence, etc.) to obtain assistance in addressing this matter. An integrated product team might be established for this purpose. International considerations to be addressed include the following, many of which should be available from the analysis used in developing the International Cooperation section of the Technology Development Strategy:

- Summarize any plans for cooperative development with foreign governments or cognizant organizations.
- Summarize plans to increase the opportunity for coalition interoperability as part of the developing DoD program.
- Assess the feasibility from a foreign disclosure and technology security perspective.
- Prepare guidance for negotiating the transfer of classified information and critical technologies involved in international agreements.
- Identify security arrangements for international programs.
- Coordinate with the disclosure authority on development of Delegation of Disclosure Authority Letter (DDL).
- Assist with development of Program Security Instruction (PSI) for a cooperative development program in support of program.
- Support decisions on the extent and timing of foreign involvement in the program,
- Foreign sales, and access to program information by foreign interests.
- Specify the potential or plans for Foreign Military Sales (FMS) and/or Direct Commercial Sales (DCS) and the impact upon program cost due to program protection and exportability features.
- Identify/nominate for consideration as a Defense Exportability Features (DEF) candidate.

13.9.2. Defense Exportability Features (DEF)

Defense Exportability Features (DEF) was established in the fiscal year 2011 National Defense Authorization Act to develop and incorporate technology protection features into a system or subsystem during its research and development phase. By doing this, exportable versions of a system or subsystem could be sold earlier in the Production and Development phase, thereby (1) enabling capability to be available to allies and friendly companies more rapidly and (2) lowering the unit cost of DoD procurements. Prior to the Engineering and Manufacturing Development Phase, programs should investigate the necessity and feasibility (from cost, engineering, and exportability perspectives) of the design and development of differential capability and enhanced protection of exportable versions of the system or subsystem. See Chapter 11.2.1.2. International Considerations within the Acquisition Management Framework for summary of Defense Exportability Features (DEF) nomination and feasibility

assessment.

13.10. Managing and Implementing PPPs

The Program Protection Plan (PPP) is a living document, required at Milestones A, B, C, and the Full-Rate Production decision through a July 18, 2011 Principal Deputy Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) policy memo. It is a best practice to also update the Program Protection Plan (PPP) prior to export decisions, and in order to report progress at each Systems Engineering Technical Review (SETR) event. The Program Protection Plan (PPP) is the single focal point for all program protection and system security activities on the program. It:

- Can serve as a focal point for capturing critical System Security Engineering (SSE) analysis and assessment results as it gathers and matures.
- Will provide previously-missing coverage of Systems Security Engineering (SSE) activities and associated analyses.
- Should contain either references to where the information can be found or the actual information.

The Program Protection Plan (PPP) is a plan a forward-looking document according to which the execution of protection will be performed. But it is also a report, which gathers the analysis and assessment results for effective program protection and system security as the plan is executed.

In this manner (plan + report), the Program Protection Plan (PPP) serves to provide the Security Assurance Case (reference International Organization for Standardization (ISO) Standard 15026 - Part 2 for a discussion on Assurance Cases), in which the preferred system concept represents the assurance claims, the system design represents the assurance arguments and the test plan results and Requirements Traceability Matrix (RTM) is the assurance evidence that can be traced to the system requirements.

All the pieces of an Assurance Case (Claims/Arguments/Evidence) are represented automatically by the inclusion of system security in System Engineering artifacts, such as the System Requirements Document (SRD), the system/subsystem specs, the preliminary and detailed design documents, the Requirements Traceability Matrix (RTM), and the Test Plans and Reports. The Assurance Case is thus built by the traceability of all the Systems Security Engineering (SSE) artifacts.

The Program Protection Plan (PPP) should tie all these things together. For example:

- Table 3.3-1 of the Program Protection Plan (PPP) Outline is used to provide traceability of critical components from mission-level documents (JCIDS (Joint Capabilities Integration Development System) Key Performance Parameters, Key System Attributes, etc.) and Critical Technology Elements (CTE) to the system architecture.
- Section 5.3 of the Program Protection Plan (PPP) Outline discusses the requirement to indicate the Request for Proposal (RFP) Contract Line Item Number (CLIN) or Data Item Description (DID) that will be used to ensure that Critical Program Information (CPI) and critical functions/components are protected in the development environment and on the system.
- Section 9.3 of the Program Protection Plan (PPP) Outline directs the implementation of Verification and Validation (V&V) to provide evidence that system security has been achieved, including a link to relevant discussion in the Test and Evaluation (T&E) documents.

The last bullet above indicates a method of checking Program Protection Plan (PPP) implementation (i.e., Verification and Validation (V&V)). Audit's/inspections are also used; namely, to ensure compliance with applicable laws, regulations, and policies. Engineering reviews are used to ensure that system security requirements are identified, traceable, and met throughout the acquisition lifecycle. These methods of checking Program Protection Plan (PPP) implementation are described in the following subparagraphs.

13.10.1. Audit's

Program Protection Surveys and other security audit's and inspections check for compliance with protection requirements. These processes check that statutory and regulatory security activities are being performed. Program Managers (PMs) should check with their Component research and development acquisition protection resources for guidance on performing these audit's.

13.10.2. Systems Engineering Technical Reviews

Section 9.2 of the Program Protection Plan (PPP) Outline requires that the Program Protection Plan (PPP) answer these questions:

- How will system security requirements be addressed in Systems Engineering Technical Reviews (SETR), functional/physical configuration audit's, etc.?
- What Program Protection entry/exit criteria will be used for these reviews?

The Systems Engineering Technical Reviews (SETR) process provides a key Systems Engineering health and risk assessment tool that is discussed in detail in Chapter 4 .

The following subparagraphs provide key Systems Security Engineering (SSE) and Supply Chain Risk Management (SCRM) criteria, recommended as Systems Engineering Technical Reviews (SETR) entry/exit criteria, in order to assess and ensure that an appropriate level and discipline of program protection activities and analyses are conducted across the full system context.

13.10.2.1. Initial Technical Review (ITR)

System security objectives and criteria are in the process of being defined and will be included in the next update.

13.10.2.2. Alternative Systems Review (ASR)

Relevant objectives include:

- System security and Supply Chain Risk Management (SCRM) are addressed as part of the alternative systems analysis and the development of the preferred system concept.
- The preferred system concept is based on an initial criticality analysis, using current threat data, informed by supply chain risk identification.
- Potential countermeasures for candidate Critical Program Information (CPI) and critical functions are identified.
- Plans are defined to protect critical functions/components, processes, tools, and data.
- The Statement of Work (SOW) for the Technology Development (TD) phase Request for Proposal (RFP) includes appropriate tasks for Systems Security

Engineering (SSE) and Supply Chain Risk Management (SCRM).

Recommended Criteria:

- Where system security and Supply Chain Risk Management (SCRM) addressed as part of the alternative systems analysis and the development of the preferred system concept?
    - Was an initial criticality analysis performed and documented for the Program Protection Plan (PPP)?
    - Did it use relevant, current threat data and potential vulnerability information?
    - Was the preferred system concept critical function/component alternatives evaluated for supply chain risks through the threat assessment center and used to add constraints to the system requirements?
    - Are the preferred concept engineering analysis and Request for Proposal (RFP) requirements being informed by supply chain risk considerations such as limited potential suppliers and defensive design?
    - Were criticality analysis results used to determine and evaluate candidate Critical Program Information (CPI) and critical functions, with rationale?
    - Have candidate countermeasures and possible sub-countermeasures been identified, with an emphasis on logic bearing components and supply chain risks?
    - Did the analysis include the full system context, including the multiple systems that support end-to-end mission threads?
- Was Systems Security Engineering (SSE) an integral part of the Milestone A phase systems engineering analysis?
    - Did all of the Systems Security Engineering (SSE) and Supply Chain Risk Management (SCRM) considerations and analyses inform the identification of requirements in the preliminary system requirements document (SRD)?
    - Have potential subsystem and component alternatives for critical functions been evaluated for potential suppliers, software assurance, and system assurance risks?
    - Has the assessment of security risks resulted in system security requirements in the System Requirements Document (SRD)?
    - Have residual Systems Security Engineering (SSE) based program protection risks and supply chain risks been identified for mitigation?
- Are plans in place to protect critical components, processes, tools, and data?
    - Do they promote awareness and provide personnel training on supply chain risks?
    - Are plans to define and protect critical processes, including the identity of users and system uses, included?
    - What tools are being used, how are they being protected (physically and operationally), and how are tools and data managed (including hardware development tools, software development tools, developer collaboration tools, and configuration management tools)?

- Have appropriate tasks been included in the Statement of Work (SOW) for the Technology Development (TD) phase Request for Proposal (RFP)?
    - Are specific responsibilities for Supply Chain Risk Management (SCRM) and for updated criticality analyses to assess critical functions and refine the identification of critical components included?
    - Is competitive prototyping and design included, as appropriate, for candidate Critical Program Information (CPI) and critical functions?
    - Are tasks to develop associated protection countermeasures included, based on the previously identified potential protection countermeasures and the system security requirements in the System Requirements Document (SRD)?
    - Are the use of software assurance databases and techniques (e.g., Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), static analysis, and penetration testing) included?

13.10.2.3. System Requirements review (SRR)

Relevant objectives include:

- System security (including criticality analysis and software assurance) and Supply Chain Risk Management (SCRM) concerns are considered in the development of the system performance requirements and non-tailorable design requirements across the full system context (e.g., including SoS).
- Initial threat and vulnerability assessments are performed and used in an updated criticality analysis.
- Lists are developed for initial Critical Program Information (CPI), critical functions (and potential components), selected countermeasures, and potential sub-countermeasures.
- Relevant Supply Chain Risk Management (SCRM) key practices, such as defensive design, are being applied.

Recommended Criteria:

- Where system security and Supply Chain Risk Management (SCRM) concerns considered in the development of the system performance requirements and non-tailorable design requirements, across the full system context (e.g., System of Systems (SoS))?
    - Are the system security and Supply Chain Risk Management (SCRM) requirements mutually understood between the Government and contractor(s)?
    - Are they testable or otherwise verifiable?
    - Will they lead to a final system that is operationally secure and consistent with cost and schedule?
- Is Systems Security Engineering (SSE) an integral part of the Technology Development (TD) phase systems engineering analysis?

    - Have contractor(s) performed and summarized their initial criticality analysis (which updates the Government provided initial criticality analysis, if available)?
    - In the absence of contractors, has the Government performed an updated criticality analysis?
    - Does it include rationale for the selection of Critical Program Information (CPI) and critical functions and potential components?
    - Have lists of initial Critical Program Information (CPI), critical functions (and potential components), selected countermeasures, and potential sub-countermeasures been developed?
    - Have initial threat and vulnerability assessments have been performed, tied to the contractors initial criticality analysis summary?
- Is/are the contractor(s) effectively fulfilling Technology Development (TD) phase Statement of Work (SOW) tasks for Systems Security Engineering (SSE) and Supply Chain Risk Management (SCRM)?
    - Are contractor-refined system security requirements derived from the countermeasures, sub-countermeasures, and defensive design or runtime features selected (e.g., design diversity and least privilege)?
    - Is there a draft allocation of sub-countermeasures and defensive requirements to preliminary design (architecture)? Does that design (architecture) extend to the full system context (e.g., System of Systems (SoS))?
    - Does the Systems Engineering Management Plan (SEMP) describe Systems Security Engineering (SSE) processes, with process updates derived from the countermeasures, sub-countermeasures, and controls selected?
    - Is there a draft allocation of process sub-countermeasures to the acquisition time line and to management and Systems Engineering (SE) sub-processes?
    - Does the contractors review package include planning to address the government provided residual security risk assessment (divided into acquisition, operational, and sustainment sections)?
    - Are tasks, funding, and schedule allocated in order to implement the Systems Security Engineering (SSE) and Supply Chain Risk Management (SCRM) requirements for the system and for management and SE sub-processes?
    - Are appropriate software assurance databases and techniques (e.g., Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), static analysis, and penetration testing) being planned and used?
- Are relevant Supply Chain Risk Management (SCRM) key practices being applied?
    - What development and configuration management tools are being used, how are they being protected (physically and operationally), and how are tools and data managed (including hardware, software, and data

configuration management)?
    - Is defensive design being used across the full system context to anticipate potential ways that an element, system, or process could fail or be misused, so that the architecture and requirements specification of the element, system, or process can minimize failures and misuse?
    - How are critical elements and processes being protected?
    - How are trustworthy elements being selected?
    - How are supply chain assurance concerns being incorporated into the requirements?
    - Does the contract language cover Supply Chain Risk Management (SCRM) considerations (e.g., the right to subcontract, etc.)?

13.10.2.4. System Functional Review (SFR)

Relevant objectives include:

- System security and Supply Chain Risk Management (SCRM) concerns are considered in establishing the functional baseline.
- An updated criticality analysis is performed, together with updated threat and vulnerability assessments, as required.
- Lists are updated for candidate Critical Program Information (CPI), critical functions and components, selected countermeasures, and potential sub-countermeasures.
- Relevant Supply Chain Risk Management (SCRM) key practices are being applied.

Recommended Criteria:

- Has an updated criticality analysis summary been generated, including rationale for Critical Program Information (CPI) and critical-function selection?
    - Does it derive and allocate critical functions?
    - Does it update the system design based on critical functions and design trade-offs?
    - Are updated threat and vulnerability analyses included, as required?
- Have derived Systems Security Engineering (SSE)/protection functional requirements been flowed into updated subsystem and preliminary component specifications?
    - Has a draft allocation of sub-countermeasures and defensive functions to preliminary functional and physical design been performed? Does this allocation extend across the full system context?
- Have candidate Critical Program Information (CPI) and critical-function countermeasure and sub-countermeasure functional requirements in the system spec been traced to lower level specifications?
    - Have Critical Program Information (CPI) and critical-function countermeasure and sub-countermeasure trade-off analyses been conducted with respect to cost, benefit, and risk?

    - Have Critical Program Information (CPI) and critical-function residual vulnerability risks been assessed?
- Are the cost and schedule of lower-level Systems Security Engineering (SSE) tasks identified and included in the lower level cost and schedule plans?
    - Are detailed Systems Security Engineering (SSE) activities in agreement with the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS)?
    - Do planning packages include required resources to complete Systems Security Engineering (SSE) tasks?
- Are relevant Supply Chain Risk Management (SCRM) key practices being applied?
    - What development tools are being used by suppliers, how are they being protected (physically and operationally), and how are tools and data managed (including hardware, software, and data configuration management)?
    - Is defensive design being applied to include defensive functions and to maximize resilience? Does this extend across the full system context?
    - How are critical elements and processes being protected?
    - How are trustworthy elements being selecting?
    - How thoroughly are suppliers and their supply chain(s) being evaluated?
    - Are the plans to promote awareness and provide personnel training on supply chain risks being executed?

13.10.2.5. Preliminary Design Review (PDR)

Relevant objectives include:

- System security and Supply Chain Risk Management (SCRM) concerns are considered in establishing the system allocated baseline.
- Preliminary system design, including security, is ready to proceed into detailed design; and, stated security performance requirements can be met within cost, schedule, risk, and other system constraints.
- An updated criticality analysis is performed and an updated list of Critical Program Information (CPI), critical functions and components, selected countermeasures, and sub-countermeasures is produced, with rationale.
- Relevant Supply Chain Risk Management (SCRM) key practices are being applied.

Recommended Criteria:

- Have system security and Supply Chain Risk Management (SCRM) concerns been considered in establishing the system allocated baseline?
    - Has an updated criticality analysis summary been generated, with rationale for Critical Program Information (CPI) and critical component selection?
    - Was an updated threat and vulnerability assessment summary, with

respect to the updated criticality analysis summary, included, and were supply chain risks included? Does this extend across the full system context (e.g., System of Systems (SoS))?
    - Does the updated Critical Program Information (CPI)/critical component list include countermeasures and sub-countermeasures?
    - Are inherited Critical Program Information (CPI) and horizontal protection adequately assessed, are they being addressed consistently at system and subsystem levels, and are they documented in the updated Acquisition Strategy (AS), Test and Evaluation Management Plan (TEMP) , and Program Protection Plan (PPP)?
    - Have Systems Security Engineering (SSE) and Supply Chain Risk Management (SCRM) processes been updated, based on the selected countermeasures, sub-countermeasures, and controls?
- Does the preliminary system design appropriately include and address security, and is it ready to proceed into detailed design?
    - Where System Requirements Document (SRD) security requirements trades based on the Program Managers (PM) assessment of cost, schedule, performance, and supply chain risks?
    - Were the security requirements specifications, updated for subsystems and components, derived from the countermeasures, sub-countermeasures and defensive design or runtime features selected (e.g., defense in depth)?
    - Was an updated residual security risk assessment performed for the summary-level critical functions and Critical Program Information (CPI), covering acquisition, operations, and sustainment activities (for both system and processes, after sub-countermeasures are applied), including supply chain considerations? Does this extend across the full system context (e.g., System of Systems (SoS))?
    - Has an Anti-Tamper (AT) plan been generated (if it is a contract deliverable)?
    - Are appropriate software assurance databases and techniques (e.g., Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), static analysis, and penetration testing) used to assess vulnerabilities and exposures to attack, common destructive attack patterns, and weaknesses in the software architecture and design?
    - Have Critical Program Information (CPI) and critical components and sub-components that were categorized as Critical Technology Elements (CTE) been demonstrated at a Technology Readiness Level (TRL) 6 or better?
- Was an allocation of sub-countermeasures and defensive functions to the design/architecture below the counterintelligence (CI) level performed?
    - Was the critical functionality of each Hardware Configuration Item (HWCI) and Computer Software Configuration Item (CSCI) allocated to lower level components?
    - Were Systems Security Engineering (SSE) fault isolation tree and system response analysis techniques used to define appropriate sub-

countermeasures?
    - Does the allocated design effectively implement appropriate sub-countermeasures?
    - Where system designs that could expose critical functionality to vulnerability assessed, and were architecture trade-offs evaluated, in order to formulate the allocated baseline?
    - Were external and subsystem interface requirements vulnerabilities assessed and used as input to the sub-countermeasure selection?
    - Do planned sub-countermeasures for design and implementation include software assurance (e.g., fail-safe defaults, defense in depth, purging of temporary data, avoidance of unsafe coding constructs, secure languages and libraries, and static and dynamic code analysis)?
- Are relevant Supply Chain Risk Management (SCRM) key practices being applied?
    - What development tools are being used by suppliers, how are they being protected (physically and operationally), and how are tools and data managed (including hardware, software, and data configuration management)?
    - How are critical elements and processes being protected?
    - How are supplier roles constrained and access limited?
    - How thoroughly are suppliers and their supply chain(s) being evaluated?
    - Are the plans to promote awareness and provide personnel training on supply chain risks being executed?

13.10.2.6. Critical Design Review (CDR)

Relevant objectives include:

- System security and Supply Chain Risk Management (SCRM) concerns are considered in establishing the system product baseline.
- Detailed system design, including security, is ready to proceed into fabrication/development; and, stated security performance requirements can be met within cost, schedule, risk, and other system constraints.
- An updated criticality analysis is performed and updated lists of Critical Program Information (CPI), critical components and sub-components, selected countermeasures, and specific sub-countermeasures are produced, with rationale. This extend across the multiple systems that support the end-to-end mission threads.
- Relevant Supply Chain Risk Management (SCRM) key practices are being applied.

Recommended Criteria:

- Is Systems Security Engineering (SSE) an integral part of the Engineering and Manufacturing Development (EMD) phase systems engineering analysis?
    - Has the contractor updated and summarized their criticality analysis, with

rationale, to include a final list of updated Critical Program Information (CPI) and critical components and sub-components, together with associated countermeasures and explicit sub-countermeasures?
    - Were inherited Critical Program Information (CPI) and horizontal protection adequately assessed in the updated criticality analysis?
    - Were adequately robust Systems Security Engineering (SSE) tools used in establishing the product baseline; e.g., the use of an updated system response matrix and Systems Security Engineering (SSE) fault isolation tree techniques?
    - Were appropriate software assurance databases and techniques (e.g., Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), static analysis, and penetration testing) used to reassess vulnerabilities and exposures and to reexamine weaknesses in the software architecture, design, and code?
    - Do sub-countermeasures for implementation and testing include software assurance (e.g., purging of temporary data, avoidance of unsafe coding constructs, secure languages and libraries, static and dynamic code analysis, fault injection, and patch management)?
    - Has a residual vulnerability risk assessment been performed to assess, mitigate and re-assess weaknesses in the detailed design, including an assessment of security in the operational environment?
- Does the detailed system design include and appropriately address security and Supply Chain Risk Management (SCRM) considerations, and is it ready to proceed into fabrication/development?
    - Have all Systems Security Engineering (SSE) requirements been flowed down and mapped to the detailed system design and the lifecycle processes?
    - Has an allocation of specific sub-countermeasures to sub-components and lower-level items in counterintelligence (CI) specifications and Statement of Work requirements been performed?
    - Have appropriate Systems Security Engineering (SSE) countermeasures and sub-countermeasures been allocated to the design with validation criteria established (e.g., engineering-in-depth for separation and layering of critical elements, addition of defensive function layers, and handling of authentication methods)?
    - Does the detailed design incorporate good Systems Security Engineering (SSE) practices, such as minimizing the attack surface, the number of critical components, and/or the number of potential weaknesses? Do these Systems Security Engineering (SSE) practices extend across the full system context (e.g., System of Systems (SoS))?
    - Are quantifiable measures being used to assess the detailed design for security and for application of countermeasures (corrective actions) to address identified deficiencies?
    - Has manufacturability been assessed, including the availability and identification of accredited suppliers for secure fabrication of Application-

specific integrated circuits (ASICs), Field-programmable gate array (FPGAs), and other programmable devices?
    - Has validation and verification of system security and Supply Chain Risk Management (SCRM) requirements been finalized and reflected in the Test and Evaluation Management Plan (TEMP), preliminary test plans, Systems Engineering Plan (SEP) , and other operational Concept of Operations (CONOPS) documents?
- Are relevant Supply Chain Risk Management (SCRM) key practices being applied?
    - What development tools are being used by suppliers, how are they being protected (physically and operationally), and how are tools and data managed (including hardware, software, and data configuration management)?
    - Was diversification of standard interfaces and defensive design used for architecting the system?
    - How will critical elements and processes be protected throughout the lifecycle, including disposal of items?
    - How will trustworthy elements continue to be selected throughout the lifecycle?
    - How are supplier roles constrained and access limited?
    - How thoroughly are suppliers, their supply chain(s), and their delivery processes being evaluated?
    - How are Government supply chain delivery mechanisms being protected?
    - Are the plans to promote awareness and provide personnel training on supply chain risks being executed?

13.10.2.7. Test Readiness Review (TRR)

Relevant objectives include:

- System security and Supply Chain Risk Management (SCRM) concerns are considered in establishing readiness of the system to begin formal acceptance testing, and this extends across the full system context (e.g., System of Systems (SoS)).
- The system test plans and objectives, including scope, procedures, and test facilities, are adequate for appropriately verifying all system security requirements.

Recommended Criteria:

- Is there a documented, comprehensive mapping of all security requirements to their test/verification methods, to include bi-directional traceability?
    - Does it include all system security requirements, clearly defined from threat analysis/modeling, and vulnerabilities identified in residual vulnerability risk assessments? Does this extend to the multiple systems that support the end-to-end mission threads?

    - Are all countermeasures for all identified vulnerabilities implemented in the detailed design included and mapped?
    - Do system verification and validation plans (including flow-down from the Test and Evaluation Management Plan (TEMP) to test plans and procedures) adequately ensure that coding and fabrication of designed components provide the required system security?
    - Is it possible to pull the thread from the initial criticality analysis identifying comprehensive security requirements across the lifecycle to the verification/validation efforts (comprising, for example, a set of organized pointers into the Program Protection Plan (PPP), System Requirements Document (SRD), flow-down requirements specifications, design documents, requirements traceability matrix, and the Test and Evaluation Management Plan (TEMP), test plans, and test procedures)?
- Are system test plans and objectives, including scope, procedures, and test facilities, adequate for appropriately verifying all system security and Supply Chain Risk Management (SCRM) requirements, across the full system context (e.g., System of Systems (SoS))?
    - Are security threat and attack scenarios included in testing?
    - Does system testing include penetration testing, testing for confidentiality of users and uses, and configuration of elements to limit access and exposure?
    - Are appropriate security test facilities and test equipment, schedule, and personnel planned in the Test and Evaluation Management Plan (TEMP) and lower level test plans, Integrated Master Plan (IMP), and Systems Engineering Plan (SEP); and, are they adequate and available?
    - Do planned measures for verification testing and operational use include software assurance sub-countermeasures/techniques (e.g., static and dynamic code analysis, fault injection, patch management, white- and black-box testing, penetration testing, sandboxing, and honey pot systems)?
    - Have Critical Program Information (CPI) and critical components and sub-components that were categorized as Critical Technology Elements (CTEs) been demonstrated at a Technology Readiness Level (TRL) 7 or better?

13.10.2.8. System Verification Review (SVR) / Functional Configuration Audit (FCA)

Relevant objectives include:

- The production system is compliant with all functional baseline system security requirements and provides full functionality, without exploitable vulnerabilities (or with security and supply chain risks mitigated to an acceptable level). This extends to the full system context (e.g., System of Systems (SoS)).
- An Updated Program Protection Plan (PPP) is being developed for delivery at

Full Rate Production (FRP).

Recommended Criteria:

- Is the production system compliant with all functional baseline system security requirements?
    - Is full system functionality provided without exploitable vulnerabilities, or with security and supply chain risks mitigated to an acceptable level? Does this include the multiple systems that support the end-to-end mission threads, as defined in the Concept of Operations (ConOps)?
    - Are system protection requirements adequate against the system specifications flowed from the Initial Capabilities Documents (ICD)?
    - Is there a complete traceability of capabilities to system security requirements to detailed design to protection verification methods to results?
    - Has a review of all analysis, inspection, demonstration, and test reports of compliance to meet security and Supply Chain Risk Management (SCRM) requirements been conducted, and do all items meet verification needs?
    - Have all planned Systems Security Engineering (SSE) activities/products been implemented, including software assurance, system assurance, and Supply Chain Risk Management (SCRM); and, have the results been documented?
    - Has a residual vulnerability risk assessment been performed to assess, mitigate, and re-assess weaknesses in the system, including an assessment of security in the operational environment?
    - Are plans in place to update the residual risk assessment periodically during sustainment?

13.10.3. Verification and Validation (V&V)

Some program protection activities have requirements testing, verification, and validation built into their processes (e.g. Anti-Tamper, Information Assurance). Further guidance on more general integration of Program Protection into Verification and Validation (V&V) activities will be provided in the next Defense Acquisition Guidebook (DAG) update.

13.10.4. Sustainment

While the primary emphasis of Program Protection is on the design and acquisition phases of a system lifecycle, some sustainment considerations must be addressed if the protection profile is to survive system delivery. Repair depots, for example, should be aware of Critical Program Information (CPI) and mission-critical functions and components on systems they are maintaining so as to appropriately protect these items from compromise. Further guidance on sustainment considerations for Program Protection will be provided in the next Defense Acquisition Guidebook (DAG) update.

13.11. Compromises

Incidents of loss, compromise, or theft of proprietary information or trade secrets involving Critical Program Information (CPI), are immediately reported in accordance with Section 1831 et seq. of Title 18 of the United States Code , DoD Instruction 5240.04 , and DoD Directive 5200.01 . Such incidents are immediately reported to the Defense Security Service (DSS), the Federal Bureau of Investigation (FBI), the applicable DoD Component counterintelligence (CI) and law enforcement organizations. If the theft of trade secrets or proprietary information might reasonably be expected to affect DoD contracting, Defense Security Service (DSS) should notify the local office of the Federal Bureau of Investigation (FBI).

DSS presently has responsibility for protecting Critical Program Information (CPI) that is classified. However, the contract may specifically assign Defense Security Service (DSS) responsibility to protect Critical Program Information (CPI) that is controlled unclassified information. Consequently, Defense Security Service (DSS) would receive reporting on unclassified Critical Program Information (CPI) incidents if it had specific protection responsibility or the incident could involve foreign intelligence activity or violate the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) .

13.12. Costs

13.12.1. Security Costs

The cost of implementing the selected countermeasures that exceed the normal

National Industrial Security Program Operating Manual (NISPOM) costs are recorded in this section of the Program Protection Plan (PPP).

13.12.2. Acquisition and Systems Engineering Protection Costs

A cost benefit risk trade-off is used to decide upon which countermeasures to implement for each of the Critical Program Information (CPI) and Critical Function (CF). Based upon the criticality analysis results and Critical Program Information (CPI) identification (Section 13.3), the threats (Section 13.4), the vulnerability assessment (Section 13.5), the risk analysis, and the list of potential countermeasures (Section 13.6) the program is now ready to prepare the cost-benefit verses risk trade-off. For each Level I and selected level II Critical Function (CF) components and each Critical Program Information (CPI) along with the associated risk analysis a cost and schedule implementation estimate is prepared for each potential countermeasure. Also estimated is the residual (remaining) risk to the Critical Function (CF) or Critical Program Information (CPI) after the countermeasure has been implemented.

Based upon this analysis the program manager can select the countermeasure or combination of countermeasures that best fit the needs of the program. It may be to implement the optimum countermeasure(s) do not fit within the programs constraints and other countermeasures can reduce the risk to an acceptable level. In some cases the program may choose to accept the risk and not implement any countermeasures. The emphasis of this analysis is to allow the program manager to perform an informed countermeasure trade-off with an awareness of the vulnerabilities and risks to the system. A summary of the trade-off analysis along with the rationale for the decision needs to be documented in this section of the Program Protection Plan (PPP).

13.13. Contracting

13.13.1. Request for Proposal (RFP) Guidance for all Phases

Comprehensive program protection needs to be addressed during the Request for Proposal (RFP) development and the system design to ensure that security is designed into the system. Program protection includes features that are included in the system design as wells as elements to be included in the processes used to develop the system. As a result program protection needs to be reflected in the system requirements document (SRD) and the statement of work (SOW) portions of the Request for Proposal (RFP) package. It may also be included in the instructions, conditions and notices to offeror’s (section L) and the evaluations factors for award (section M) of the Request for Proposal (RFP).

The program protection analysis needs to be performed iteratively prior to Milestone A and prior to each of the planned Systems Engineering Technical Reviews (SETRs) to ensure that the security features are considered and traded-off in conjunction with the other “ilities” and system performance. The program protection analysis begins with the identification of the Critical Program Information (CPI) and Mission Critical Functions

and components (described in Section 13.3) followed by the identification of vulnerabilities (described in Section 13.5), a risk assessment and the identification of potential countermeasures (described in Section 13.7).

13.13.1.1. System Requirements Document

The system requirements document should include security requirements based upon the initial countermeasures identified at Milestone A and good security practices. For example, if a particular Critical Program Information (CPI) component requires anti-tamper protection it may have a requirement to have seals, encryption, environmental and logging requirements for the component (see Section 13.7.1). An Information Assurance countermeasure example may be a requirement to include one of the controls specified in the DoD Information Assurance Certification and Accreditation Process (DIACAP) in the component (see Section 13.7.2).

Examples of software assurance countermeasures include requirements for exception handling and degraded mode recovery. There may also be requirements for specific secure coding practices for critical function components such as input validation, default deny, address execution prevention and least privilege (see Section 13.7.3). A supply chain countermeasure example for critical function components may be a requirement for redundancy diversity or checksum validation during startup (see Section 13.7.4)

13.13.1.2. Statement of Work

During the Request for Proposal (RFP) development not all of the system security requirements and design features have been determined. As a result it is necessary to transfer a major part of the program protection analysis, specification, and countermeasure implementation to the contractor to protect the system from loss of advanced technology, malicious insertion, tampering and supply chain risks. The following responsibilities should be considered for inclusion in the Statement of Work:

- The contractor shall perform or update a criticality analysis, vulnerability assessment, risk assessment, and countermeasure selection and implementation, with assumptions, rationale, and results, before each of the Systems Engineering Technical Reviews (SETRs) defined for the program.
- For each level I and level II component (in accordance with Table 13.3.2.1.T1), the contractor shall identify the associated logic-bearing hardware, software and firmware that implements critical functions or introduces vulnerability to the associated components (designated as "critical components).
- The contractor shall demonstrate that the contractor has visibility into its supply chain for critical components, understands the risks to that supply chain, and has implemented or plans to implement risk mitigations to counter those risks.

- The contractor shall plan for and implement countermeasures which mitigate foreign intelligence, technology exploitation, supply chain and battlefield threats and system vulnerabilities that result in the catastrophic (Level I) and critical

(Level II) protection failures, including:

1. The application of supply chain risk management best practices, applied as appropriate to the development of the system. Supply chain risk management key practices may be found in the National Institute of Standards and Technology (NIST) Interagency Report 7622, *Piloting Supply Chain Risk Management for Federal Information Systems* , and the National Defense Industrial Association Guidebook, *Engineering for System Assurance* , both publicly available.
2. The enumeration of *potential* suppliers of critical components, as they are identified, including cost, schedule and performance information relevant for choice among alternates and planned selection for the purpose of engaging with the government to develop mutually-agreeable risk management plans for the suppliers to be solicited.
3. The processes to control access by foreign nationals to program information, including, but not limited to, system design information, DoD-unique technology, and software or hardware used to integrate commercial technology.
4. The processes and practices employed to ensure that genuine hardware, software and logic elements will be employed in the solution and that processes and requirements for genuine components are levied upon subcontractors.
5. The process used to protect unclassified DoD information in the development environment.

- The preceding clauses shall be included in the solicitations and subcontracts for all suppliers, suitably modified to identify the parties.
- The contractor shall develop a set of secure design and coding practices to be followed for implementation of Level I and II critical components, drawing upon the top 10 secure coding practices (https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices) and the Common Weakness Enumeration (CWE)/SysAdmin, Audit, Network, Security (SANS) top 25 most dangerous software errors (http://cwe.mitre.org/top25/index.html).
- The contractor shall develop a Program Protection Implementation Plan (PPIP) that addresses the following sections of the Program Protection Plan (PPP) outline and example:
  - Section 2 Identifying what to protect
  - Section 4 Vulnerabilities
  - Section 5 Countermeasures
  - Section 7 Program Protection Risks
  - Section 8 Managing and Implementing Program Protection Plan (PPP)
  - Section 9 --Process for Management and Implementation of Program Protection Plan (PPP)
  - Section 10 Process for Monitoring and Reporting Compromises
  - Appendix C: Criticality Analysis

13.13.1.3. Instructions, Conditions and Notice to Offeror's (Section L)

For many Request for Proposal (RFP) packages system security engineering may not have any explicit clauses in this section. If it is determined to identify specific program protection content for the proposal the following items should be considered:

- The offeror, as part of its technical proposal, shall describe the use of its systems security engineering process in specifying and designing a system that is protected from loss of advanced technology, malicious insertion, tampering and supply chain risks.
- The offer shall describe the offeror's Critical Program Information (CPI) identification, mission criticality analysis, vulnerability assessment, risk evaluation and countermeasure implementation in arriving at its system specification and design.
- The offeror shall describe the offeror's secure design and coding practices.

13.13.1.4. Evaluation Factors for Award (Section M)

For most Request for Proposal (RFP) packages systems security engineering may not rise to the level of an evaluation factor. If it does programs should consider following as evaluation criteria:

- The extent to which the offeror employs a disciplined, structured systems security engineering (SSE) process, including Critical Program Information (CPI) identification, criticality analysis, vulnerability assessment, risk analysis and countermeasure implementation in arriving at its system specification and design.

13.14. Detailed System Security Engineering

13.14.1. Systems Security Engineering (SSE) Organization

13.14.2. Systems Security Engineering (SSE) Process

13.14.2.1. Military Handbook 1785

13.14.2.2. Systems Security Engineering (SSE) Activities by Phase

13.14.2.2.1. Materiel Solution Analysis (MSA) Phase

13.14.2.2.2. Technology Development (TD) Phase

13.14.2.2.3. Engineering and Manufacturing Development (EMD) Phase

13.14.3. Security Engineering for International Programs

13.14. Detailed System Security Engineering

An overview of System Security Engineering (SSE) is provided in Section 13.7.6 , including:

- A clear definition of Systems Security Engineering (SSE), taken from MIL-HDBK-1785 (Section 13.7.6.1)
- A discussion of the context of Systems Security Engineering (SSE) within Systems Engineering (SE) as a key sub-discipline, including how security requirements are mapped to the evolving system design, specifications, associated baselines, and Systems Engineering Technical Reviews (SETR) events (Section 13.7.6.2)
- An overview of the Systems Security Engineering (SSE) activity considerations by lifecycle phase (Section 13.7.6.3)

The subparagraphs below provide further details.

13.14.1. Systems Security Engineering (SSE) Organization

Systems Security Engineering (SSE) is performed by a variety of professionals. These professionals may have specific expertise in one or more areas (e.g., threat assessment, networking, expertise in one or more security technologies, software assurance, and vulnerability assessment). While serving in the role of the system security engineer, these professionals are responsible for maintaining a comprehensive and holistic system-view while addressing stakeholder security requirements. Systems Security Engineering (SSE) leverages and adapts the principles and practices of Systems Engineering (SE) within the same system life cycle framework that governs Systems Engineering (SE) processes. The system security engineer should have a foundational understanding of systems engineering to include the roles and processes

for which the systems engineer is responsible.

The program manager should utilize a Working-level Integrated Product Team (WIPT) to perform comprehensive program protection analysis. It is the responsibility of the program manager to ensure that the Working-level Integrated Product Team (WIPT) is comprised of appropriate representatives (including Systems Engineers (SEs), Systems Security Engineering (SSE) Subject Matter Experts (SMEs), logistics, system user representatives, and supporting counterintelligence, intelligence, foreign disclosure, and security personnel) to ensure a comprehensive analysis of system technology, hardware, software, firmware, and information. This Working-level Integrated Product Team (WIPT) or a sub-group (such as a System Security Engineering Working Group (SSEWG)) should focus on engineering aspects of security. They should define and identify all Systems Security Engineering (SSE) aspects of the system, develop an Systems Security Engineering (SSE) architecture, review the implementation of the architecture, and participate in design validation. This sub-Working Integrated Product Team (WIPT)/ System Security Engineering Working Group (SSEWG) should be formed as early in the acquisition process as possible.

13.14.2. Systems Security Engineering (SSE) Process

Systems Security Engineering (SSE) supports the development of programs and design-to specifications providing life-cycle protection for critical defense resources. Systems Security Engineering (SSE) secures the initial investment by "designing-in" necessary countermeasures and "engineering-out" vulnerabilities, and thus results in saving time and resources over the long term. During the system design phase, Systems Security Engineering (SSE) should identify, evaluate, and eliminate (or contain) known or potential system vulnerabilities, spanning the life cycle.

13.14.2.1. Military Handbook 1785

While very dated, MIL-HDBK-1785 contains still-useful information on pertinent Systems Security Engineering (SSE) activities and procedures and for contracting necessary Systems Security Engineering (SSE) efforts, including the practice of generating a System Security Management Plan (SSMP). The format and contents for the System Security Management Plan (SSMP) are outlined in the appropriate Data Item Descriptions listed in MIL-HDBK-1785. Current guidance calls for including most of the System Security Management Plan (SSMP) material in the Systems Engineering Plan (SEP) and the Program Protection Plan (PPP).

13.14.2.2. Systems Security Engineering (SSE) Activities by Phase

Systems Security Engineering (SSE) is the vehicle for interfacing research and technology protection into the Systems Engineering (SE) acquisition process, whereby Systems Engineering (SE) activities prevent exploitation of critical functions and components of U.S. defense systems. The benefit of Systems Security Engineering (SSE) is derived after acquisition is complete by mitigation of threats against the system

during deployment, operations, and support. Systems Security Engineering (SSE) also addresses threats during the acquisition process (typically through the supply chain) as well as the possible capture of the system by enemies during combat or hostile actions. Note that Systems Security Engineering (SSE) might be required in localized situations where stakeholder security requirements are addressed in the absence of full implementation of Systems Engineering (SE) activities. This can occur at any stage in the system lifecycle. Key Systems Security Engineering (SSE) criteria can be specified for each of the phases leading up to a major program Milestone, and it is important to establish these criteria across the full lifecycle in order to build security into the system.

13.14.2.2.1. Materiel Solution Analysis (MSA) Phase

During the Milestone A phase, most of the Systems Security Engineering (SSE) related activities, criteria, and results can be mapped to content of the Milestone A Program Protection Plan (PPP), as described in the Program Protection Plan (PPP) Outline. Associated Milestone A engineering analyses and Program Protection Plan (PPP) content include the following:

- Include system security in the architectural/design trade-offs and the construction of notional system designs
- Leverage available threat and vulnerability understanding in the engineering analysis to identify candidate mission-critical functions and define security requirements
- Evaluate concept of operations (CONOPS) and notional system architectures to identify mission-critical functions
    - Apply Systems Engineering (SE) tools to Systems Security Engineering (SSE); e.g., protection fault isolation tree methods and system response matrix analysis
- Perform an initial Criticality Analysis (CA) based on mission threads and system functions to identify and prioritize a reasonable and thorough list of mission-critical functions for protection
    - Identify rationale for inclusion or exclusion of system functions in the list
    - Ensure that comprehensive program protection is fulfilled by the identification of critical functions (completeness will comprise critical functions, critical information, and critical technology; indigenous/organic Critical Program Information (CPI) and inherited Critical Program Information (CPI))
- Identify candidate countermeasures and sub-countermeasures to be applied to each critical function, with emphasis on logic bearing components
- Perform trade-offs of design concepts and potential alternative countermeasures to minimize vulnerabilities, weaknesses, and implementation costs
- Examine residual vulnerability rationale for residual risks and plan for threat and vulnerability residual risk assessments after countermeasures have been applied
    - Use cost benefit trade-offs and other rationale

The threat analyses and plans/schedule to counter them, as captured in the PPP,

should correlate with and point to the discussion provided in Section 2.3 of the Technology Development Strategy (TDS) (see the Technology Development Strategy (TDS)-Acquisition Strategy (AS) Outline).

Other key Systems Security Engineering (SSE) activities during the Milestone A phase, not necessarily captured in specific documents, include:

- Ensure that criticality analyses and the development of security requirements extends to multiple systems that support the end-to-end mission threads, including System of Systems (SoS)/Family of Systems (FoS) interdependencies.
- For the trade-off analysis that considers implementation of critical functions via software, include an evaluation of Software Assurance countermeasures that uses:
    - Common Vulnerabilities and Exposures (CVE) To identify vulnerabilities that enable various types of attacks.
    - Common Attack Pattern Enumeration and Classification (CAPEC) To analyze development and operational environments, and potential interfaces, for common destructive attack patterns.
    - Common Weakness Enumeration (CWE) To examine software architectures and notional designs for weaknesses.
- Ensure that the preferred system concept(s) includes preliminary level security requirements derived from risk assessment and mitigation for critical functions. These requirements will typically be reflected in the preliminary System Requirements Document (SRD), if one exists. (See below for other expected System Requirements Document (SRD) content.)
- Ensure that candidate Critical Program Information (CPI) and potential critical components associated with mission-critical functions are mature enough to adequately address security; i.e., those that are potential Critical Technology Elements (CTE) (being matured to a Technology Readiness Level (TRL) of 4 by Milestone A) include validation of expected security in a laboratory environment.
- Consider Systems Security Engineering (SSE) in planning for technology maturation during the Technology Development (TD) phase, including:
    - Mitigation of candidate critical function risks, including countermeasures and candidate sub-countermeasures.
    - Inclusion of candidate critical functions in competitive prototyping plans for critical components.
    - Inclusion of threats in the definition of relevant environment for a Technology Readiness Level (TRL) of 6.
- Incorporate trade study results into the developing system requirements and the Request for Proposal (RFP) Statement of Work for the Technology Development (TD) phase (See Section 13.13.1 for other expected Request for Proposal (RFP) and Statement of Work content).

Other documents generated during the Milestone A phase should also contain Systems Security Engineering (SSE) relevant content. A thorough discussion of the Systems Engineering Plan (SEP) is given in Chapter 4 . Expected Systems Security Engineering

(SSE) content in the Systems Engineering Plan (SEP) can be highlighted as follows:

- Description of Systems Security Engineering (SSE) within the overall Systems Engineering (SE) approach, including processes to be used by the Government and contractors.
- Identification of system level security requirements generation as part of the System Requirements process.
- Technical Risk Plan includes a summary of the mission-critical functions with risks, candidate countermeasures and sub-countermeasures, and residual risk (or a reference to the Program Protection Plan (PPP) if included there).
- Each identified Systems Engineering Technical Review (SETR) event includes Systems Security Engineering (SSE) criteria (see Section 13.10.2 for amplification).

The Test and Evaluation Strategy (TES) provides an overall system Verification and Validation (V&V) strategy; and, pertinent details for ensuring system security are further discussed in Section 13.10.3. Expected Systems Security Engineering (SSE) content in the Test and Evaluation Strategy (TES) is highlighted as follows:

- Prototype/risk reduction testing that involves candidate critical functions and components and/or material countermeasures: In Part I (Introduction), Part II (Program Management and schedule), and Part III (Test and Evaluation Strategy (TES)).
- Long-lead post Milestone-B special-item resources, such as test range facilities and tools, for security requirements testing: In Part IV (Resource Summary).

Security requirements are first baselined in the System Requirements Document (SRD); related Systems Security Engineering (SSE) criteria and requirements are flowed down to contractor(s) via a solid Statement of Work and Request for Proposal (RFP) as follows:

- Expected Systems Security Engineering (SSE) content in the Request for Proposal (RFP) for the Technology Development (TD) phase (if available):
    - Request for Proposal (RFP) Section C:
        - Detailed Statement of Work requirements (see below).
        - System Requirements Document (SRD) is included (see below for level of detail expected).
    - Request for Proposal (RFP) Section L: Request a lifecycle description of the Systems Security Engineering (SSE) and Program Protection (PP) processes with how they integrate into the overall Systems Engineering (SE) process.
    - Request for Proposal (RFP) Section M: Evaluate proposed disciplined, structured Systems Security Engineering (SSE) and Program Protection (PP) processes, including Criticality Analyses (CA(s)) to inform the system specification and design, which mitigates threats and vulnerabilities to system/mission effectiveness.

- The Technology Development (TD) phase will involve prototyping efforts and system design trade-off considerations for risk reduction. Ensure that the Statement of Work requires the following level of Systems Security Engineering (SSE) activities from contractor(s) engaged in these activities:
    - Use and maintain current Critical Program Information (CPI) and critical function and component threat assessments (current within 2 years).
    - Update the Criticality Analysis (CA) to identify critical functions and components, with rationale, and to allocate countermeasures and sub-countermeasures to the system design, the allocated baseline, and to follow-on development efforts (e.g., the product baseline).
    - Flow down the Systems Security Engineering (SSE) requirements from the System Requirements Document (SRD) to the System Specification, with verification criteria for risk reduction efforts.
    - Refine the allocation of countermeasures and sub-countermeasures to system critical components (features included in system design) as well as lifecycle phases (processes used to develop the system).
    - Include detailed Systems Security Engineering (SSE) criteria for Systems Engineering Technical Reviews (SETRs), which should be reflected in their System Engineering Management Plan (SEMP).
        - Include coverage of Criticality Analysis (CA) results and supply chain risk information (see Section 13.10.2 for further details).
    - Include security requirements and critical function/component artifacts within their Systems Engineering (SE) and design Contract Data Requirements Lists (CDRLs).
    - Protection of all critical function and Critical Program Information (CPI)-related prototyping and preliminary design work during technology maturation efforts.
    - Demonstrate visibility into the supply chain for hardware and software elements to be used during the technology maturation efforts. Allow Government oversight reviewers to inspect results of Systems Security Engineering (SSE) processes (including countermeasures and Systems Security Engineering (SSE) activities) upon request.
- If an System Requirements Document (SRD) is available, the following Systems Security Engineering (SSE) considerations apply:
    - System Requirements Document (SRD) contains security requirements derived from:
        - Operational performance requirements requiring protection.
        - Security focused mission threads in the Concept of Operations (CONOPS).
        - Threats and vulnerabilities in the Initial Capabilities Documents (ICD) and draft Capability Development Documents (CDD).
    - System security requirements in the verification matrix should be traceable to Joint Capabilities Integration Development System (JCIDS) requirements (Initial Capabilities Documents (ICD), draft Capability Development Documents (CDD)) and regulatory requirements.
    - Includes system level countermeasures and sub-countermeasures

requirements.

13.14.2.2.2. Technology Development (TD) Phase

During the Technology Development (TD) phase, most of the Systems Security Engineering (SSE) related activities, criteria, and results can be mapped to content of the Milestone-B Program Protection Plan (PPP), as described in the Program Protection Plan (PPP) Outline. Associated Technology Development (TD) engineering analyses and Program Protection Plan (PPP) content include the material covered in Section 13.7.6, as well as the following:

- Perform an updated Criticality Analysis (CA), based on the previous Criticality Analysis (CA) results and current (within 2 years) threat and vulnerability data, in order to refine the mission-critical function list and identify critical components and potential subcomponents (hardware, software, and firmware)
    - Performed by the Government and/or contractor(s)
    - Employ Systems Security Engineering (SSE) protection fault isolation tree analysis and examine system response matrix for protection of Preliminary Design Review (PDR) level design
    - Use security scenarios in the operational Concept of Operations (CONOPS)
    - Identify logic bearing elements and failure effects for impact in order to assign criticality failure levels
    - Assign levels of criticality in order to prioritize critical functions and components for further analysis, focusing on Level I (Catastrophic) and Level II (Critical)
    - Identify rationale for inclusion or exclusion of critical functions and components in the list
    - Ensure that comprehensive program protection is fulfilled by the identification of critical components (completeness will comprise critical functions and components, critical information, and critical technology; indigenous/organic Critical Program Information (CPI) and inherited Critical Program Information (CPI))
- Identify program protection required to the level of specific countermeasures and sub-countermeasures, with plans for using mature technology
- Ensure that prototyping efforts and system design trade-off considerations for risk reduction focus on minimizing the attack surface and system security risks, and on employing affordable, risk-based countermeasures
- Use allocation to the Work Breakdown Structure (WBS) in order to refine the list of countermeasures and sub-countermeasures to be applied to each critical function and component
- Examine residual vulnerability rationale for residual risks and plan for threat and vulnerability residual risk assessments after sub-countermeasures have been applied
    - Use cost benefit trade-offs and other rationale
- Include provisions for evaluations of threats and countermeasure effectiveness at

each level of design

The threat analyses and plans/schedule to counter them, as captured in the Program Protection Plan (PPP), should correlate with and point to the discussion provided in paragraph 2.3 of the Acquisition Strategy (AS) (see the Technology Development Strategy (TDS)-Acquisition Strategy (AS) Outline).

Other key Systems Security Engineering (SSE) activities during the Technology Development (TD) phase, not necessarily captured in specific documents, include:

- Monitor contractor performance against the Systems Security Engineering (SSE) criteria for the Technology Development (TD) Statement of Work that were enumerated in Section 13.7.6.1
- Analyze intra- and inter-system dependencies and plan for corresponding mitigation of exploitable vulnerabilities that could compromise mission-critical system components
- Ensure that criticality analyses and the development and implementation of security requirements extends to multiple systems that support the end-to-end mission threads, including System of Systems (SoS)/Family of Systems (FoS) interdependencies
- For software prototyping and design trade analyses, include an updated evaluation of Software Assurance countermeasures that uses Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), and Common Weakness Enumeration (CWE)
- Ensure that Critical Program Information (CPI) and critical components are mature enough to fulfill related security requirements; i.e., those that are Critical Technology Elements (CTEs) (being matured to an assessed Technology Readiness Level (TRL) of 6 by Milestone B) demonstrate all required security in a relevant environment
- Consider Systems Security Engineering (SSE) in planning for the Engineering and Manufacturing Development (EMD) phase, including:
    - Inclusion of updated threats and vulnerabilities in the definition of operational environment for a Technology Readiness Level (TRL) of 7

Other documents generated during the Technology Development (TD) phase should also contain Systems Security Engineering (SSE) relevant content. For example, Systems Security Engineering (SSE) tasks to implement requirements should be included in the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS), including security verification tied to the Test and Evaluation Management Plan (TEMP) .

A thorough discussion of the Systems Engineering Plan (SEP), updated for Milestone B, is given in Chapter 4. Expected Systems Security Engineering (SSE) content in the updated Systems Engineering Plan (SEP) can be highlighted as follows:

- Updated description of Systems Security Engineering (SSE) within the overall

Systems Engineering (SE) approach, including processes used by the Government and contractors, as well as Technology Development (TD) phase Systems Security Engineering (SSE) accomplishments and guidance for Engineering and Manufacturing Development (EMD)
- Refinement and allocation of system level security requirements as part of the System Requirements process
- Technical baseline management for system security requirements at the System Requirements Document (SRD) and System Specification level by the Government and lower level specifications by the contractor(s)
- Technical Risk Plan includes a summary of the mission-critical components with risks, countermeasures and candidate sub-countermeasures, and residual risk (or a reference to Program Protection Plan (PPP))
- Comprehensive end-to-end test approach for system security
- Each identified Systems Engineering Technical Reviews (SETR) event includes Systems Security Engineering (SSE) criteria (see Section 13.7.6 for amplification)

The Test and Evaluation Master Plan (TEMP) provides an integrated system plan for Verification and Validation (V&V); and, pertinent details for ensuring system security are further discussed in Section 13.10.3. It should be noted, however, that the Test and Evaluation (T&E) associated with critical components and their testable sub-countermeasures will likely not be a part of a programs Test and Evaluation Management Plan (TEMP). A large portion of security Test and Evaluation (T&E) will be planned for and conducted by the contractor as part of the contracts Statement of Work. That said, expected Systems Security Engineering (SSE) content in the Test and Evaluation Management Plan (TEMP) is highlighted as follows:

- System security Developmental Testing (DT)
    - Key system security critical technical parameters (CTPs)
    - Verify system level security requirements as documented in the Requirements Verification Traceability Matrix (RVTM)
- System security Operational Testing (OT)
    - Include system security as a Measure of Suitability (MOS)
- Specific system security resources
    - Developmental Testing (DT)/Operational Testing (OT) test articles with sub-countermeasures
    - Test sites, instrumentation, and support equipment

Security requirements and related system functions are baselined in the Government System Requirements Document (SRD) and the contractors System Specification. Related Systems Security Engineering (SSE) criteria and requirements are flowed down to contractors via a solid Statement of Work and Request for Proposal (RFP) as follows:

- Expected Systems Security Engineering (SSE) content in the Request for Proposal (RFP) for the Engineering and Manufacturing Development (EMD) phase:

    - Request for Proposal (RFP) Section C:
        - detailed Statement of Work requirements (see below)
        - final System Requirements Document (SRD) is included (see below for level of detail expected)
    - Request for Proposal (RFP) Section L: Request a lifecycle description of the Systems Security Engineering (SSE) and Program Protection (PP) processes with how they integrate into the overall Systems Engineering (SE) process. Provide specific security scenario(s) for bidders to describe their proposed system response
    - Request for Proposal (RFP) Section M: Evaluate proposed disciplined, structured Systems Security Engineering (SSE) and Program Protection (PP) processes, including Criticality Analysis (CA), in system specification, detailed design, build/code, and test, with emphasis on countermeasure and sub-countermeasure implementation
- The Engineering and Manufacturing Development (EMD) phase Statement of Work should require the following level of Systems Security Engineering (SSE) activities from contractor(s):
    - Update the Criticality Analysis (CA) to refine the identification of critical functions and components, with rationale
    - Work with appropriate agencies (e.g., Defense Intelligence Agency (DIA) and National Security Agency (NSA)) to maintain Critical Program Information (CPI) and critical function and component threat assessments (current within 2 years)
    - Allocate sub-countermeasures to critical components and subcomponents (i.e., system detailed design and the product baseline) as well as to lifecycle phases for the processes used to develop the system.
    - For Software Assurance evaluations, use:
        - Common Vulnerabilities and Exposures (CVE) To identify vulnerabilities that enable various types of attacks
        - Common Attack Pattern Enumeration and Classification (CAPEC) To analyze environments, code, and interfaces for common destructive attack patterns
        - Common Weakness Enumeration (CWE) To examine software architectures, designs, and source code for weaknesses
    - Flow down the Systems Security Engineering (SSE) requirements from the System Requirements Document (SRD) to the System Specification and to lower-level specifications, with verification criteria for risk reduction efforts
        - Include detailed allocation of sub-countermeasures to lower-level specifications
    - Include detailed Systems Security Engineering (SSE) criteria for Systems Engineering Technical Reviews (SETRs), which should be reflected in the contractor Systems Engineering Management Plan (SEMP)
        - Include coverage of Criticality Analysis (CA) results and supply chain risk information (see Section 13.10.2 for further details)
    - Include security requirements and critical function/component artifacts

within contractor Systems Engineering (SE) and design Contract Data Requirements Lists (CDRLs)
    - Demonstrate visibility into the supply chain for critical components and subcomponents. Allow Government oversight reviewers to inspect results of Systems Security Engineering (SSE) processes (countermeasures, sub- countermeasures, and activities) upon request
- Expected Systems Security Engineering (SSE) content in the System Requirements Document (SRD) and/or preliminary System Specification:
    - Specific security requirements to protect Critical Program Information (CPI) and critical functions and components, based on:
        - Operational performance requirements needing protection
        - Threats and vulnerabilities identified via system-specific assessments as well as those contained in the Capability Development Document
        - Use cases (including common-attack countermeasures) that are comprehensive and traceable to the Concept of Operations (CONOPS)
    - Each security requirement in the verification matrix should be traceable from Joint Capabilities Integration Development System (JCIDS) requirements (Initial Capabilities Document (ICD) and Capability Development Document (CDD)) to countermeasures and sub-countermeasures allocated to system requirements, and adjusted for associated cost, risk, and schedule
    - Identification of specific countermeasures and sub-countermeasures requirements. For example, for Software Assurance countermeasures to be applied to a specific component, the identification of sub-countermeasures, such as:
        - Static code analysis (for development process application)
        - Secure exception handling (for built-in component security)
        - Sandboxing (for operational threat mitigation)
    - All identified Critical Program Information (CPI) and critical functions and components have specified countermeasure and sub-countermeasure requirements documented in the contractors Spec Tree, with justification of accepted risk

The contractors preliminary Subsystem and Component Specifications should:

- Contain derived system protection requirements that are comprehensive, verifiable, and traced from the System Requirements Document (SRD)
- Provide security and protection verification matrices that are traced and properly allocated from the System Requirements Document (SRD) so that system level protection requirements can be validated
- Reflect the trade-off analysis of the Preliminary Design Review (PDR) with respect to Criticality Analysis (CA), mission-critical functions and components, countermeasures and sub-countermeasures, updated vulnerability assessment,

and allocation of sub-countermeasures to design and verification

13.14.2.2.3. Engineering and Manufacturing Development (EMD) Phase

During the Engineering and Manufacturing Development (EMD) phase, most of the Systems Security Engineering (SSE) related activities, criteria, and results can be mapped to content of the Milestone-C Program Protection Plan (PPP), as described in the Program Protection Plan (PPP) Outline. Associated Engineering and Manufacturing Development (EMD) engineering analyses and Program Protection Plan (PPP) content include the material covered in Section 13.7.6 , as well as the following:

- Perform an updated Criticality Analysis (CA), based on the previous Criticality Analysis (CA) results and current (within 2 years) threat and vulnerability data, in order to refine the list of critical components and subcomponents (hardware, software, and firmware) for comprehensive protection
    - Verify threat and vulnerability assessments are current against the product baseline and system operational concept
    - Identify rationale for inclusion or exclusion of system components and subcomponents in the list
- Update the threat and residual vulnerability risk assessment(s), consistent with the updated Criticality Analysis (CA) summary and rationale
    - Ensure that threat and vulnerability residual risk assessment after sub-countermeasures are applied have been tracked and mitigated
- Update the software evaluations using Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), and Common Attack Pattern Enumeration and Classification (CAPEC)
- Update the identification of countermeasures and sub-countermeasures to be applied to specific critical functions and components
- Ensure, prior to Milestone C, that all Critical Program Information (CPI) and mission-critical functions and components are identified, together with all associated Systems Security Engineering (SSE) countermeasures and sub-countermeasures applied to them
- Assess Critical Program Information (CPI) and critical function/component countermeasures and sub-countermeasures for production, deployment, operations, and sustainment
    - Ensure countermeasures and sub-countermeasures have been integrated into the product baseline, production planning, and system operational concept
    - Ensure completeness, comprising critical functions/components/subcomponents, critical information, and critical technology, Indigenous/Organic Critical Program Information (CPI) and Inherited Critical Program Information (CPI)
- Apply residual vulnerability risk assessment after sub-countermeasures applied
- Examine verification results (Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E)) for security requirements
- Ensure that Systems Security Engineering (SSE) requirements flow down to

detailed design elements with verification criteria:
    - Allocate sub-countermeasures to counterintelligence (CI) Specifications (detailed design) and to verification criteria in the Statement of Work
    - Update the Systems Security Engineering (SSE) protection fault isolation tree and system response matrix
    - Ensure flow down of key Systems Security Engineering (SSE) requirements to appropriate Systems Engineering Technical Reviews (SETR) criteria (Critical Design Review (CDR), Test Readiness Review (TRR), and System Verification Review (SVR)) (see Section 13.10.2 for amplification)

Other key Systems Security Engineering (SSE) activities during the Engineering and Manufacturing Development (EMD) phase include:

- Monitor contractor performance against the Systems Security Engineering (SSE) criteria for the Engineering and Manufacturing Development (EMD) Statement of Work that were enumerated in Section 13.13.1.2
- Ensure that criticality analyses and the implementation and testing of security requirements extends to multiple systems that support the end-to-end mission threads, including System of Systems (SoS)/Family of Systems (FoS) interdependencies
- Update the residual risk assessment after sub-countermeasures have been applied, examine residual vulnerabilities for prioritized risks, and apply mitigations and plans that will ensure system security through deployment and operations
- Ensure that system security is properly reflected in the product baseline and in production planning for Low rate initial production (LRIP) and beyond
    - Systems Security Engineering (SSE) requirements flow down to the product baseline, with application of sub-countermeasures to subcomponents verified and validated
    - Ensure that the Lifecycle Sustainment Plan includes periodic assessment of threats, vulnerabilities, and maintenance of countermeasures and sub-countermeasures
    - Ensure that the sustainment strategy contains sustainment related contracts to ensure secure supply chain acquisitions correlated with paragraph 7.4.3.6 of the AS (see the Technology Development Strategy (TDS)-Acquisition Strategy (AS) Outline)
    - Ensure that all security-related logic bearing subcomponents have viable contractors
- Specify the impact upon program cost due to program protection and exportability features associated with the potential/plans for Foreign Military Sale correlated with paragraph 10.3 of the AS (see the Technology Development Strategy (TDS)-Acquisition Strategy (AS) Outline)
- Ensure that Critical Program Information (CPI) and critical components and subcomponents are matured to fulfill related security requirements; i.e., those that are Critical Technology Elements (CTEs) (being matured to an assessed

Technology Readiness Level (TRL) of 7 by Milestone C) demonstrate all required security in an operational environment
    - Verify manufacturability of needed sub-countermeasures
- Ensure verification of system protection functional requirements:
    - Systems Security Engineering (SSE) functional requirements flow down to detailed design elements and are verified against valid criteria and verification methods
    - Countermeasures and sub-countermeasures are analyzed and tested throughout the detailed design and testing/verification phases
    - Physical and operational countermeasures and sub-countermeasures are included in system operational instructions and training documentation
    - Configuration management system is used to track vulnerability risks and mitigation via design changes
    - Performance of sub-countermeasures is verified against attacks
    - Updated test plans and procedures reflect additional verification requirements and stress attack scenarios
- Ensure that Systems Security Engineering (SSE) tasks to implement requirements are updated in the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS)

Other relevant Engineering and Manufacturing Development (EMD) documents include the contractors Test Plans. Expected Systems Security Engineering (SSE) content includes:

- Test Plan activities are traced from the System Requirements Document (SRD) to system, subsystem, and lower-level component requirements, to verification testing needs
- Ensure that all Systems Security Engineering (SSE) testing requirements from system, subsystem, component, and subcomponent level documentation are included in the verification matrix according to agreed verification objectives
- Clear pass-fail criteria are identified for all tests as they apply to system security and protection
- Test processes and facilities, test equipment, Modeling and Simulation (M&S), and the software environment are adequately planned to validate protection countermeasure requirements
- Systems Security Engineering (SSE)-specific needs for personnel and schedule are considered and adequately addressed
- Test plans reflect the Test and Evaluation Management Plan (TEMP)
- Testing includes attack stress use cases
- Security and protection validation testing may require outside accreditation authorities, and appropriate schedule is allocated in the Test Plans

13.14.3. Security Engineering for International Programs

System Security Engineering should include an assessment of security criteria that sets limits for international cooperative programs, direct commercial sales, and/or foreign

military sales cases. From this assessment, engineering and software alternatives (e.g., dial-down functionality, export variants, anti-tamper provisions, etc.) should be identified that would permit such transactions.

13.15. Program Protection Plan (PPP) Review/Approval

Program Protection Plan (PPPs) must be approved by the Milestone Decision Authority at Milestones A, B, C, and the Full-Rate Production decision (or business system equivalent). A final draft Program Protection Plan (PPP) must be submitted for the Pre-Engineering and Manufacturing Development (EMD) review prior to Milestone B. This guidance summarizes the approval process that Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and DoD Chief Information Officer (CIO) jointly developed for programs under their cognizance. Programs under Component, Program Executive Office (PEO), or other oversight should consult their Milestone Decision Authority (MDA) for applicable approval guidance.

The Program Protection Plan (PPP) Review and Approval Process should be initiated approximately 180 days prior to the programs Defense Acquisition Board (DAB) to allow sufficient time for the comprehensive Office of the Secretary of Defense (OSD) review. The review process iterates as the program responds to Office of the Secretary of Defense (OSD) comments and resubmit' s the Program Protection Plan (PPP) for approval. Once all comments are resolved, the Program Protection Plan (PPP) will be coordinated and routed to the Milestone Decision Authority (MDA) for approval.

13.15.1. Review Process

When a Program Protection Plan (PPP) is ready for Office of the Secretary of Defense (OSD) review, the program will send the document to Deputy Assistant Secretary of Defense (Systems Engineering) (DASD (SE)) Major Program Support (MPS) Program Support Team Lead (PSTL) and Action Officer (AO). The Program Protection Plan (PPP) will be reviewed by SMEs across Office of the Secretary of Defense (OSD) to validate that the Program Protection Plan (PPP) sufficiently addresses all aspects of program protection planning and implementation. If comments are generated, consolidated comments from this comprehensive review are returned to the program for adjudication and resubmission for approval.

An important lesson learned is the program should act early to engage the Component Anti-Tamper community and address any concerns, as Anti-Tamper (AT) Plan approval is commonly a holdup for overall Program Protection Plan (PPP) approval. Additionally, Program Managers (PMs) may delay receiving Program Executive Office (PEO) or Service Acquisition Executive (SAE) signatures on Program Protection Plans (PPPs) prior to initial Office of the Secretary of Defense (OSD) reviews, as many initial reviews generate comments requiring rework that may need to be re-approved at those levels.

13.15.1.1. Program-Level View of Program Protection Plan (PPP) Review Process

The program sends the draft Program Protection Plan (PPP) to its Program Support Team Lead (PSTL) and Action Officer (AO). Approximately three weeks later, the program will receive a comments matrix from the Program Support Team Lead (PSTL)/ Action Officer (AO) with comments the program needs to address. After addressing the comments, the program will submit an updated Program Protection Plan (PPP) with the adjudicated comments matrix to the Program Support Team Lead (PSTL) and Action Officer (AO). Once all comments have been addressed, the Program Protection Plan (PPP) Review Team will coordinate and staff the Program Protection Plan (PPP) for a Milestone Decision Authority (MDA) signature. Once it is signed, the approved Program Protection Plan (PPP) will be sent back to the program.

13.15.2. Reviewing Organizations

- Deputy Assistant Secretary of Defense (Systems Engineering) (DASD (SE)) from a systems engineering perspective
- DoD Anti-Tamper Executive Agent (ATEA) from an Anti-Tamper (AT) perspective
- DoD Chief Information Officer (CIO) from an Information Assurance and supply chain perspective
- Acquisition, Technology, and Logistics (AT&L) Industrial Policy from a supply chain perspective
- Under Secretary of Defense (Intelligence) from security and counterintelligence perspective
- Acquisition, Technology, and Logistics (AT&L) International Negotiations from an international cooperation perspective

13.15.3. Approval Process

13.15.3.1. Coordination

Once all Office of the Secretary of Defense (OSD) comments are adjudicated, the Program Protection Plan (PPP) is then sent out for Principal-level coordination across Office of the Secretary of Defense (OSD). The following organizations submit Principal-level coordination:

- DoD Anti-Tamper Executive Agent (ATEA)
- DoD Chief Information Officer (CIO)
- Acquisition, Technology, and Logistics (AT&L) Industrial Policy
- Acquisition, Technology, and Logistics (AT&L) International Negotiations
- Acquisition, Technology, and Logistics (AT&L) Acquisition Resources & Analysis
- Acquisition, Technology, and Logistics (AT&L) Strategic & Tactical Systems
- Office of the General Counsel

Once coordination is complete, the Program Protection Plan (PPP) is routed to the

Milestone Decision Authority (MDA) for signature.

13.15.3.2. Approval Authority

The approval authority for Program Protection Plans (PPPs) is the Milestone Decision Authority (MDA). The Milestone Decision Authority (MDA) for Acquisition Category (ACAT) ID, special interest, and non-delegated Acquisition Category (ACAT) IAM programs, is Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DoD Chief Information Officer (CIO) is the Milestone Decision Authority (MDA) for all other IAM programs . For Acquisition Category (ACAT) ICs and below, the Program Protection Plan (PPP) does not need to be reviewed at the Office of the Secretary of Defense (OSD) level.

13.16. Program Protection Plan (PPP) Classification Guidance

The Program Protection Plan (PPP) should be classified by content. There is no overarching Security Classification Guide for DoD Program Protection original classification authority for Critical Program Information (CPI), mission-critical functions and components, threats and vulnerabilities to those items, and protections of those items remain the responsibilities of their respective owners. Program Protection Plans (PPPs) are frequently developed with unclassified bodies and classified appendices as necessary.

DEFENSE ACQUISITION GUIDEBOOK
Chapter 14 - Acquisition of Services

14.0. Overview

14.0.1. Purpose

This chapter provides acquisition teams with a disciplined, three-phase, seven step process, for the acquisition of services.

14.0.2. Contents

14.1. Introduction to the Acquisition of Services

The acquisition of services plays a vital role in advancing and maintaining the mission capability of the Department of Defense (DoD). Services acquisition covers a broad spectrum of requirements from research and development, advisor services, information technology support, medical, to maintaining equipment and facilities. For over ten years the DoD has spent more on service requirements than it has on equipment acquisitions. While the acquisition of major systems follows a much defined process, the acquisition of services tends to be more ad hoc. Services acquisition is not about awarding a contract; it's about acquiring performance results that meet performance requirements needed to successfully execute an organization's mission.

This guidebook provides acquisition teams with a disciplined, seven step process, for the acquisition of services. Applying this rigorous and systematic approach requires the dedicated effort of an acquisition team composed of functional experts, contracting specialists, contracting officer representatives, and others working together to achieve performance results and value their mission requirements. It's important to remember that the Federal Acquisition Regulation (FAR) states that the acquisition process is a shared team responsibility. Completing this process, like all acquisitions, takes allocated planning time. Getting your acquisition team organized and focused early in the process is a fundamental key to successfully achieving the mission results your customer's require.

14.1.1. The Services Acquisition Process

When does the process start? It starts with a valid mission requirement for a service essential for the successful execution of the organizations mission. The process continues through a planning phase, which develops the foundation for defining your requirement and business strategy, and ultimately ends with the delivery and

assessment of the services provided.

The service could be provided by a new contract you develop; it could be provided by an already existing contract within your agency (or outside your agency); or could be part of your Agency's strategic sourcing efforts. The services acquisition process requires that you keep an open mind about where best to source the requirement until you have explored and assessed all the alternatives and developed a clear picture of the requirement and supporting acquisition strategy.

The services acquisition process has three phases.

Planning Phase:

Step One: Form the Team

Step Two: Review Current Strategy

Step Three: Market Research

Development Phase:

Step Four: Requirements Definition

Step Five: Acquisition Strategy

Execution Phase:

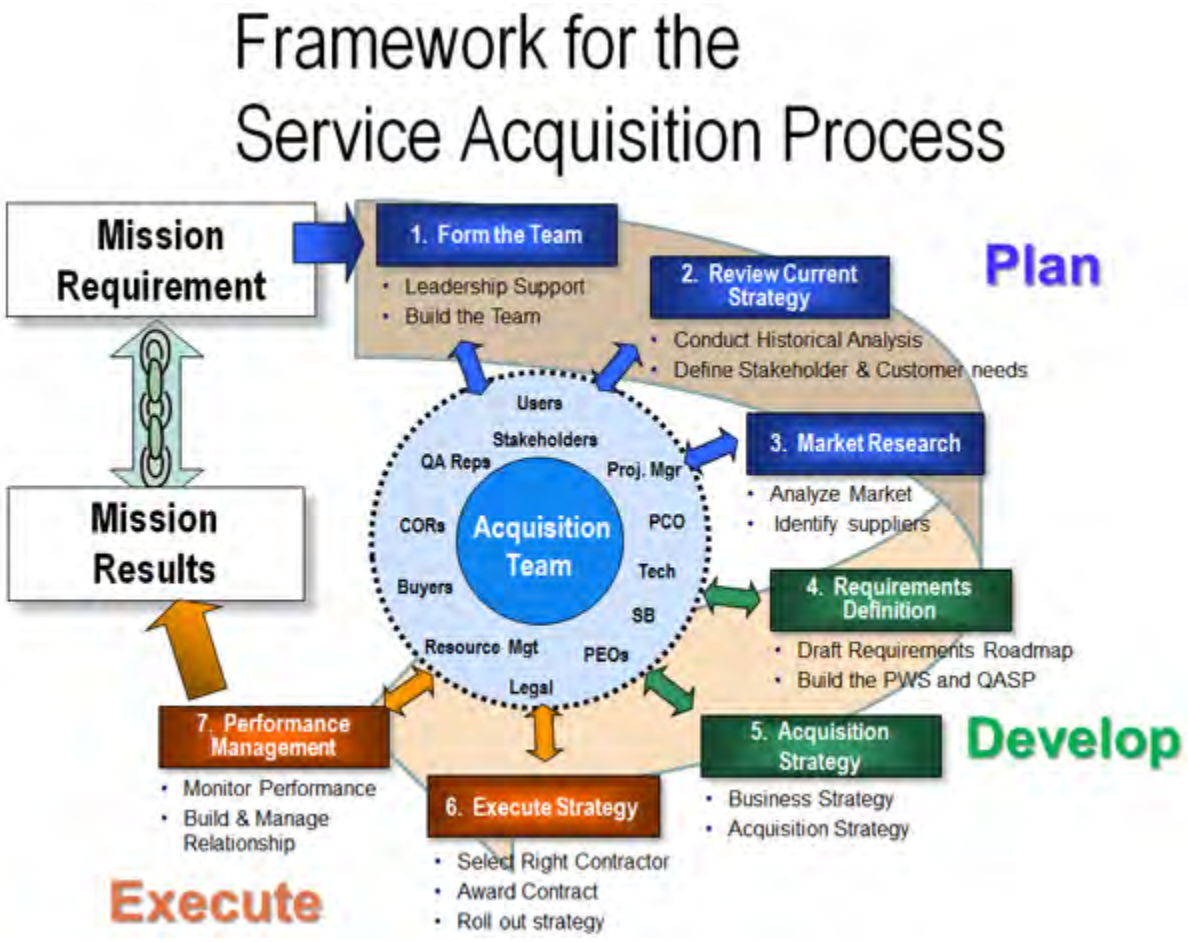
Step Six: Execute Strategy

Step Seven: Performance Management

Each phase builds on the knowledge gained in the previous phase. Some actions within each phase can be completed in parallel; others should be completed sequentially to make more informed decisions based on new knowledge gained. The project plan in Appendix B will help you tailor a plan for your service acquisition. This guidebook will cover each of the steps in detail and illustrate how to use the requirements roadmap tool to assist you in developing performance-based requirements documents.

The process is pictured below in Figure 14.1.1.F1.

Figure 14.1.1.F1. The Services Acquisition Process



The **Planning Phase** , steps 1, 2, and 3, lays the foundation for action. During the planning phase, you form the acquisition team and get leadership support for all the actions that must happen to ensure the mission is supported. Baseline and analyze your current service strategies; identify problem areas and projected mission changes; and get your stakeholders to define their key performance outcomes for this requirement. Also analyze the market place to assess current technology and business practices, competition and small business opportunities, existing and potential new sources of providing the service, and determine if commercial buying practices can be adapted.

During the **Development Phase** , steps 4 and 5, use the requirements roadmap process to define your High Level Objectives and tasks, standards, allowable variations, and method of inspection. After completing the roadmap you will then be in the best position to develop a performance work statement (PWS) and quality assurance surveillance plan (QASP) . During this phase you will also identify your funding sources, develop a government estimate of contract price for the required service, and get industry feedback on your working documents. Finally, synthesize an acquisition strategy that leverages contract type and performance incentives to deliver a best value

mission performance to the customer. The basic performance principle is to tell the contractor what the performance results are, not how to do the job. Let industry develop the solution.

In the **Execution Phase** , steps 6 and 7, you put all your planning and development efforts into action. You create a solicitation document that formally communicates to industry your requirements and strategy. You receive contractor proposals for how they will meet your performance results and standards and then evaluate them against criteria selected that will best determine the success of a potential contractors approach. After contract award, the business relationship you have with the service providing contractor should foster innovation and improvements to mission performance outcomes. This part of the process involves two key areas: administering contract requirements such as invoicing and payments; and managing the relationships and expectations of both the contractor and customer's in meeting the terms of the contract and achieving the required mission performance results. You also start the planning phase for a follow-on acquisition if there is a continuing need for the service being provided.

14.1.2. What is a Service Requirement?

A service requirements primary purpose is to perform an identifiable task rather than furnish an end item of supply. It's primary purpose directly engages a contractors time and effort. A service requirement may be either non-personal or personal and performed by professional or nonprofessional workers whether on an individual or organizational basis. Some of the areas in which service requirements are found include the following:

- Maintenance, overhaul, repair, servicing, rehabilitation, salvage, modernization, or modification of supplies, systems, or equipment
- Routine recurring maintenance of real property
- Housekeeping and base services
- Advisory and assistance services (A&AS)
- Operation of government-owned equipment, facilities, and systems
- Communication services
- Architect-engineering (see FAR part 36.6)
- Transportation and related services (see FAR part 47)
- Research and development (see FAR part 35)

For DoD, the various types of services are grouped into portfolio categories within the taxonomy for the acquisition of services (reference DFARS Procedures, Guidance, and Instruction PGI 237.102-74). The contracting officer is responsible for determining whether the services needed are non-personal or personal using the definitions found in FAR 37.101 and 37.4 and the guidelines found in FAR 37.104 . Agencies **shall not** award personal service contracts unless specifically authorized by statute to do so.

14.1.3. Non-Personal Services Requirements

Non-personal service means that the personnel rendering the services are not subject, either by the contracts terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the government and its employees. Non-personal service contracts are authorized by the government in accordance with FAR 37.102 , under general contracting authority, and do not require specific statutory authorization.

14.1.4. Personal Services Requirements

A personal service is characterized by the employer-employee relationship it creates between the government and the contractors personnel. The government is normally required to obtain it's employees by direct hire under competitive appointment or other procedures required by the civil service laws. Obtaining personal services by contract, rather than by direct hire, circumvents those laws unless Congress has specifically authorized acquisition of the services by contract as indicated in FAR 37.104 .

In a personal services contract, the contractor is considered to be, and is treated as, an employee of the government. In this type of relationship, a government officer or employee directly supervises and controls the contractors personnel on a continuing basis. Personal service contracts require specific authorization.

14.1.5. Preference for Performance-Based Acquisitions (PBA) for Services

The FAR, in implementing Public Law 106-398, states that performance based acquisition methods should be used to the maximum extent practicable. PBA for services involves performance requirements and acquisition strategies that describe and communicate measurable outcomes rather than direct specific performance processes. It is structured around defining a service requirement in terms of performance results and providing contractors the latitude to determine how to meet those objectives. Simply put, it is a method for acquiring *what results are required* and placing the responsibility for *how it is accomplished* on the contractor.

To be considered performance-based, an acquisition should contain, at a minimum, the following elements:

- Performance Work Statement (PWS) - Describes the requirement in terms of measurable outcomes rather than by means of prescriptive methods.
- Measurable performance standards -Determines whether performance outcomes have been met; defines what is considered acceptable performance.
- Incentives / Disincentives - Addresses how to manage performance that does not meet (or exceed) performance standards. While not mandatory, incentives should be used, where appropriate, to encourage performance that will exceed performance standards. Incentives can be both monetary and non-monetary.
- Quality Assurance Surveillance Plan (QASP) - Describes how the government

will assess contractor performance against the performance standards contained in the PWS.

14.1.6. Objectives of Performance-Based Acquisition (PBA)

By describing requirements in terms of performance outcomes, agencies can help achieve the following objectives:

Maximize performance: Allows a contractor to deliver the required service by following its own best practices. Since the prime focus is on the end result, contractors can adjust their processes, as appropriate, through the life of the contract without the burden of contract modifications, provided the delivered service (outcome) remains in accordance with the contract. The use of incentives further motivates contractors to continue to exceed minimum contract performance requirements.

Maximize competition and innovation: Encouraging innovation from the supplier base by using performance requirements maximizes opportunities for competitive alternatives in lieu of government-directed solutions. Since PBA allows for greater innovation, it has the potential to attract a broader industry base.

Encourage and promote the use of commercial services: The vast majority of service requirements are commercial in nature. FAR Part 12 (Acquisition of Commercial Items) applies to the acquisition of commercial services and provides procedures that offer the benefit reducing the use of government-unique contract clauses and similar requirements, which can help attract a broader industry base. However, it is often the case that commercial services will be acquired through contracts awarded under FAR Part 15 (Contracting by Negotiation) given the limited contract types authorized under FAR Part 12.

Shift in risk: Much of the risk is shifted from the government to industry, since contractors become responsible for achieving the performance results contained in the Performance Work Statement through the use of their own best practices and processes. Agencies should consider this shift in responsibility in determining the appropriate acquisition incentives and contract type.

Achieve savings: Experience in both government and industry has demonstrated that use of performance requirements results in cost savings.

14.1.7. Principles of Performance-Based Acquisition (PBA) for Service Requirements

PBA is not a new procurement strategy. Many procurement activities have never stopped using PBA techniques. The Department of the Navy, as one example among many, has used PBA techniques effectively for facilities maintenance services for decades. The Department of the Air Force and the Army Corps of Engineers has

employed PBA techniques in many of their service acquisitions.

PBA techniques are applicable to a broad range of service requirements. Simply stated, PBA methods structure a contract around the contractor achieving stated performance results and standards. The contractors performance against the required standards must be measurable through an objective process. This means that the government acquisition team must describe the required performance results in clearly defined terms with performance standards that can be effectively measured. This is often the most difficult part of implementing PBA techniques. Writing a Performance Work Statement in a way that describes performance results requires us to focus on the relationship between what needs to be done and how well it must be accomplished, not how it must be accomplished or how many full-time equivalents (FTEs) are required. When PBA techniques are not appropriate for use, the decision shall be documented and included in the contract file.

Let's examine a couple of examples of writing a requirement that focus on achieving a specified outcome rather than how to perform the function. The Navy decided to outsource it's ordering, inventory management, and delivery of aircraft tires. They could have developed a detailed specification on how to order, inventory, and deliver aircraft tires. What the Navy did was to review what performance outcomes the fleet needed to support aircraft operations around the world. Through this review and analysis they developed the following performance objectives, performance standards, and acceptable level of deviation depicted in Table 14.1.7.T1.

Table 14.1.7.T1. Performance Outcomes

Performance Objective	Performance Standard	AQL or Tolerance
Deliver any Navy aircraft tire required within CONUS	Within 48 Hours	95% On Time
Deliver any Navy aircraft tire required outside the CONUS	Within 96 Hours	95% On Time

With this simple set of performance outcomes, contractors were given wide latitude to develop an ordering, inventory, and delivery methodology to support Navy flying operations. Through the innovation introduced by industry the Navy achieved the following benefit's:

- $3M per year in supply chain management savings
- Reduction from approximately 1.5 years wholesale inventory to three months
- Reduction from 60 days to 15 days retail inventory at all Continental United States (U.S.) (CONUS) Naval Air Stations
- Response times reduced to two days in U.S., four days outside CONUS (OCONUS)
- On-time delivery improvement from 81% to 99+%

- Over $49 million net savings to the Navy over life of contract

Another example of the challenges you'll face in developing performance outcomes is illustrated by an example from the Corps of Engineers. The Corps had developed a comprehensive Statement of Work (SOW) for a dredging requirement. It specified where to dredge, how to dredge, when to dredge, and provided little opportunity for innovation; after all it's just dredging, right. So let's step back and try to understand what the real requirement was. Why was the dredging required? Was that the real requirement? Isn't dredging a process to achieve an objective or outcome? After some prolonged and heated discussion, they determined that the dredging was required so that shipping could proceed through a specified channel without underwater obstructions. In other words keeping the channel open was their performance objective, not dredging.

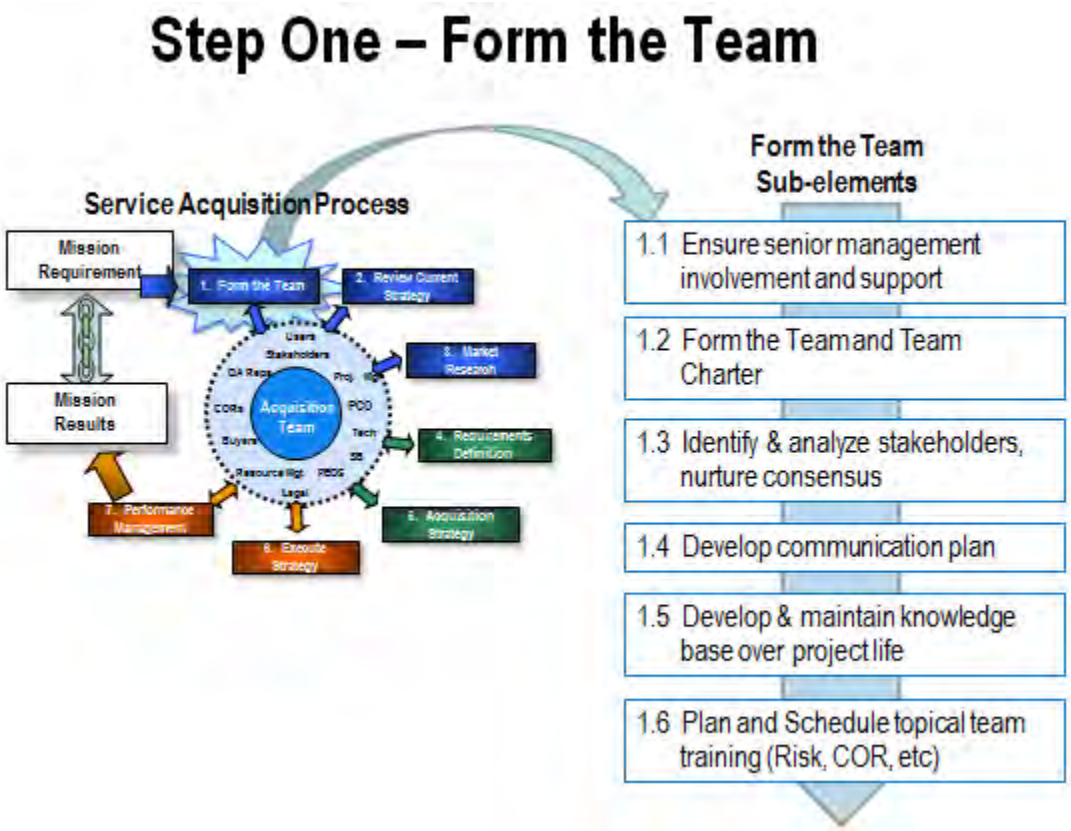
With this new focus, the next question was how well or to what standard must the channel be kept (not dredging)? The answer was 100 feet wide and 12 feet deep mean low water. Now they had a performance standard, but how would they know if the contractor was meeting that performance standard? Their answer was providing a boat with a global positioning system (GPS) and sonar system that could measure depth and position to ensure the channel met the specified standard. With their new performance objective, performance standard, and a means of inspection, they were well on their way to developing a simpler, more performance-based requirement.

No matter where you are in the services acquisition process, it's very easy to get trapped into a preconceived idea of how a particular function should or must be performed. Like the examples cited above, you need to keep the focus on what mission outcomes you are trying to achieve, not how the process must be accomplished. If you can keep a higher view of what you're asking a contractor to accomplish, you will have far more success in implementing a performance-based approach for your service requirements.

14.2.1.6. Plan and Schedule Topical Team Training

14.2. The Planning Phase

Figure 14.2.1.F1. Model of Step One



14.2.1. Step One Form the Team

The acquisition team should be a customer-focused, multi-functional team that plans and manages the service requirement throughout its life cycle. We will refer to the multi-functional team as the acquisition team during this guide. The requirement may be for a single function or for multiple functions. Estimated dollar value is not the sole determinant of the amount of effort devoted to the acquisition. Previously, it was common for contracting and other functional experts to work independently in functional stove pipes when acquiring services. This method is outdated and costly. Service acquisition requires a team effort. It is essential that all stakeholders be involved throughout the service acquisition life cycle, from the planning and development phase through the execution phase. The duties, expertise, and contributions of each team member are important to the success of any service acquisition. Many functional experts should make up an acquisition team.

14.2.1.1. Ensure Senior Management Involvement and Support

Early in your acquisition efforts you should make sure you've got senior leadership support. It is important to understand leaderships concerns and expectations for your acquisition. What priority does this requirement have in their portfolio of service requirements? Your leadership can help you get the right people on your team and overcome roadblocks when necessary when they understand your team is committed to the success of their mission.

14.2.1.2. Form the Team and Team Charter

The goal of every acquisition team should be to obtain quality, timely contract services in both a legal and cost-effective manner, placing the responsibility for quality performance on the contractor. Nonetheless, achieving this goal can be challenging. The interdisciplinary nature of your acquisition efforts means no single individual or function is likely to have all the requisite knowledge and experience in the majority of cases. Therefore, personnel such as the program manager, contracting officer, contracting officer's representative (COR), responsible fiscal officer, and legal counsel (among others) should form the acquisition team as soon as possible in order to:

- Develop a team vision and charter for the acquisition.
- Develop an effective level of dialogue and teamwork.
- Analyze stakeholders and create a communication plan.
- Develop a project plan and the timeline for the acquisition. A project plan provides the detail of what has to be accomplished and who is responsible to accomplish each task.

Although the composition of the acquisition team may vary depending on the nature of the requirement, a few key members are essential to the success of any contract. They are as follows:

The Customer/User: The customer's representative or functional manager normally brings to the team detailed knowledge of the user requirements. They are responsible for defining the required performance outcomes or results. The requirements definition most likely will include an assessment of the risk that the government might assume when relying on commercial specifications and common marketplace performance and quality standards. The customer/user plays an important role in deciding what tradeoffs are necessary when considering a commercially available service to fulfill an agency requirement. Your customer/user is the key individual in determining the organizations needs and in providing the historical data and perspective.

Program Manager/Technical Specialist/Project Manager: The program manager (PM) is the acquisition team leader and is responsible for ensuring that the acquisition plan is properly executed and the desired results are achieved. The PM provides coordination and facilitates communication among the acquisition team members, closely tracks the milestone schedule, and provides leadership and guidance to overcome and resolve

any problems or delays. This individual is responsible for drafting the PWS, which means ensuring that performance requirements are clearly and concisely defined and articulated. PMs identify, plan, and control various areas, such as delivery requirements, scheduling, market research, COR nomination, cost estimating, budgeting, and specific project formulation. The PM normally participates in the source selection as well. This individual serves as the principal technical expert, is most familiar with the requirement, best able to identify potential technical tradeoffs, and whether the requirement can be met by a commercial solution.

The Contracting Officer: The warranted contracting officer is responsible for performing all relevant contract functions, to include assisting in requirements development and market research. Within this context, the contracting officer does not determine the government's need, but is responsible for advising the PM in preparing a PWS. This individual serves as the principal business advisor and principal agent for the government responsible for developing the business strategy, solicitation, conducting the source selection, and administrating the resultant contract and business arrangement.

Performance Assessment Personnel (Quality Assurance Personnel): Performance assessment personnel are known by many names, such as COR, or quality assurance evaluator (QAE), but their duties are essentially the same. They serve as the on-site technical manager responsible for assessing actual contractor performance against contract performance standards. The COR provides the team with their field experience and surveillance of service contracts (Frequently, this individual is the same person who initiates the program requirements and normally serves as the primary person responsible for assessing performance). They provide guidance to the PM to ensure contract requirements are described in a manner which enables the government to objectively and effectively assess the contractors work performance in terms of outcome. They serve as the "eyes and ears" of the contracting officer and when applicable, the COR performs the actual surveillance of the contractor's work. A letter of appointment signed by the contracting officer provides scope and limitations of the CORs authority.

Small Business Specialist (SBS): The SBS serves as the principal advisor and advocate for small business engagement. This individual serves as the chief analyst on small business laws, regulations and command policy. They can provide insight for market research and an understanding of industry small business capability. He or she may also serve as the liaison with the Small Business Administration (SBA).

Cost/Price Analyst: The cost/price analyst evaluates the financial price and cost-based data for reasonableness, completeness, accuracy, and affordability. Alternatively, some agencies utilize cost engineering personnel from within an engineering division to conduct cost/price analysis from a technical standpoint.

Finance/Budget Officer: The finance/budget officer serves as an advisor for fiscal and

budgetary issues.

Legal Advisor: The legal advisor ensures that the commercial practices, and terms and conditions contemplated are consistent with the governments legal rights, duties, and responsibilities; will review the acquisition documents for legal sufficiency; and provides advice on acquisition strategies and contract terms to the PBA team.

Miscellaneous Others: In addition to individuals mentioned above, personnel from outside the agency may also be useful, depending on their area of expertise. This includes individuals from agencies such as the Defense Contract Management Agency, Defense Logistics Agency, the Defense Contract Audit Agency, and the Environmental Protection Agency, to name a few.

Team Charter and Vision Statement:

Developing a team charter is an important step in getting the team focused on the objectives to be accomplished and to assign key roles and responsibilities. Everyone involved must understand how they will contribute to achieving the required mission results. The charter starts with the acquisition teams vision statement. The vision statement should capture the high level objective of the teams effort and be an objective that unites the team.

Use the project plan (Appendix B) and tailor it for your specific acquisition. This will help you identify all the actions needed to complete each step of the seven step process. It also enables you to assign responsibility for specific actions and develop a time line for how long it will take you to get to performance management. Examples of a team charter and project plan are available in the Service Acquisition Mall (SAM, Appendix C) (http://sam.dau.mil/).

14.2.1.3. Identify and Analyze Stakeholders, Nurture Consensus

Every acquisition has stakeholders. Your acquisition team should identify who are the key stakeholders that will be impacted by your acquisition. Stakeholders often fall into three major categories:

Internal - These are within your organization either as customer’s for the service being procured or leaders of activities your effort will be supporting.

Governance These are individuals or organizations that must approve your requirement and acquisition strategies. They are often at higher headquarter levels outside your immediate organization. Their involvement is often dictated by agency policy.

External These are stakeholders not directly tied to your acquisition. They can be local communities, industry, or anyone else who might be affected or have an interest in your actions.

14.2.1.4. Develop a Communication Plan

Once you have identified your key stakeholders, how will you communicate with them and keep them advised of your progress? A communication plan is a good way to target specific communications to specific stakeholders. Well informed stakeholders can be effective advocates for your actions. Your communication plan should determine the method and frequency of communications. The Communication Plan is a living document and should also be adjusted over time as new stakeholders are discovered and you move through the different phases of the service acquisition process.

14.2.1.5. Develop and Maintain Knowledge Base over the Project Life

Depending on the size and complexity of your service requirement it can take up to two years from this point in the process to step seven where you are finally receiving the service. During this period team members will leave and new ones arrive. It's important for the new team members to understand the decisions that have been made and the rationale that supported them. That's why developing a project library that can be easily shared among the acquisition team, will help new team members get on board quickly and provide everyone with a common understanding of the project and decisions made.

14.2.1.6. Plan and Schedule Topical Team Training

As part of your project plan identify which individuals will need specialized training such as for the COR or for individuals involved with your source selection. Consult current DoD directives for COR training requirements. Also consider requesting DAUs Service Acquisition Workshop (SAW) as a total team training event. There are many training resources available at the Defense Acquisition University (DAU), but if classroom training is needed, plan early.

14.2.2. Step Two Review Current Strategy

14.2.2.1. Identify Current Initiatives/Contracts

14.2.2.2. Review and Document Current Level of Performance

14.2.2.3. Begin Program Risk Identification

14.2.2.4. Document Current Processes

14.2.2.5. Determine Status of Government Furnished Property/Materials/Facilities

14.2.2.6. Stakeholder Submits Current and Projected Requirements Forecast

14.2.2.7. Review Current/Statutory Requirements

[14.2.2.8. Define (at a High Level) Desired Results]

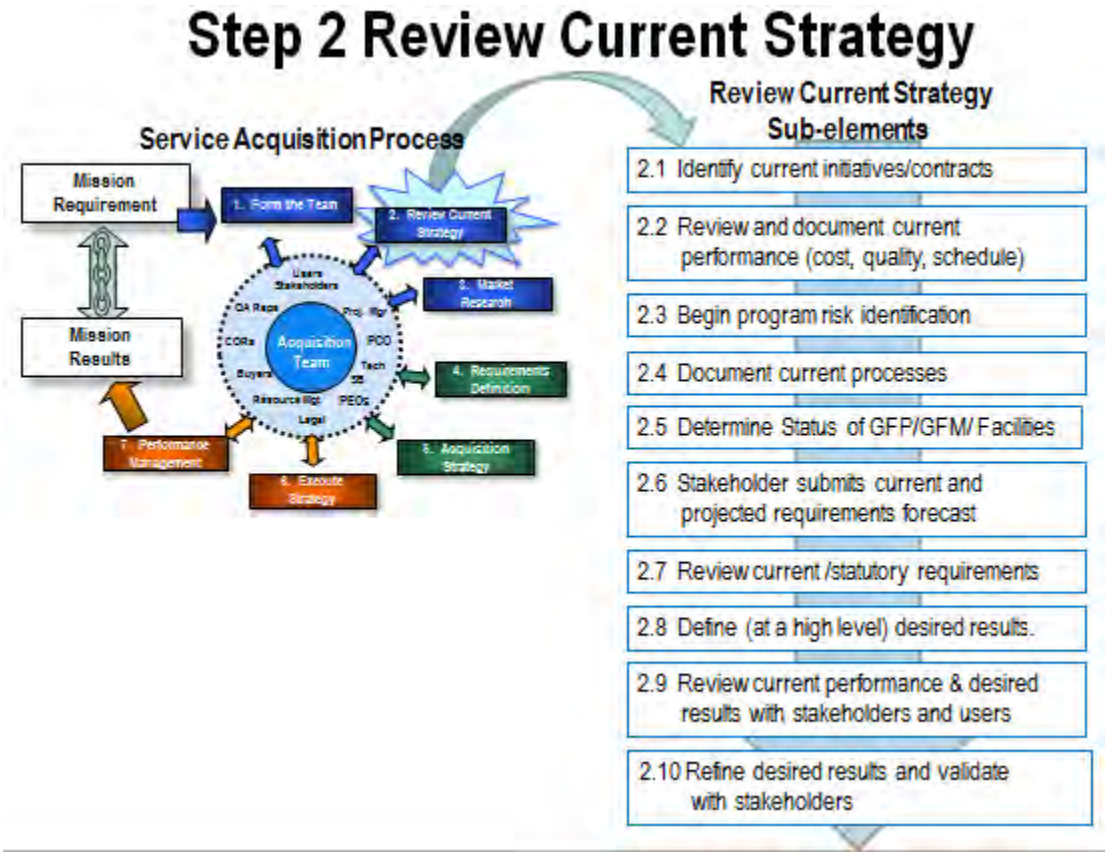
[14.2.2.9. Review Current Performance and Desired Results with Stakeholders and Users]

[14.2.2.10. Refine Desired Results and Validate with Stakeholders]

14.2.2. Step Two Review Current Strategy

The most effective foundation for an acquisition is the intended effect it will have in supporting and improving an agency's mission and performance goals and objectives. Describing an acquisition in terms of how it supports these mission-based performance goals allows an agency to establish a clear relationship between the acquisition and the agency's mission. It sets the stage for crafting an acquisition in which the performance goals of the contractor and the government are in sync. It's important to remember that a service acquisition is a skillful linking of the performance requirement and results with a contract vehicle that motivates contractor performance aligned with the activities mission objectives. This requires the best efforts of the acquisition team.

Figure 14.2.2.F1. Model of Step Two



14.2.2.1. Identify Current Initiatives/Contracts

Identify current contracts that support this requirement or are closely related to it. Are these a part of your agencies strategic sourcing initiatives? Does your activity have new initiatives in the planning stages that might affect this requirement? All this helps develop a baseline for planning and minimize surprises.

14.2.2.2. Review and Document Current Level of Performance

To develop your baseline, identify any current performance issues; does the current requirement still meet the mission? Interview key stakeholders and understand how they define mission success, what their concerns are, and what mission changes do they see in the future that will affect this requirement. Effective planning requires that we can understand the objectives and focus on the desired outcomes. The first consideration is answering these three questions:

- What is the problem the agency needs to solve?
- What results are required to meet mission requirements?
- Will it meet the organizational and mission needs?

14.2.2.3. Begin Program Risk Identification

Risk assessment is a process that continues through the whole service acquisition cycle. As part of your discussion with stakeholders, begin collecting concerns and risks that might have a mission impact. Risk assessment is a team responsibility, but the program manager must take the lead in identifying and organizing risk areas. This knowledge will help you as you develop the requirement and your acquisition strategy. Risk analysis is discussed in more depth in Step Four.

14.2.2.4. Document Current Processes

This involves understanding how things are actually being done today. How do you capture performance, what metrics are you tracking and reporting, what are the challenges with current performance, and what are the issues associated with resolving problems? What is the current small business strategy for the prime contracts and subcontracts? What you are seeking to develop is a good understanding of the as is state. Based on this, you can more effectively develop plans and actions that will improve performance on your new requirement and implementation strategy.

14.2.2.5. Determine Status of Government Furnished Property/Materials/Facilities

In service contracts the government may furnish property or facilities for the contractors use. Determine if this is still in the best interest of the government. Also determine the condition of the material or facilities and if it is still suitable for use.

14.2.2.6. Stakeholder Submits Current and Projected Requirements Forecast

Interview stakeholders to identify their current requirements, and what mission changes they see coming that may affect the requirements you're planning. What areas hold the most concern for your stakeholders? How will contingency operations affect this requirement? This knowledge will help you develop the scope for your requirement and plan for the flexibility you may need in your contract vehicle to adjust for future requirements. These stakeholder engagements will help ensure alignment of your efforts with your stakeholders expectations.

14.2.2.7. Review Current/Statutory Requirements

As part of the baseline planning process, review current regulations and legislation that could impact your requirement and acquisition strategy. Service contracts normally cover several years, so be sure the plan you develop complies with current regulations and not the ones that were in place at the beginning of the last contract.

14.2.2.8. Define (at a High Level) Desired Results

Based on your stakeholder interviews, knowledge issues, and pending changes, start refining the requirements desired results (outcomes). Is it providing a certain level of help desk support to an organization? Is it a reduction of computer down time? Is it providing a level of information assurance among its customer's? Is it providing a level of systems and software engineering and support? What is the ultimate intended result of the contract and how does it relate to the agency's strategic plan? What are the critical results your stakeholders have identified?

14.2.2.9. Review Current Performance and Desired Results with Stakeholders and Users

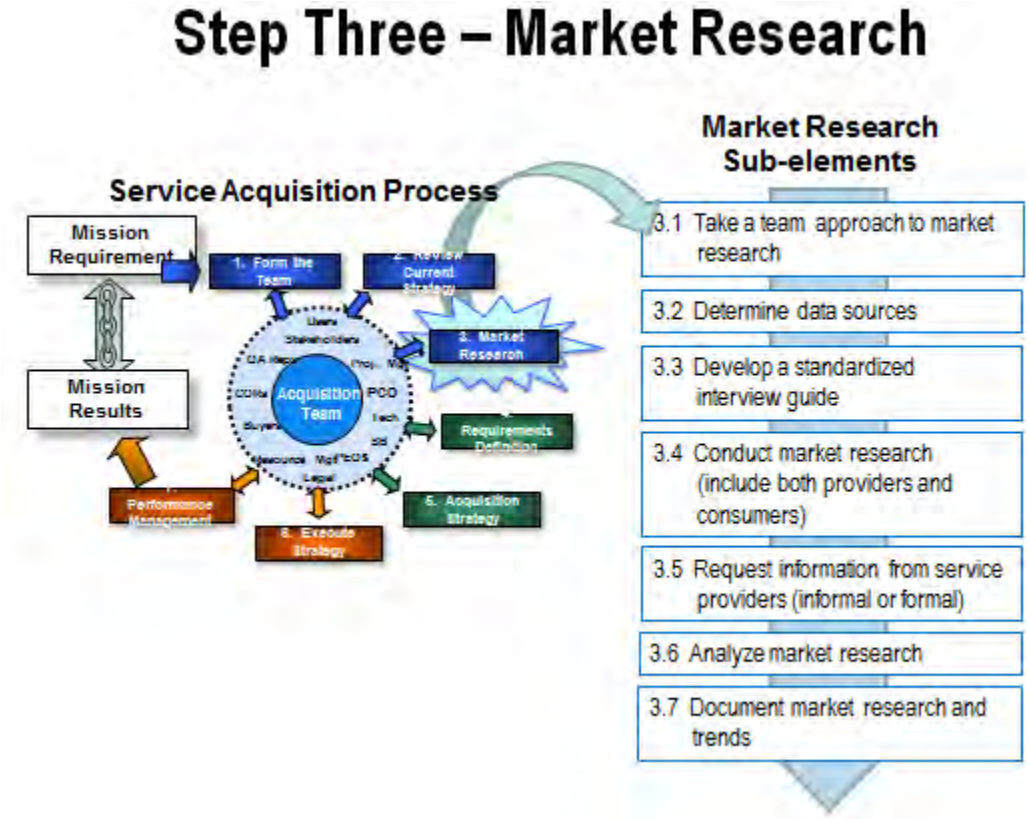
Review your high level results with your stakeholders and customer's to validate that your team has defined the right results. Describe the gaps between current performance and your understanding of what stakeholders are asking. Discuss the funding impact if desired results are significantly beyond current budget levels. This feedback is vital to ensure the actions you take in subsequent steps are aligned with your stakeholder outcomes and results. Failure to do this now can result in a lot of rework later.

14.2.2.10. Refine Desired Results and Validate with Stakeholders

Take the feedback you generated in Section 14.2.2.9 and refine the desired results your team has developed. Validate these refined results one more time with your stakeholders to ensure you are moving in the right direction. Time invested here will pay large dividends later in the process.

14.2.3. Step Three Market Research

Figure 14.2.3.F1. Model of Step Three



Market research is required by FAR Part 10 and is a vital means of arming the acquisition team with the knowledge needed to conduct an effective performance-based service acquisition. This type of information helps determine the suitability of the marketplace for satisfying a need or requirement. Market research is the continuous process of collecting information to maximize reliance on the commercial marketplace and to benefit from its capabilities, technologies, and competitive forces in meeting an agency need. Market research is an essential process enabling the government to buy best-value products and services that solve mission-critical problems. Appendix D also provides a list of helpful sites as you are conducting your market research.

14.2.3.1. Take a Team Approach to Market Research

The ultimate goal of market research is to help the acquisition team become informed consumers. To understand the cost drivers in providing the service, research what leverage the team may discover in the marketplace that could affect both the requirement and the business strategy. In short it helps the acquisition team optimize a strategy for meeting their requirement. Since market research should address both business and technical considerations of a requirement, it requires the active

participation of all acquisition team members as appropriate.

Market research should be done before:

- Developing new requirements documents;
- Soliciting any offers over the simplified acquisition threshold (SAT);
- Soliciting offers under the SAT when adequate information is not available and cost to conduct the research is justified; and
- Soliciting offers for acquisitions that could lead to a bundled contract (DFARS 210.001).

It is not unusual for the technical staff to conduct market research about marketplace offerings while the contracting staff conducts market research that focuses on industry practices and pricing. However, a better approach to conducting market research is for the entire acquisition team to be a part of the effort. This enables the members of the team to share in the understanding and knowledge of the marketplace and develop a common understanding of what features, schedules, terms and conditions are key for their projects success. The team should consider such factors as urgency, estimated dollar value, complexity, and past experience as a guideline for determining the amount of time and resources to invest in the effort. Don't invest more resources (e.g., lead time, available personnel, and money) than are warranted by the potential benefits. In addition, when acquiring services under the SAT, conduct market research when adequate information is not available and the circumstances justify the cost of such research. One of the purposes of market research is to effectively identify the capabilities of small businesses. Small businesses offer attributes of agility and innovation in the services sector with generally lower overhead costs. Keep in mind that each acquisition of supplies and services that are under the SAT should automatically be reserved exclusively for small business concerns unless the contracting officer determines there is not a reasonable expectation of obtaining two or more responsible offers from small business concerns that are competitive in terms of market prices, quality and delivery (FAR 19.502-2).

14.2.3.2. Determine Data Sources

Acquisition histories may not give the whole picture needed for planning a specific acquisition, particularly if commercial practices or technologies to deliver the service are changing rapidly. There may be times when this information is not adequate, such as first time purchases, rapidly changing technology, change in market capability, and no known sources. In determining and identifying the scope and extent of additional research needed, you should follow these steps:

- Review information already in hand (including your personal knowledge of the market from prior requirements and the findings of recent research on like requirements);
- Identify information deficiencies;
- Select sources of additional information; and

- Plan the collection of additional market information (i.e. when and how) during the acquisition planning, pre-solicitation, solicitation, and evaluation phases.

14.2.3.3. Develop a Standardized Interview Guide

The reason it's critical to conduct market research as the entire acquisition team is it makes it easier when each member of the team knows what his/her responsibility is during this step. Determine who will do what and by when. As the team begins making calls or visiting with providers, having a standard interview guide may help provide accuracy and consistency. Try not to ask questions that will provide a yes or no response. The interview guide should ask what experience they have in providing this service.

14.2.3.4. Conduct Market Research

While many are familiar with examining private-sector sources and solutions as part of market research, looking to the public-sector is not as common a practice. Yet it makes a great deal of sense on several levels. First, there is an increased interest in cross-agency cooperation and collaboration. Second, agencies with similar needs may be able to provide lessons learned and best practices. So it is important for the acquisition team to talk to their counterparts in other agencies. Taking the time to do so may help avert problems that could otherwise arise in the acquisition. Other resources include state and local governments that are experienced in procuring certain services that have not been procured by the Federal Government.

14.2.3.4.1. Customer's

A wealth of information can be obtained from customers of prospective contractors regarding:

- How well a contractor performs;
- Depth of competition;
- The reliability and quality of the product or service;
- The price they may have paid; and
- Delivery terms and conditions, and incentive provisions.

14.2.3.4.2. Consider One-on-One Meetings with Industry

One-on-one meetings with industry leaders are not only permissible (ref FAR15.201(c)(4)) they are highly encouraged. Note that when market research is conducted before a solicitation or PWS is drafted, the rules are different. FAR 15.201(f) states that general information about agency mission needs and future requirements may be disclosed at any time. As long as the requirements have not (or should not have) been defined, disclosure of procurement-sensitive information is not an issue. Focus your market research on commercial and industry best practices, performance metrics and measurements, innovative delivery methods for the required services, and

incentive programs that providers have found particularly effective. This type of research can expand the range of potential solutions, change the very nature of the acquisition, establish the performance-based approach, and represent the agency's first step on the way to implementing an effective and meaningful "incentivized" business relationship with a contractor.

14.2.3.4.3. Look for Existing Contracts

A thorough review of acquisition histories on current or prior contracts for the same/similar items helps determine the type of market information needed for a particular acquisition. FAR part 10 describes techniques for conducting market research. This includes querying the Government wide database of contracts and other procurement instruments intended for use by multiple agencies available at https://www.contractdirectory.gov/contractdirectory/ and other Government and commercial databases that provide information relevant to agency acquisitions.

14.2.3.5. Request Information From Service Providers

With regard to the more traditional private-sector market research, it is important to be knowledgeable about commercial offerings, capabilities, and practices before structuring the acquisition in any detail. In today's marketplace it's vital to understand how private sector buyers structure their requirements and business deals when buying similar services. Whether it's facility management, food services, or consulting support, major companies buy most of the same services we do. Unlike the public sector, the private sector must sustain their competitive advantage through efficiencies. The more we understand how and why industry buys the way they do, the better we can be at creating innovative requirements packages and business solutions that will improve performance and reduce costs.

Traditional ways to identify who can deliver the required services are to issue "sources sought" notices at FedBizOps.gov, conduct "Industry Days," issue requests for information, and hold pre-solicitation conferences. Also, consider reviewing current FedBizOps solicitations. It's also okay to pick up the phone and call private-sector company representatives. Contact with vendors and suppliers, for purposes of market research, is encouraged, FAR 15.201(a) specifically promotes the exchange of information "among all interested parties, from the earliest identification of a requirement through receipt of proposals." Once the solicitation has been issued and the procurement is underway, the treatment of potential offeror's must be fair and impartial and the standards of procurement integrity (FAR 3.104) must be maintained. So, the real key is to begin market research early before the procurement action is underway.

14.2.3.6. Analyze Market Research

Once the market research is completed, it's now time to analyze the information and data accumulated. This also is a task for the entire acquisition team. Some of the things to consider as market research is analyzed are what are the opportunities for

competition and/or small business considerations? Did your market research reveal any new emerging technologies? Sometimes market research can reveal things such as market trends (supply/demand) which can provide leverage during negotiations. Once the market research is analyzed, it's time to document your findings.

14.2.3.7. Document Market Research and Trends

The market research report is the document prepared after all information has been compiled. It provides a summary of the market research teams activities and should provide a logical basis for supporting your business strategy such as a commercial service acquisition, full and open competition or small business set aside. FAR 10.002(e) encourages agencies to document the results of market research in a manner appropriate to the size and complexity of the acquisition. The amount of research should be commensurate with the size, complexity and criticality of the acquisition. You should always check with your local agency for any additional requirements that may not be listed. Your market research report can help build the business case for change in how you approach your requirement and support your decisions on an acquisition approach. Remember, it is easier to compile all the information gathered during your market research into one document that will be included in the contract file.

14.3. The Development Phase

14.3.1. Step Four Requirement Definition

14.3.1.1. Conduct Performance Risk Analysis

14.3.1.2. Conduct a Requirements Analysis

14.3.1.3. Build Requirements Roadmap

14.3.1.3.1. Automated Requirements Roadmap Tool

14.3.1.3.2. Acceptable Quality Levels (AQLs)

14.3.1.3.3. Performance Assessment Strategies

14.3.1.3.4. Performance Assessment Personnel

14.3.1.3.5. Assessment Methods

14.3.1.3.6. Contractors Quality Control Plan

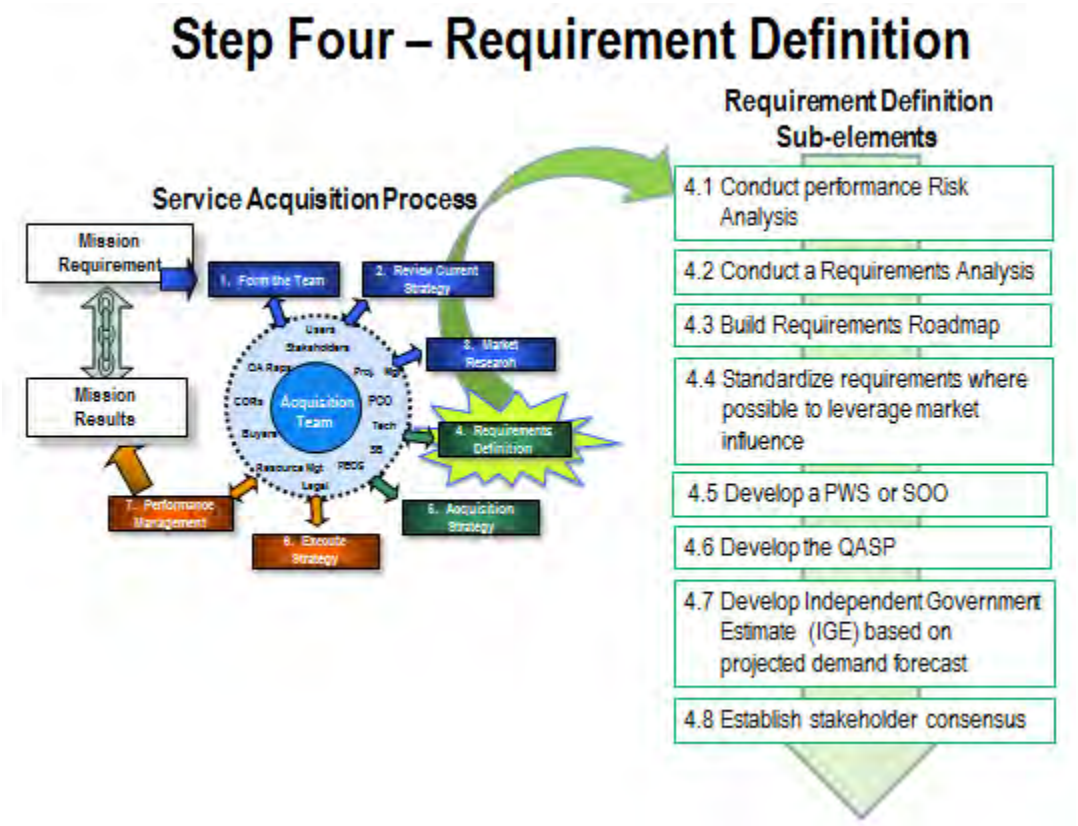
14.3.1.3.7. Create Your Performance Reporting Structure

14.3.1.4. Standardize Requirements Where Possible to Leverage Market Influence

14.3. The Development Phase

At this point of the process, the Planning Phase of the seven step service acquisition process has been completed. The acquisition team is now ready to use the collected data from the previous three steps (Form the Team, Current Strategy and Market Research) to begin developing the Requirements Document (Step 4) and the Acquisition Strategy (Step 5).

Figure 14.3.1.F1. Model of Step Four



14.3.1. Step Four Requirement Definition

14.3.1.1. Conduct Performance Risk Analysis

As part of the requirements development process you must identify and analyze risk areas that can impact the performance results you are trying to achieve. Identify possible events that can reasonably be predicted which may threaten your acquisition. Risk is a measure of future uncertainties in achieving successful program performance goals. Risk can be associated with all aspects of your requirement. Risk addresses the potential variation from the planned approach and it's expected outcome. Risk assessment consists of two components: (1) probability (or likelihood) of that risk occurring in the future and (2) the consequence (or impact) of that future occurrence.

Risk analysis includes all risk events and their relationships to each other. Therefore, risk management requires a top-level assessment of the impact on your requirement when all risk events are considered, including those at the lower levels. Risk assessment should be the roll-up of all low-level events; however, most likely, it is a subjective evaluation of the known risks, based on the judgment and experience of the team. Therefore, any roll-up of requirements risks must be carefully done to prevent key

risk issues from slipping through the cracks.

It is difficult, and probably impossible, to assess every potential area and process. The program or project office should focus on the critical areas that could impact your program and thus impact your performance results. Risk events may be determined by examining each required performance element and process in terms of sources or areas of risk. Broadly speaking, these areas generally can be grouped as cost, schedule, and performance, with the latter including technical risk. When the word system is used, it refers to the requirement for services as a system with many different activities and events. The more complex the service requirement is, the more likely it will have the components and characteristics of a system. The following are some typical risk areas:

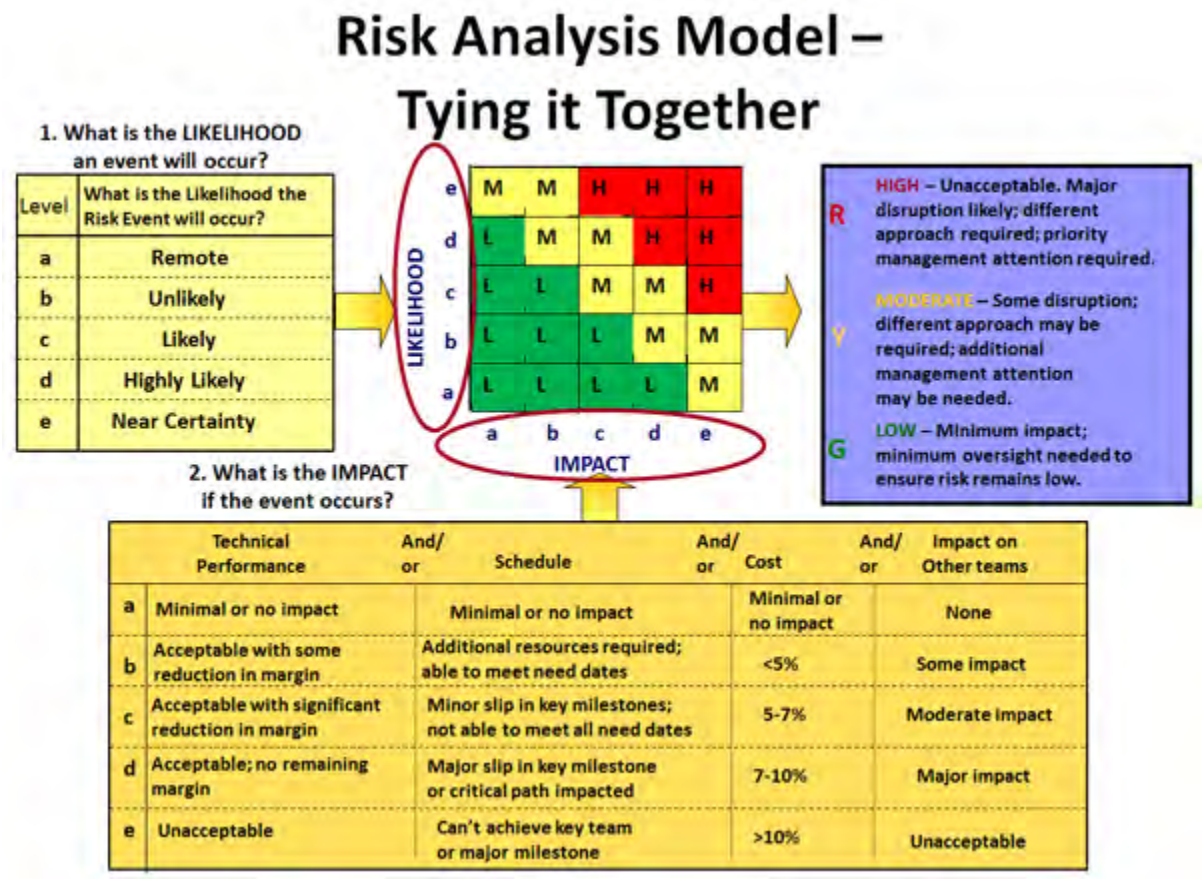
- Business/Programmatic Risk
- Scheduling issues that may impact success?
- Technical Risk
- Maturity of technology and processes reliant on technology
- Funding Risk
- Are funds identified for which availability is reliant on pending events or approvals? Have adequate funds been identified?
- Process Risk
- Are new processes required to be implemented?
- Will the best contractors have time to propose?
- Organizational Risk
- Implementing change within an organization
- Risk Summary
- Overview of the risk associated with implementing the initiative e.g. Is there adequate service life remaining to justify this change?

Additional areas, such as environmental impact, security, safety, and occupational health are also analyzed during the requirements definition phase. The acquisition team should consider these areas for early assessment since failure to do so could cause significant consequences. Program/project managers must recognize that any work being performed on government property or government workspace should have the proper control and oversight into access of facilities, clearances, and visitor control.

Identifying risk areas requires the acquisition team to consider relationships among all these risks and may identify potential areas of concern that would have otherwise been overlooked. This is a continuous process that examines each identified risk (which may change as circumstances change), isolate the cause, determine the effects, and then determine the appropriate risk mitigation plan. If your acquisition team is requesting the contractor to provide a solution as part of their proposal that contains a performance-based statement of work and performance metrics and measures, then it is also appropriate to have the contractor provide a risk mitigation plan that is aligned with that solution.

To learn more about risk management and using a risk mitigation plan, we suggest you take the DAU online course, entitled Continuous Learning Module (CLM) 017, Risk Management. Figure 14.3.1.1.F1 is a typical risk analysis model.

Figure 14.3.1.1.F1. Risk Analysis Model



14.3.1.2. Conduct a Requirements Analysis

Like risk analysis, requirements analysis means conducting a systematic review of your requirement given the guidance you captured from your stakeholders during the planning phase steps One, Two, and Three. The objective of this step is to describe the work in terms of required results rather than either how the work is to be accomplished or the number of hours to be provided (FAR 37.602). This analysis is the basis for establishing the high level objectives, developing performance tasks, and standards, writing the Performance Work Statement, and producing the Quality Assurance Surveillance Plan.

The acquisition team needs to identify the essential processes, and outputs or results required. One approach is to use the "so what?" test during this analysis. For example, once the analysis identifies the outputs, the acquisition team should verify the continued

need for the output. The team should ask questions like the following:

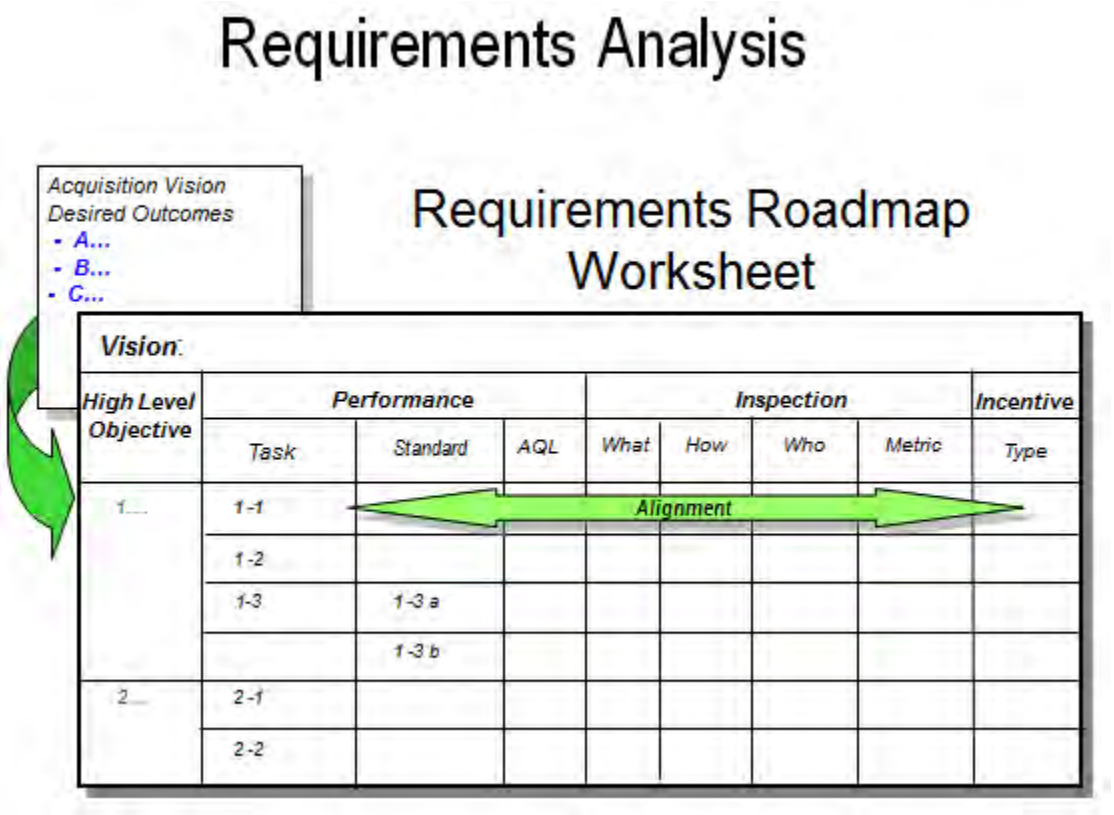
- Who needs the output or result?
- Why is the output needed?
- What is done with it?
- What occurs as a result?
- Is it worth the effort and cost?
- Would a different output be preferable?
- And so on...

14.3.1.3. Build Requirements Roadmap

The requirements roadmap worksheet (Appendix A) provides a method that links required performance to the overall acquisition desired outcomes. The roadmap takes the performance tasks and aligns performance standards and acceptable quality levels (AQLs). It also includes detailed inspection information and responsibilities. Each of these areas will be discussed in greater detail in this step. When using this approach, it is vital that all elements of the document be aligned with the mission objectives you are trying to deliver. If you develop a performance task and standard, but have no way to inspect it, you have a problem. In this case you will need to revisit the objective or find new technology for the inspection. All the elements must fit together as a whole before writing the PWS.

As you build your roadmap with high level objectives and task statements, prioritize them in descending order of importance based on risk, criticality or priority. This will help you later when determining what you want to evaluate in a contractors proposal.

Figure 14.3.1.3.F1. Requirements Roadmap Worksheet



Initially, the High Level Objectives (HLO) need to be defined. What must be accomplished to satisfy the requirement? This should have been accomplished during steps 1 and 2 when you were talking with your stakeholders and customer's. To define HLOs, list what needs to be accomplished to satisfy the overall requirement, from a top-level perspective. HLOs are similar to level two in work bread down structures.

Tasks are the results or actions required to achieve the HLO. It may take several tasks to satisfy a HLO. Tasks consist of results, the context of what or who the results pertain to and what actions are required to complete the task. Defining the task goes into greater detail and expands the stakeholder analysis beyond the top-level perspective. The goal of a task is to adequately describe what action or result is required (not how to accomplish it).

Tasks are generally nouns and verbs and tend to be declarative statements such as the following:

- Conduct a study on
- Provide financial analysis of
- Maintain vehicles
- Review and assess
- Develop a strategic plan

- Identify potential
- Perform and document

When developing tasks ask the question WHY is this action needed? A because answer usually drives the focus on the performance results needed. Why do you want the river to be dredged? Because we want the boats to be able to go in and out. Bottom line: we need to keep the river navigable. That is the objective.

Next, identify appropriate and reasonable performance standards (i.e., how well the work must be performed to successfully support mission requirements). The purpose is to establish measurable standards (adjectives and adverbs) for each of the tasks that have been identified. The focus is on adjectives and adverbs that describe the desired quality of the services outcome. How fast, how thorough, how complete, how error free, etc. Examples of performance standards could include the following:

- Response times, delivery times, timeliness (meeting deadlines or due dates), and adherence to schedules.
- Error rates or the number of mistakes or errors allowed in meeting the performance standard.
- Accuracy rates.
- Milestone completion rates (the percent of a milestone completed at a given date).
- Cost control (performing within the estimated cost or target cost), as applied to flexibly priced contracts.

This should reflect the minimum needs to meet the task results. The standards you set are cost drivers because they describe the performance levels that the contractor must reach to satisfy the task. Therefore, they should accurately reflect what is needed and should not be overstated. In the case of keeping a river navigable, the standard might be: 100 feet wide, 12 feet deep at mean low water. Thus we have a measure for what we define as navigable.

Standards should accurately reflect what is needed and should not be overstated. We should ask the following questions in this area:

- Is this level of performance necessary?
- What is the risk to the government if it does not have this level of performance?
- What is the minimum acceptable level of performance necessary to successfully support your mission?

In the case of the navigable river, 12 feet deep means low water might be sufficient for pleasure craft type usage. However, setting a depth of 34 feet which might be needed for larger commercial watercraft that may never use that river would be considered overkill and a waste of money. The standard must fit, or be appropriate to, the outcomes need.

Another way of describing a performance standard is using terms like measurement threshold or defining it as the limit that establishes that point at which successful performance has been accomplished. Performance standards should:

- Address quantity, quality and timeliness;
- Be objective, not subjective (if possible);
- Be clear and understandable;
- Be realistically achievable;
- Be true indicators of outcome or output; and
- Reflect the government's needs.

The performance standards should describe the outcome or output measures but does not give specific procedures or instructions on how to produce them. When the government specifies the how-to, the government also assumes responsibility for ensuring that the design or procedure will successfully deliver the desired result. On the other hand, if the government specifies only the performance outcome and accompanying quality standards, the contractor must then use its best judgment in determining how to achieve that level of performance. Remember that a key PBA tenet is that the contractor will be entrusted to meet the governments requirements and will be handed both the batons of responsibility and authority to decide how to best meet the government's needs. The governments job is to then to evaluate the contractors performance against the standards set forth in the PWS. Those assessment methods identified in the QASP, together with the contractors quality control plan, will also help in evaluating the success with which the contractor delivers the contracted level of performance.

14.3.1.3.1. Automated Requirements Roadmap Tool

The Automated Requirements Roadmap Tool (ARRT) is a job assistance tool that enables users to develop and organize performance requirements into draft versions of the performance work statement (PWS), the quality assurance surveillance plan (QASP), and the performance requirements summary (PRS). ARRT provides a standard template for these documents and some default text that can be modified to suit the needs of a particular contract. This tool should be used to prepare contract documents for all performance-based acquisitions for services. The ARRT is available for download at: http://sam.dau.mil/ARRTRegistration.aspx

14.3.1.3.2. Acceptable Quality Levels (AQLs)

The acquisition team may also establish an AQL for the task, if appropriate. The AQL is a recognition that unacceptable work can happen, and that in most cases zero tolerance is prohibitively expensive. In general, the AQL is the minimum number (or percentage) of acceptable outcomes that the government will permit. An AQL is a deviation from a standard. For example, in a requirement for taxi services, the performance standard might be "pick up the passenger within five minutes of an agreed upon time." The AQL then might be 95 percent; i.e., the taxi must pick up the passenger within five minutes

95 percent of the time. Failure to perform at or above the 95 percent level could result in a contract price reduction or other action. AQLs might not be applicable for all standards especially for some services such as Advisory and Assistance Services (A&AS) or research and development (R&D) services.

Once the team has established the AQLs, they should review them:

- Are the AQLs realistic?
- Do they represent true minimum levels of acceptable performance?
- Are they consistent with the selected method of surveillance?
- Are they aligned with the task and standard?
- Is the AQL clearly understood and communicated?

14.3.1.3.3. Performance Assessment Strategies

Traditional acquisition methods have used the term quality assurance to refer to the functions performed by the government to determine whether a contractor has met the contract performance standards. The QASP is the governments surveillance document used to validate that the contractor has met the standards for each performance task.

The QASP describes how government personnel will evaluate and assess contractor performance. It is intended to be a living document that should be revised or modified as circumstances warrant. It's based on the premise that the contractor, not the government, is responsible for delivering quality performance that meets the contract performance standards. The level of performance assessment should be based on the criticality of the service or associated risk and on the resources available to accomplish the assessment.

Performance assessment answers the basic question How are you going to know if it is good when you get it? Your methods and types of assessment should focus on how you will approach the oversight of the contractors actual performance and if they are meeting the standards that are set in the PWS. Completing the assessment elements of the requirements roadmap will ensure that you determine who and how you will assess each performance task before you write the PWS. If you develop a task or standard that cannot be assessed you should go back and reconsider or redefine the task or standard into one that can be assessed. This section of the roadmap provides the foundation for your QASP. The QASP is not incorporated into the contract since this enables the government to make adjustments in the method and frequency of inspections without disturbing the contract. An informational copy of the QASP should be furnished to the contractor.

14.3.1.3.4. Performance Assessment Personnel

The COR plays an essential role in the service acquisition process and should be a key member of your acquisition team. During the requirements development process his/her input is vital, because they will be living with this requirement during performance. In

accordance with DFARS 201.602-2, A COR must be qualified by training and experience commensurate with the responsibilities to be delegated in accordance with department/agency guidelines.

The method for assessing the contractors performance must be addressed before the contract is awarded. It is the responsibility of the COR, as part of the acquisition team, to assist in developing performance requirements and quality levels/standards, because the COR will be the one responsible for conducting that oversight. The number of assessment criteria and requirements will vary widely depending on the task and standard as it relates to the performance risk involved, and the type of contract selected. Using the requirements roadmap worksheet (Appendix A) will help ensure that the requirement and assessment strategies are aligned.

14.3.1.3.5. Assessment Methods

Several methods can be used to assess contractor performance. Performance tasks with the most risk or mission criticality warrant a higher level of assessment than other areas. No matter which method you select you should periodically review your assessment strategy based on documented contractor performance and adjust as necessary. Below are some examples of commonly used assessment methods.

Random sampling: Random sampling is a statistically based method that assumes receipt of acceptable performance if a given percentage or number of scheduled assessments is found to be acceptable. The results of these assessments help determine the governments next course of action when assessing further performance of the contractor. If performance is considered marginal or unsatisfactory, the evaluators should document the discrepancy, begin corrective action and ask the contractor why their quality control program failed. If performance is satisfactory or exceptional, they should consider adjusting the sample size or sampling frequency. Random sampling is the most appropriate method for frequently recurring tasks. It works best when the number of instances is very large and a statistically valid sample can be obtained.

Periodic sampling: Periodic sampling is similar to random sampling, but it is planned at specific intervals or dates. It may be appropriate for tasks that occur infrequently. Selecting this tool to determine a contractors compliance with contract requirements can be quite effective, and it allows for assessing confidence in the contractor without consuming a significant amount of time.

Trend analysis: Trend analysis should be used regularly and continually to assess the contractors ongoing performance over time. It is a good idea to build a database from data that have been gathered through performance assessment. Additionally, contractor-managed metrics may provide any added information needed for the analysis. This database should be created and maintained by government personnel.

Customer feedback: Customer feedback is firsthand information from the actual users of the service. It should be used to supplement other forms of evaluation and assessment,

and it is especially useful for those areas that do not lend themselves to the typical forms of assessment. However, customer feedback information should be used prudently. Sometimes customer feedback is complaint-oriented, likely to be subjective in nature, and may not always relate to actual requirements of the contract. Such information requires thorough validation.

Third-party audit's: The term third-party audit refers to contractor evaluation by a third-party organization that is independent of the government and the contractor. All documentation supplied to, and produced by, the third party should be made available to both the government and the contractor. Remember, the QASP should also describe how performance information is to be captured and documented. This will later serve as past performance information. Effective use of the QASP, in conjunction with the contractors quality control plan, will allow the government to evaluate the contractors success in meeting the specified contract requirements. Those assessment methods identified in the QASP, together with the contractors quality control plan will help evaluate the success with which the contractor delivers the level of performance agreed to in the contract.

In our case of the navigable river, the method of inspection might be using a boat with sonar and GPS, thus measuring the channel depth and width from bridge A to Z. The results would document actual depths and identify where any depths are not compliant with the standards.

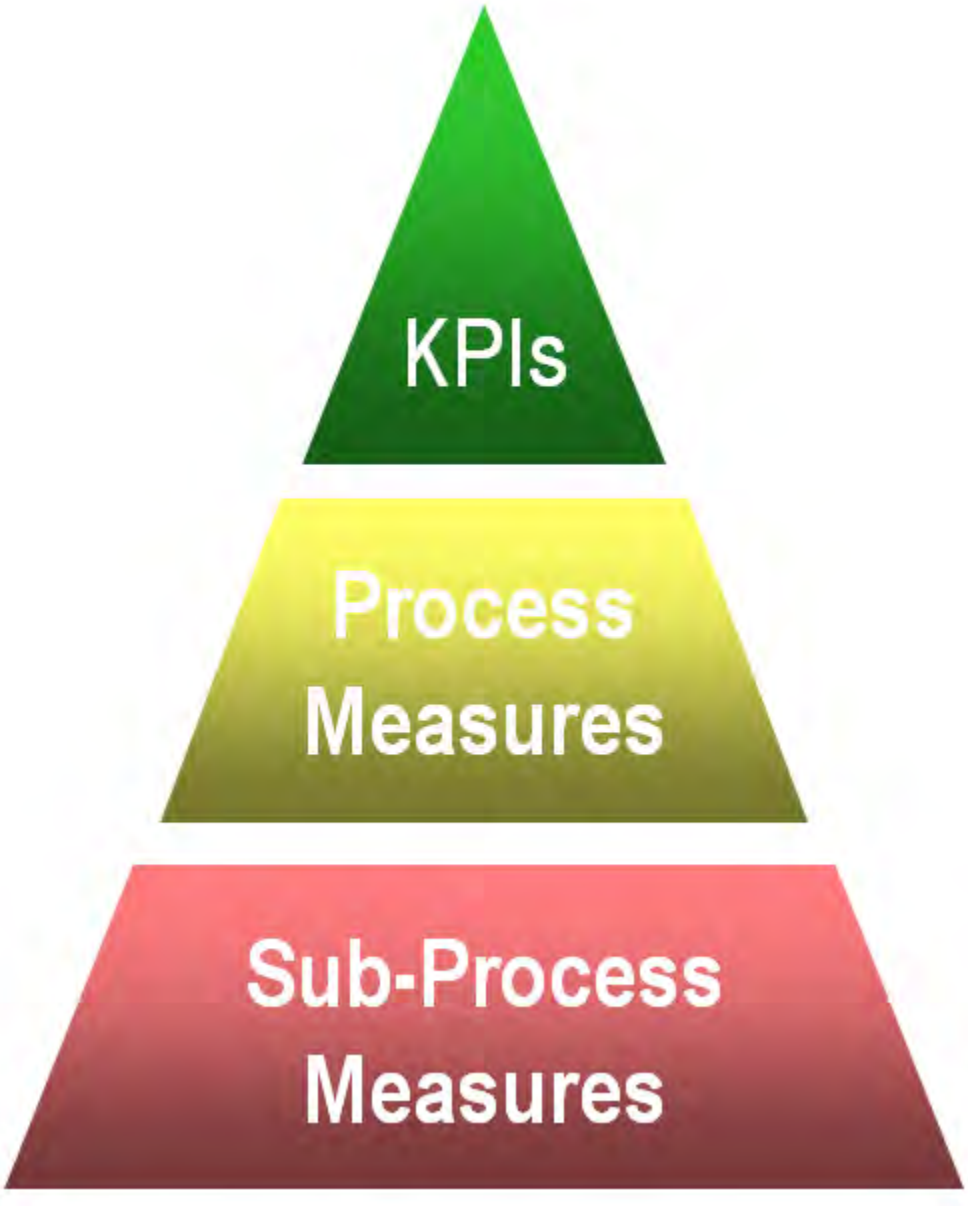
14.3.1.3.6. Contractors Quality Control Plan

A quality control plan is a plan developed by the contractor for its internal use to ensure that it delivers the service levels contained in the contract. The quality control plan should be part of the contractors original proposal, and in many cases, it is incorporated into the resultant contract. The inspection of services clause requires that the quality control plan be acceptable to the government.

14.3.1.3.7. Create Your Performance Reporting Structure

Invest some time to determine how and to whom you will present the contractors performance results. Most often this is to your leadership and stakeholders. This should take the form of periodic performance reviews that quickly capture summary performance results yet also provide the drill down capability when necessary to identify and resolve performance problems. One way to structure your performance reporting is to use the key stakeholder outcomes as key performance indicators (KPIs). These measures are few in number, but supported by the process and sub-process measures in your PWS. The chart below, Figure 14.3.1.3.7.F1, illustrates this approach.

Figure 14.3.1.3.7.F1. Performance Indicators



Key Process Indicators (KPIs): Top level summary metrics that quickly capture current performance status that link to your stakeholder desired outcomes.

Process Measures: Capture the overall status of each process area contained in your PWS.

Sub Process Measures: Capture specific performance outcomes for each performance task in your PWS.

More on performance reporting will be discussed in step seven, but remember that in developing your approach make sure that the effort required for collection and measurement does not exceed the value of the information.

14.3.1.4. Standardize Requirements Where Possible to Leverage Market Influence

Market research may reveal that commercially acceptable performance standards will satisfy the customer with the potential of a lower price. The acquisition team may also discover that industry standards and tolerances are measured in different terms than those that the customer has used in the past. Rather than inventing metrics or quality or performance standards, the acquisition team should use existing commercial quality standards (identified during market research), when applicable. It is generally a best practice to use commercial standards where they exist, unless the commercial standard proves inappropriate for the particular requirement. Industry's involvement, accomplished through public meetings, requests for information (RFI), or draft request for proposals (RFPs), will help in finding inefficiencies in the PWS, and will also lead to cost efficiencies that can be achieved through the use of commercial practices.

14.3.1.5. Develop a Performance Work Statement (PWS) and Statement of Objectives (SOO)

The PWS comprises the heart of any service acquisition and the success or failure of a contract is greatly dependent on the quality of the PWS. Ensure you have completed all elements of the requirements roadmap worksheet including inspection before starting to write the PWS. There is no mandatory template or outline for a PWS. The FAR only requires that agencies to the maximum extent practicable:

- Describe work in terms of required results rather than how the work is to be accomplished or the number of hours to be provided.
- Enable assessment of work performance against measurable performance standards.
- Rely on measurable performance standards and financial incentives in a competitive environment to encourage innovation and cost effective methods of performing the work.

The roadmap worksheet contains the basic outline for the requirements section of your PWS. The HLOs and supporting performance tasks and standards should be the main component of your PWS. After the introduction and general sections, the nuts and bolts of your PWS might have the HLOs listed as 3.1, 3.2, 3.3, as appropriate. Under HLO 3.1, you would list the tasks and standards associated with this HLO. For example, 3.1.1 would be task 1 under that HLO 3.1. A task can have multiple performance standards and AQLs associated with it from your roadmap such as timeliness, quality etc. Make sure they are accurately captured in your PWS.

14.3.1.5.1. Format

There is no mandatory format for a PWS; however, one normally includes the following:

1. Introduction: It should capture the importance of your mission and how this requirement contributes to the overall mission of your organization. The introduction describes your overall acquisition vision and desired mission results. It sets your expectations of contractor performance in terms of teamwork and improving mission results thru efficiencies and process improvements. Keep this section focused and relatively brief, but capture the importance of achieving mission results and your performance expectations.

2. Background: This section briefly describes the scope of the performance requirement and the desired outcome. Provide a brief historical description of the program/requirement that provides the context for this effort (include who is being supported and where). Describe the general desired outcomes of your new requirement. Consider that a contractor will have a greater chance at success with adequate information that clearly defines the magnitude, quality, and scope of the desired outcomes.

3. General Requirements: Describe general requirements that are not specifically related to performance outcomes but have an impact on the success of the mission. (Place of performance, period of performance, security clearance requirements, etc.)

4. Performance Requirements: This portion is basically transference of the HLOs, tasks and standards from the roadmap into the PWS. Specify standards to which the task must be completed. Your major paragraphs and subparagraphs should be in descending order of importance based on your earlier risk analysis.

5. Deliverables: This section contains information on deliverables such as data requirements, reports or any other items contained within a contract data requirements list (CDRL). Some agencies list CDRL items separately in Section J of the contract. Limit CDRL requirements to those needed by the government to make a decision, measure performance, or to comply with a higher level requirement. The inspection portion of your roadmap identifies what is going to be inspected, and this often results in a data deliverable.

6. Special Requirements: This section will include information on Government Furnished Property (GFP) or Equipment (GFE). Also include any special security or safety information, environmental requirements, special work hours and contingency requirements. If necessary, include a transition plan and a listing of all applicable documents and/or directives. The number of directives referenced should be limited to those required for this specific effort such as quality standards, statutory, or regulatory.

7. Task Orders: If task orders will be used, you need to address their use and ensure each task order has a well-written PWS that includes HLOs, tasks, standards, data

deliverables and incentives as appropriate. Task descriptions should clearly define each deliverable outcome. Subtasks should be listed in their appropriate order and should conform to the numbering within the basic PWS from which the task order derives. All task orders must capture performance assessments gathered using the task order QASP. Each task order should have a trained COR assigned.

However, the team can adapt this outline as appropriate. Before completing the PWS, there should be final reviews, so be sure your team examines every performance requirement carefully and delete any that are not essential. Many agencies have posted examples of a PWS that can provide some guidance or helpful ideas. Because the nature of performance-based acquisition is tied to mission-unique or program-unique needs, keep in mind that another agency's solution may not be an applicable model for your requirement.

14.3.1.5.2. Best Practices and Lessons Learned for Developing PWS

Best practices and lessons learned for developing a PWS include:

- The purpose of defining your requirement at high level objectives and tasks is to encourage innovative solutions for your requirement. Don't specify the requirement so tightly that you get the same solution from each offeror. If all offeror’s provide the same solution, there is no creativity and innovation in the proposals.
- The acquisition team must move beyond less efficient approaches of buying services (time and material or labor hour), and challenge offeror’s to propose their own innovative solutions. Specifically, specifying labor categories, educational requirements, or number of hours of support required should be avoided because they are "how to" approaches. Instead, let contractors propose the best people with the best skill sets to meet the need and fit the solution. The government can then evaluate the proposals based both on the quality of the solution and the experience of the proposed personnel.
- Prescribing manpower requirements limits the ability of offeror’s to propose their best solutions, and it could preclude the use of qualified contractor personnel who may be well suited for performing the requirement but may be lacking -- for example a complete college degree or the exact years of specified experience.
- Remember that how the PWS is written will either empower the private sector to craft innovative solutions, or stifle that ability.

14.3.1.5.3. Style Guidelines for Writing PWS

The most important points for writing style guidelines are summarized below:

Style: Write in a clear, concise and logical sequence. If the PWS is ambiguous, the contractor may not interpret your requirements correctly and courts are likely to side with the contractors interpretation of the PWS.

Sentences: Replace long, complicated sentences with two or three shorter, simpler sentences. Each sentence should be limited to a single thought or idea.

Vocabulary: Avoid using seldom-used vocabulary, legal phrases, technical jargon, and other elaborate phrases.

Paragraphs: State the main idea in the first sentence at the beginning of the paragraph so that readers can grasp it immediately. Avoid long paragraphs by breaking them up into several, shorter paragraphs.

Language Use: Use active voice rather than passive.

Abbreviations: Define abbreviations the first time they are used, and include an appendix of abbreviations for large documents.

Symbols: Avoid using symbols that have other meanings.

Use shall and don't use will: The term shall is used to specify that a provision is binding and usually references the work required to be done by the contractor. The word will expresses a declaration of purpose or intent.

Be careful using any or either. These words clearly imply a choice in what needs to be done contractually. For instance, the word any means in whatever quantity or number, great or small which leaves it at the discretion of the contractor.

Don't use and/or since the two words together (and/or) are meaningless; that is, they mean both conditions may be true, or only one may be true.

Avoid the use of etc. because the reader would not necessarily have any idea of the items that could be missing.

Ambiguity: Avoid the use of vague, indefinite, uncertain terms and words with double meanings.

Do not use catch-all/open-ended phrases or colloquialisms/jargon. Examples of unacceptable phrases include common practice in the industry, as directed, and subject to approval.

Terms: Do not use terms without adequately defining them.

14.3.1.5.4. Reviewing your PWS

You can review the PWS by answering the following questions:

- Does the PWS avoid specifying the number of contractor employees required to perform the work (except when absolutely necessary)?

- Does the PWS describe the outcomes (or results) rather than how to do the work?
- What constraints have you placed in the PWS that restrict the contractors ability to perform efficiently? Are they essential? Do they support your vision?
- Does the PWS avoid specifying the educational or skill level of the contract workers (except when absolutely necessary)?
- Can the contractor implement new technology to improve performance or to lower cost?
- Are commercial performance standards utilized?
- Do the performance standards address quantity, quality and timeliness?
- Are the performance standards objectives easy to measure and timely?
- Is the assessment of quality a quantitative or qualitative assessment?
- Will two different CORs come to the same conclusion about the contractors performance based on the performance standards in the PWS?
- Are AQLs clearly defined?
- Are the AQL levels realistic and achievable?
- Will the customer be satisfied if the AQL levels are exactly met? (Or will they only be satisfied at a higher quality level?
- Are the persons who will perform the evaluations identified?

14.3.1.6. Develop Quality Assessment Surveillance Plan (QASP) Outline

The heart of your QASP comes directly from your roadmap. It addresses each HLO and its tasks with their associated standards. It includes the methods and types of inspection (who is going to do the inspection, how the inspections are to be conducted and how often they are to be conducted). Numerous organizations use the term performance requirements summary (PRS), while others incorporate the standards within the PWS. Either way, as long as the HLOs and tasks are tied to the standards in the resultant contract, that is what is important.

Recognize that the methods and degree of performance assessment may change over time in proportion to the evaluators level of confidence in the contractors performance. Like the PWS there is no required format for a QASP, a suggested format is shown below:

- Purpose
- Roles and Responsibilities
- Performance Requirements and Assessments
- Objective, Standard, AQL, Assessment Methodology
- Assessment Rating Structure Outline (1 to 5)
- Performance Reporting - establish reporting frequency to leadership
- Metrics
- Remedies used and impacts
- CPARS Report
- Attachments
- Sample Contract Deficiency Report

- Sample Performance Report Structure

Reviewing Your QASP

You can review the QASP by answering the following questions:

- Is the value of evaluating the contractors performance on a certain task worth the cost of surveillance?
- Has customer feedback been incorporated into the QASP?
- Have random or periodic sampling been utilized in the QASP?
- Are there incentives to motivate the contractor to improve performance or to reduce costs?
- Are there disincentives to handle poor performance?
- Will the contractor focus on continuous improvement?

14.3.1.7. Develop Independent Government Estimate (IGE) Based on Projected Demand Forecast

Determining an accurate IGE can be a challenging task for the acquisition team. This will involve various skills sets from the team to project demand forecasts for the service. What sort of constraints do you have in computing your IGE? You could have cost constraints that can limit what you require in the PWS or Statement of Objectives (SOO). Program scope may also be an issue if it's difficult to determine exactly what the contractor is being asked to propose. Remember, if you can't develop an IGE, how do you expect the contractor to propose based on the PWS?

14.3.1.8. Establish Stakeholder Consensus

This is the point where it would be beneficial to revisit the customer and stakeholders to ensure everyone is satisfied with the PWS and the way forward. It is typical to have varying levels of resistance to the teams strategy. The key is to develop an acquisition team approach to sell the strategy to the customer and stakeholders and then schedule review cycles.

14.3.2. Step Five Develop an Acquisition Strategy

14.3.2.1. Develop Preliminary Business Case and Acquisition Strategy

14.3.2.2. Finalize Acquisition Strategy

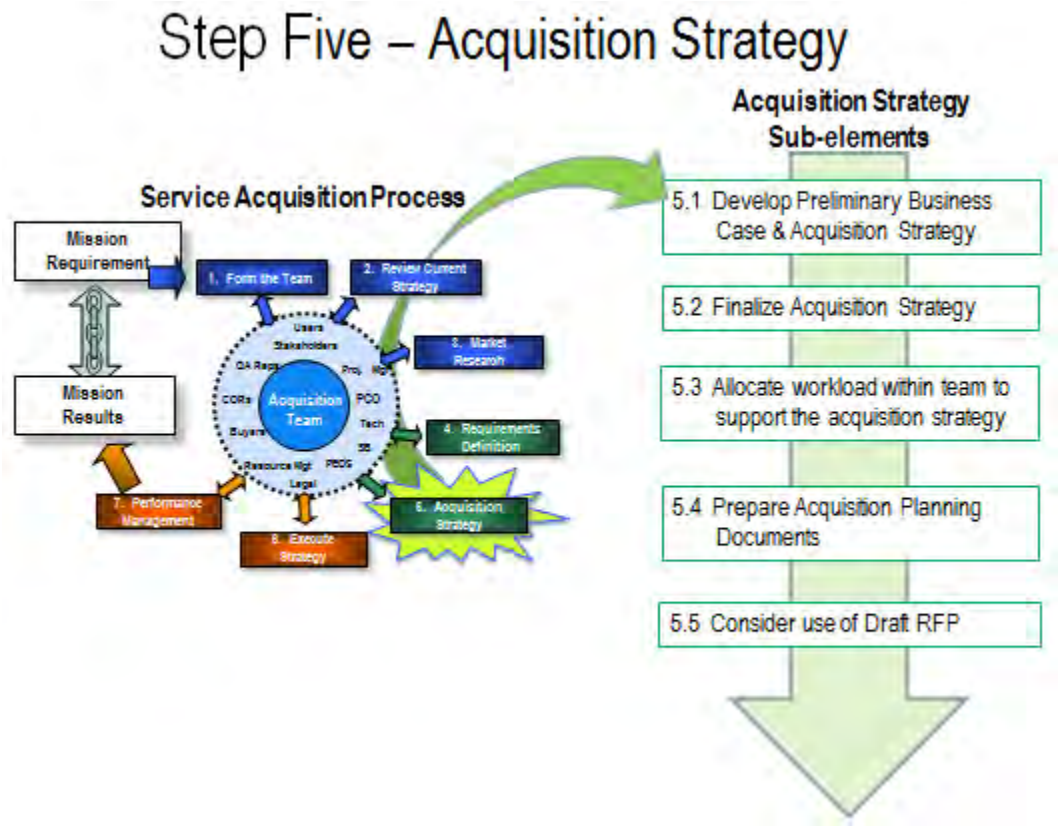
14.3.2.2.1. Types of Contracts

14.3.2.2.1.1. Fixed-Price Contract Types

14.3.2.2.1.2. Cost Reimbursement Contract Types

14.3.2. Step Five Develop an Acquisition Strategy

Figure 14.3.2.F1. Model of Step Five



14.3.2.1. Develop Preliminary Business Case and Acquisition Strategy

At this point in the process you should have a well-defined PWS and QASP. Now it's time to start developing your business strategy to determine the type of contract vehicle,

incentive arrangement if any, and how you will acquire a contract service provider. Review your market research results, how competitive is the market, what are small business opportunities, can this service be acquired using FAR Part 12 , Acquisition of Commercial Items, how are other organizations acquiring this type of service? Is this requirement part of your agency's strategic acquisition initiative? During market research did you find another agency's existing contract suitable for use in supporting this requirement? When reviewing external acquisition options, you should examine your agencies external acquisition policies to make sure there are no potential conflicts. Another important consideration when using another agency's contract is to clearly determine who will provide the performance oversight of the resulting contract to ensure it delivers the required performance results.

If no other viable option is available you will need to develop an effective business case that supports the most effective way to achieve your mission requirements. The business strategy involves selecting the right contract type, incentive structure and contractor selection process that will best deliver mission results.

14.3.2.2. Finalize Acquisition Strategy

Your acquisition strategy involves several key components: (1) what type of contract type is best suited for your requirement; (2) what incentive strategy, if any, to use; and (3) what method you will use to select a contractor. Developing your strategy must be a thoughtful, integrated team effort defined by the specifics of your mission requirement.

14.3.2.2.1. Types of Contracts

The FAR does not make any recommendation on the type of contract to be used when contracting for services. However, the selection of contract type must be reflective of the nature of the service requirement and risks associated with performance. Selection of a contract type should motivate the contractor to deliver optimum performance. Your observations during market research provide a good basis for analyzing commercial practices, level of competition, maturity level of the service, to guide the selection of contract type. There are two basic types of contract types, fixed price types and cost reimbursable types. Although the FAR provides for the use of time and materials (T&M) contracts under part 12 commercial contracts, DoD policy discourages it's use and therefore T&M should only be used in those rare circumstances where it is justified.

14.3.2.2.1.1. Fixed-Price Contract Types

As a general rule, contracts for routine services, or efforts involving stable requirements, manageable performance risk, are normally a fixed-price type. Work must meet minimum stated performance standards. Service must be delivered within a specified time and meet the performance standards in the contract. Price should be supported by robust competition or recent competitive pricing history.

The contract price represents full payment for the work. Exceeding this amount is at the

contractors own risk and expense. This type of contract is used when technical and cost can be accurately estimated (i.e., low or predictable risk). It is also the most appropriate type of contract to use when work can be clearly defined (or when the requirement is constant with no need for flexibility). The contractor bears full responsibility for the performance costs and resulting profit (or loss).

14.3.2.2.1.2. Cost Reimbursement Contract Types

Cost type contracts are used when requirements cannot be accurately defined and performance risk is not easily quantified or managed. These types of contracts require the contractor to deliver their best effort to provide the specified service. Reasonable, allowable, allocable costs will be reimbursed, up to the total estimated amount specified in the contract. This amount represents an estimate of total costs, including fee, as a not-to-exceed ceiling that cannot be exceeded without contracting officer approval. When using a cost type contract ensure that the contractor has an adequate accounting system and the government monitoring during performance provides assurance of efficient methods and effective cost controls. Cost contracts place more risk on the government because the contractor bears less responsibility for completing the performance requirement within the established cost ceiling.

Two common types of Cost Plus Fixed Fee (CPFF) contracts for services are either completion or term.

- CPFF Completion: If the contractor fails to complete the contract within time or budget, then the government pays only additional costs, but no additional fee to complete the effort. This is an incentive since contractors are in business to earn fees. This type of CPFF contract is applicable when there is a clearly defined result at the outset, but there are considerable unknowns with risks that need to be shared.
- CPFF Term: This form of CPFF contract allows you to describe the scope of work in general terms and the contractor will be required to perform a specified level of effort in a given period of time.

14.3.2.2.2. Incentives - Recognize the Power of Profit as a Motivator

Incentives will drive behavior so one of the keys to effective incentives involves recognizing that the actions of the private sector are motivated by profit. The government relies on industry to provide customers with products and services. We have regulations, policies, and procedures that allow industry to be compensated for these efforts. One contractor was heard to say, "You give us the incentive, we will earn every available dollar." It is important to understand the cause and effect relationship between contractor performance and the type of incentive used. In another words, whatever your team decides to incentivize, that is the area in which the contractor will focus or concentrate on, so your team needs to assure that you are creating a behavior that will deliver the right mission results.

For example, link the incentive program to high priority or high risk performance requirements with measureable metrics. Then, incorporate share-in-savings strategies that reward the contractor for suggesting innovations that improve performance and reduce total overall cost. Develop an acquisition approach that aligns the interests of both parties. In other words develop a strategy in which both the contractor and the government benefit from economies, efficiencies, and innovations delivered during contract performance. If the incentives are right, and if the contractor and the agency share the same goals, risk is largely controlled and effective performance is almost the inevitable outcome. The key to incentives is to make them work for both parties.

Performance Incentives: These are incentives designed to relate profit or fee to results achieved by the contractor in relation to identified cost-based, performance or schedule based targets. For example, a large Cost Plus Incentive Fee, Base Operating Support contract, contained an incentive provision for sharing cost savings generated by the contractor, on a 50/50 basis, when actual costs came in under target cost. In each year of a five-year contract the contractor delivered cost savings earning additional fee for the contractor and cost savings for the installation. This incentive structure also put the contactors base fee at risk if performance suffered as a result of cost cutting. Schedule incentives focus on getting a contractor to exceed delivery expectations with either quality, or timeliness. These can be important on construction or maintenance requirements. They can be defined in terms of calendar days or months, attaining or exceeding milestones, or meeting urgent requirements.

Award Fee Contract Arrangements: This type of incentive uses an award fee plan that contains the criteria for earning the incentive. Generally, award fee contracts should only be used when objective incentive targets are not feasible for critical aspects of performance, judgmental standards can be fairly applied, and potential award fees would provide a meaningful incentive to motivate the service provider to perform.

Past Performance: Past performance documentation and reporting is a no cost incentive for the government. Maintaining a record of good past performance always motivates contractors. This information affects decisions to exercise options and future contract awards. Past performance assessments are a quick way for motivating improved performance or to reinforce exceptional performance. Keep in mind that the integrity of a past performance evaluation is essential.

Small Business Participation Incentives: There will be times when the nature or value of an acquisition exceeds the ability for small business to be the prime contractor. Large prime contractors develop subcontracting plans in accordance with FAR 19.702 where the use of small business provides value to the government. DoD can incentivize prime contractors to achieve their small business subcontracting goals thus supporting a healthy industrial base for future competition. One means to this end is to use actual small business participation as a factor or sub-factor in best value source selections. Finally, the government needs follow up and ensure that small businesses that are featured in prime contractor proposals as prospective subcontractors are actually successful in attaining subcontract awards if the prime contractor is awarded the

contract.

14.3.2.2.2.1. Positive and Negative Incentive Examples

The government can incentivize the contractors performance on just about any contractual aspect, so long as that performance incentive provides ultimate benefit to the government. Ultimately, whatever incentives you prescribe must be based on predetermined, objective performance standards that you can quantify, measure, and perform surveillance as needed. The list below provides examples of positive and negative ways to use incentives:

Positive:

- When performance exceeds standard, pay x% of monthly payment into pool. At the end of y months, pay contractor amount accrued in pool.
- When performance exceeds standard, pay x% of monthly payment into pool. When pool has reached y dollars, pay contractor amount accrued in pool.
- When performance has exceeded the standard for x consecutive months, reduce government oversight or contractor reporting, as appropriate.
- Document past-performance report card, paying particular attention to performance that exceeded the standard.

Negative:

- When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the government.
- When performance is below standard for a given time period, x% of the periods payment will be withheld or deducted.
- When performance is below standard for x consecutive months, increase surveillance or contractor reporting.
- Document past-performance report card, paying particular attention to performance that failed to meet the standard.

14.3.2.2.2.2. Considerations When Contemplating Incentives

Make sure incentives are realistic and attainable. They must focus on achieving the service acquisition objectives, taking into account the mission, the key characteristics, and other unique features of the service. The acquisition team may jointly develop and negotiate these incentive criteria with contractor(s) and all potential stakeholders so that all parties buy in to the merits of this approach. Additionally, soliciting stakeholders input and feedback will help identify what the customer feels are most important. Understand that a contractor will not spend a dime to earn a nickel. Here are some best practice questions the team should address when developing an incentive strategy:

- Is the incentive consistent with the mission, goals, and operational requirements?
- Will it deliver additional value to the mission?

- Which areas of the requirement would benefit most from enhanced performance?
- Which areas do not need added incentives (or which areas can do without)?
- Is your agency willing to pay more to achieve a level of performance beyond the performance standard? Is the incentive affordable?
- Is what we want to incentivize measurable?
- How accurately can we capture and record performance data?
- Is there potential for using cost-sharing?
- Will it affect timelines or schedules in a positive way?
- Does the strategy work to benefit both parties?
- Does the contractor have complete control of performance?

14.3.2.2.3. Determine How You Will Select a Contractor

There are two primary best value methods of selecting a contractor. One of the goals of PBA is to achieve the highest degree of quality and efficiency at a reasonable price. Best-value source selections allow the government to establish factors used to evaluate contractor proposal submissions. These two types of selection methods are:

Low Price Technically Acceptable (LPTA): The government establishes minimum technical criteria and standards for determining which offeror's are technically acceptable. Among those that are determined to be technically acceptable, the contract is awarded to the offeror with the lowest price. One limitation with this approach is that there is no consideration for better technical solutions; the award is based primarily on price.

Trade-off Method: This process allows for consideration of technical, past performance and cost factors. The contract is awarded to the offeror that represents the best value in accordance with the evaluation criteria contained in the RFP. This process provides for tradeoffs between technical factors and price. Using this method allows the source selection authority (SSA) to select a contractor that represents the best value versus low cost.

Both methods enable the acquisition team to define evaluation factors to be used in selecting the successful offeror. The key to successful use of any evaluation factor is to establish a clear relationship between the PWS, Section L of the solicitation (*either FAR Part 12 Acquisition of Commercial Item or FAR Part 15 Contracting by Negotiation*), and Section M of the solicitation (Evaluation Factors for Award). The evaluation factors selected should link clearly with the PWS and represent those areas that are important to stakeholders or have been identified as high risk during risk analysis. A good rule of thumb is to look at the roadmap you have completed and make an assessment as to which HLOs and tasks are the highest risk, highest priority or most critical and should carry the most weight. The Departments standard source selection procedures are found at DFARS 215.300 .

14.3.2.3. Allocate Workload Within the Acquisition Team

Either best value selection process involves a significant investment in manpower to develop the selection criteria and conduct the technical and cost evaluations. Make sure you have resource commitments in both people and facilities to conduct your proposal evaluations. People involved in the technical evaluations should have good technical backgrounds, yet be open to new approaches they may see in contractor proposals. DAUs continuous learning course CLC007, Contract Source Selection, can provide more information on conducting source selections.

14.3.2.4. Prepare Acquisition Planning Documents

The key documents are the Acquisition Plan, the Acquisition Strategy, and the Source Selection Plan. The acquisition plan is prescribed by the FAR and it spells out the business case for the selected acquisition approach. It utilizes all the information generated from the planning phase such as the nature of the requirement, risk areas, customer concerns, and market analysis to support the plan. Acquisition plans for services must also describe strategies for implementing PBA methods or provide a rationale for not using them and provide a rationale if contract type is other than firm-fixed price (FFP). The acquisition plan also communicates the requiring activities approach to higher approval levels. These authorities will likely ask the following questions:

- Is the plan consistent with current DoD priority and/or policies? (For example, providing for full and open competition, small business set-aside competition and the appropriate use of fixed-price type contracts.)
- Is the plan executable?
- Are the top-level objectives appropriate and in the best interest of the Government?

The acquisition plan and the acquisition strategy serve as a permanent record of decisions made regarding the acquisition strategy for future reference. Acquisition strategies for services are prescribed by DoD Instruction 5000.02 (Enclosure 9).

The source selection plan outlines the membership, evaluation factors, and provides a description of the evaluation process, including specific procedures and techniques to be used in evaluating contractor proposals. Both documents require approvals in accordance with agency procedures.

14.3.2.5. Consider use of Draft Request for Proposal (RFP)

Issuing a draft RFP is an effective way to get industry feedback. The draft RFP contains both the requirement and the proposed business strategy that you are contemplating. You can request feedback on both. Drafts provide any interested party with an opportunity to provide comments before the actual acquisition process starts. The government can benefit from this process by considering the industry feedback and how

it could improve the acquisition. It also gives potential contractors an opportunity to get an early start on planning and proposal development since we often give contractors the minimum 30 days to prepare a proposal once we issue the formal RFP.

The primary disadvantage is the time required to issue the draft and evaluate industry comments, so plan accordingly if you anticipate using this very effective technique.

14.4. The Execution Phase

14.4.1. Step Six Execute the Strategy

14.4.1.1. Issue Request for Proposal (RFP) or Military Interdepartmental Purchase Request

14.4.1.2. Conduct Source Selection

14.4.1.2.1. Instructions to Offeror's

14.4.1.2.2. Section L

14.4.1.2.3. Section M Evaluation Factors for Award

14.4.1.2.4. Relationship between PWS, Section L, and Section M

14.4.1.2.5. Role of Past Performance in Best Value Procurements

14.4.1.3. Pre-Award Approval Documents

14.4.1.4. Contract Award

14.4.1.5. Debrief Unsuccessful Offeror's

14.4.1.6. Finalize Quality Assurance Surveillance Plan (QASP)

14.4.1.7. Post-Award Implementation/Transition

14.4. The Execution Phase

14.4.1. Step Six - Execute the Strategy

Figure 14.4.1.F1. Model of Step Six

14.4.1.1. Issue Request for Proposal (RFP) or Military Interdepartmental Purchase Request

The formal acquisition process starts with the issuance of the final RFP or if the acquisition team has determined to use another activity's acquisition vehicle to complete their action the issuance of a MIPR. FAR Part 15.201 states After release of the solicitation, the contracting officer must be the focal point of any exchange with potential offeror's. When specific information about a proposed acquisition that would be necessary for the preparation of proposals is disclosed to one or more potential offeror's, that information must be made available to the public as soon as practicable, but no later than the next general release of information, in order to avoid creating an unfair competitive advantage.

14.4.1.2. Conduct Source Selection

The objective of source selection is to select the offeror, whose proposal represents the

best value in accordance with the criteria stated in the RFP. The FAR gives the government wide latitude in setting the ground rules for how a contractors proposal will be evaluated and for setting the basis of award.

The RFPs Section L *Instructions to Offeror's* and Section M *Evaluation Factors for Award* provide industry information regarding how to submit their offer and how it will be evaluated. Both of these are critical for a successful acquisition.

14.4.1.2.1. Instructions to Offeror's

Section L of the solicitation is where information and guidance are provided to instruct offeror's how to prepare proposals in response to the solicitation. As previously stated, the PWS, Section L and Section M all tie together. The PWS describes the requirement. Section L requests information relating to how the offeror will execute that requirement, for evaluation purposes. Section M describes how their proposal will be evaluated for source selection purposes.

14.4.1.2.2. Section L

You MUST explain in section L of the RFP the structure in which the offeror's will submit their proposals (proposal instructions), and the requirement to specifically address those areas that will be evaluated and scored/rated during the source selection.

Proposal instructions: The instructions for submission of proposals should be complete and thorough, but not overly long, complex, or restrictive. Submission instructions vary, but most agencies have a standard or preferred format that is familiar to contracting officers and evaluators. For example, proposals may be submitted via disks, electronic media, orally, or in paper based form.

Contents of instructions: The most common content items to be prescribed in the instructions include the following: number of volumes, page limit's, font, spacing, and other layout instructions.

Number of volumes: You should determine how many proposal volumes you want the contractor to submit. Proposal volumes can consist of technical, quality control plan, past performance and cost.

Page limit's: Technical and business proposals can be very difficult to evaluate because of their great size and bulk, much of which may be caused by repetition. Placing a limit on the number of pages each proposal may contain reduces this problem. The typical limit is 50 to 100 pages, but be sure that the technical personnel concur that the technical and business approaches can be adequately explained within the limit's that have been established.

Font, spacing, and other layout instructions: Instructions for these areas enforce a certain uniformity of appearance for proposals so evaluators will not be unduly

influenced by a flashy layout, but will find it easier to concentrate on the essentials. However, do not impose unnecessary restrictions on the contractors ability to communicate the necessary information in their proposals (i.e., complicated charts and graphics).

Evaluation areas: Instructions should clearly require contractors to thoroughly address all evaluation areas. It is important for the contractor to know exactly what is going to be evaluated and what should be included in each volume of the proposal.

Oral presentations: Oral presentations are verbal submissions of proposal information. This information is used to determine the offeror's understanding of the requirements and it's capability to perform. When using oral presentations have the presenter be the proposed program manager and not a professional speaker.

14.4.1.2.3. Section M Evaluation Factors for Award

Section M is uniquely tailored for each procurement and is intended to give offeror's guidance concerning the basis of award. You must explain all the evaluation factors and significant sub-factors that will be considered in making the source selection along with their relative order of importance (see FAR 15.304). Section M must clearly state whether all evaluation factors, other than cost or price, when combined, are significantly more important than, approximately equal to, or significantly less important than cost or price.

Evaluation Factors/Sub-Factors: Be sure that section M is clear and complete in describing the evaluation factors and significant sub-factors to be used. Each factor/sub-factor must be fully explained, and their relationship to each other (relative importance) must be clearly stated. The goal here is to make the offeror's fully aware of how the source selection will be made.

One of the main challenges in determining best value is assessing performance risk. This is challenging because the offeror's may be proposing different approaches that can be difficult to compare (an apples to oranges comparison). While Section M of a solicitation provides the basis for evaluation, there is no precise science to assessing dissimilar approaches toward fulfilling a PBA requirement.

14.4.1.2.4. Relationship between PWS, Section L, and Section M

The PWS, Section L, and Section M must all tie together. The PWS describes the requirement. Section L requests information relating to how the offeror will execute that requirement for evaluation purposes and Section M describes how the proposal will be evaluated for source selection purposes. The following example, Table 14.4.1.2.4.T1., describes one piece of a requirement to illustrate the relationship between the three areas.

Table 14.4.1.2.4.T1. Sections L and M Relationship Example

Performance Work Statement	Section L	Section M
Provide taxi service so that pickup time is within 5 minutes of request time, 95% of the time.	The offeror shall describe how taxi service will be provided in accordance with the stated requirement.	The agency will evaluate the offeror's approach for meeting the standards for taxi service. The offer will be evaluated for best value, in terms of technical merit and cost, with additional consideration for the offeror's relevant and recent past performance (track record).

14.4.1.2.5. Role of Past Performance in Best Value Procurements

The FAR mandates that government assess contractors past performance in order to use this information as a significant evaluation factor in the source selection process. Past performance data is an influential factor in motivating contractors toward excellence. The essential premise is that a record of good performance is an important predictor of future performance. When evaluating large business past performance an additional factor to consider is how effective they have been in meeting their small business subcontracting goals.

For those situations where an offeror has no past contract performance or the performance information is either unavailable or irrelevant, the FAR states that the offeror may not be evaluated either favorably or unfavorably on the past performance factor.

14.4.1.3. Pre-Award Approval Documents

These actions vary depending on the dollar value of the acquisition and organization policy. They may include pre-award surveys, pre-negotiation business clearances and Congressional notification, depending on the amount of the award.

14.4.1.4. Contract Award

Upon receipt of all required pre-award approvals and completion of required notifications, the contracting officer executes the contract. To give publicity to the award and recognize the team members, a formal contract signing ceremony often is conducted. This particularly is desirable in large and/or complex acquisitions.

14.4.1.5. Debrief Unsuccessful Offeror's

FAR Section 15.5 requires that all unsuccessful offeror's be given an opportunity for a

debriefing concerning their proposal and how they can improve their chances in future procurements. Debriefings are conducted following contract award notification by the contracting officer and lead technical evaluator from the technical evaluation team.

14.4.1.6. Finalize Quality Assurance Surveillance Plan (QASP)

Once a contractor has been selected, the QASP needs to be updated and finalized. If any significant changes were made to the performance requirements during the competition, the QASP needs to be updated to reflect the final requirement. Also now include the contractors information and the names and role of their key personnel. If a quality control (QC) plan was a required and evaluated as part of the contractors proposal package, the team may consider including the contractors compliance with their QC plan as an assessment area in the QASP. Make sure the COR has been appointed and completed all required training prior to contract award.

14.4.1.7. Post-Award Implementation/Transition

Following contract award, it's advisable to conduct a "kick-off meeting" or more formally, a "post-award conference," attended by those who will be involved in contract performance. This meeting will help both agency and contractor personnel achieve a clear and mutual understanding of contract requirements and further establish the foundation for good communications and a win-win relationship. It is very important that the contractor become part of the team, and that agency and contractor personnel work closely together to achieve the mission results embodied in the contract.

14.4.2. Step Seven Performance Management

14.4.2.1. Transition to Performance Management

14.4.2.2. Manage and Administer Overall Program

14.4.2.3. Manage Performance Results

14.4.2.3.1. Monitor Contract Performance

14.4.2.3.2. CPARS Report and Past Performance Information Retrieval System (PPIRS)

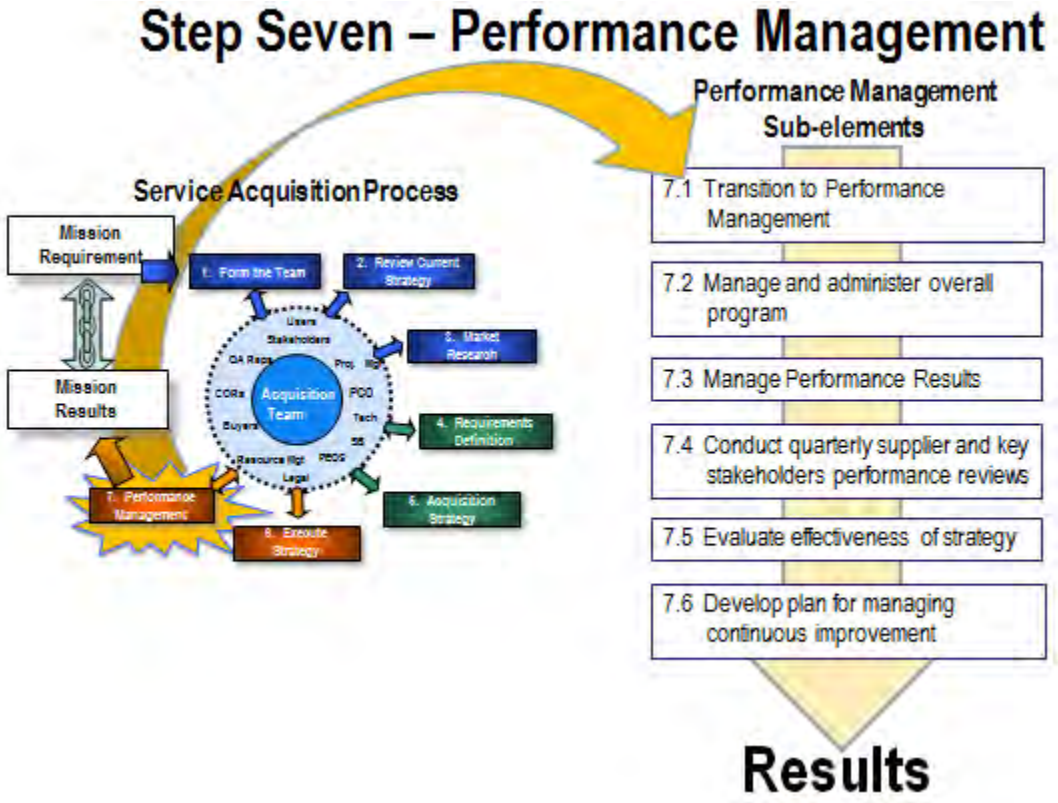
14.4.2.4. Conduct Quarterly Supplier and Key Stakeholders Performance Reviews

14.4.2.5. Evaluate Effectiveness of Strategy

14.4.2.6. Develop Plan for Managing Continuous Improvement

14.4.2. Step Seven Performance Management

Figure 14.4.2.F1. Model of Step Seven



Steps One through Six have prepared you for this step. Step Seven delivers the performance results your stakeholders need to successfully support their mission. It's not time to declare victory and move on. Your engagement with your contractor and stakeholders will often cover several years.

There are two key elements to this step. First are the basic functions of administering the contract such as validating contractor invoices, tracking cost data when required, managing change as it occurs and making sure the contractor is getting paid on a timely basis. The second key function is managing the relationship and expectations between three key groups; customer's, stakeholders and the contractor. Developing an environment of trust and fair play is vital to keeping all parties focused on achieving the intended mission results. This includes assessing performance using the QASP, documenting performance for any incentive arrangement you may have created, and finally making sure performance is documented annually in the government past performance database with a fair and objective Contractor Performance Assessment Reporting System (CPARS).

14.4.2.1. Transition to Performance Management

As new contract performance starts the team must shift from acquisition to performance management. This means focusing on ensuring that the performance results contained in the contract are delivered. To accomplish this effectively, everyone involved clearly understands their role and responsibilities in completing the assessment strategies contained in the QASP. The two key responsible parties are the contracting officer and the COR.

Contracting officers have specific responsibilities that can't be delegated or assumed by the other members of the team. These include, for example, making any commitment relating to an award of a task or contract; modification; negotiating technical or pricing issues with the contractor; or modifying the stated terms and conditions of the contract. The contracting officer relies on the COR to be his/her eyes and ears for providing an accurate assessment of contractor performance.

The duties and responsibilities of the COR are contained in a designation letter signed by the contracting officer. Make sure the COR and anyone else involved with monitoring contract performance has read and understands the contract and has the training, knowledge, experience, skills, and ability to perform his/her roles. The COR must know the performance requirements and standards in depth and understand the assessment strategies contained in the QASP. The COR should also be effective communicators with good interpersonal skills.

To complete the transition, incorporate the contractor into the performance management team. An essential element of performance management is open and frequent communication between the government and the contractor. Make sure that the contractor clearly understands how performance is being measured to ensure there are no surprises. Remember the contractors successful performance is your goal too. At its most fundamental level, a contract is much like a marriage. It takes work by both parties throughout the life of the relationship to make it successful. Characteristics of strong relationships include the following:

- Trust and open communication
- Strong leadership on both sides
- Ongoing, honest self-assessment
- Ongoing interaction
- Creating and maintaining mutual benefit or value throughout the relationship

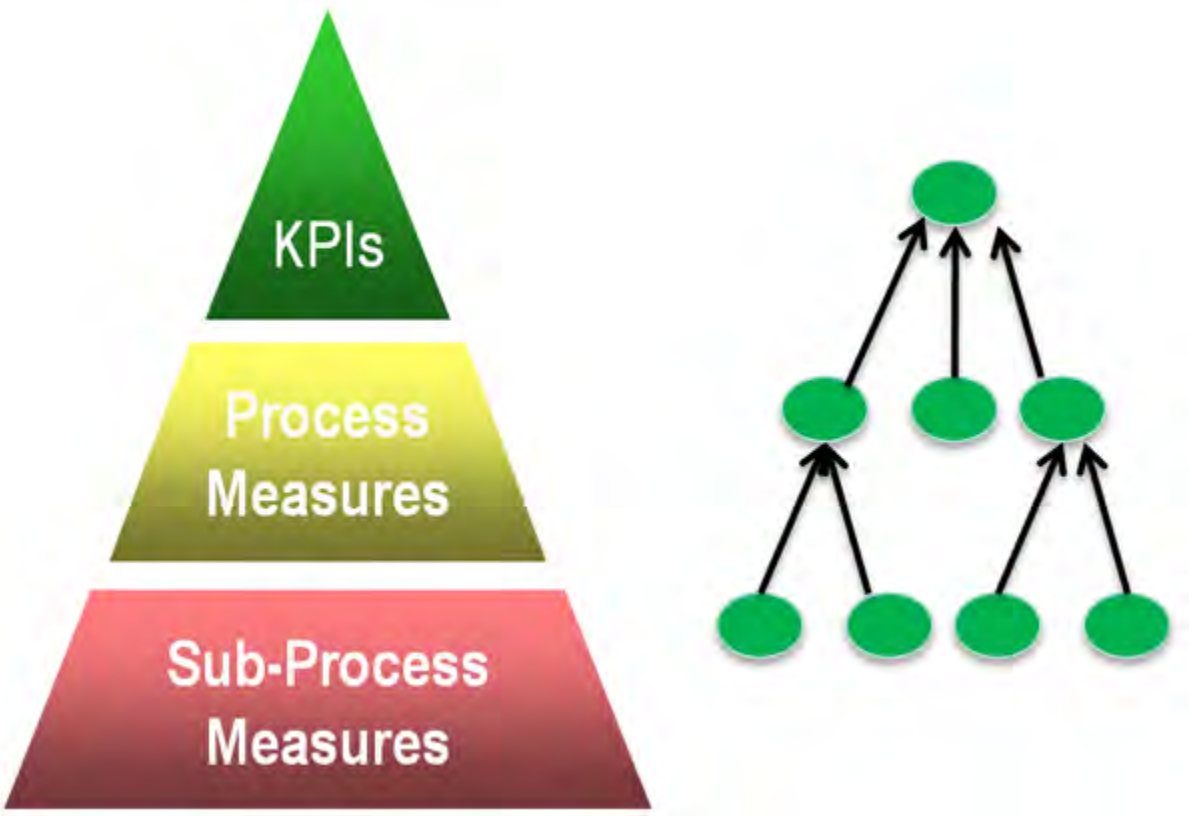
14.4.2.2. Manage and Administer Overall Program

If your requirement involves a contract vehicle that uses task orders for individual requirements make sure you develop a plan to capture performance at the task order level. This task order performance information should flow up the contract level to be captured and reported.

14.4.2.3. Manage Performance Results

Following contract award you should review your communication plan and determine how and to whom you will report contractor performance information. It's vital to keep the communication links open with both your contractor and stakeholders throughout the performance period of the contract. Establish regularly scheduled meetings with the contractor to keep everyone informed of pending actions that could impact performance such as scheduled exercises and IG visit's. Discuss any issues the contractor may have such as invoicing or payment problems. Identifying potential problems early is a key way to keep them from having performance impacts. Implement the performance reporting structure you developed in Step Four.

Figure 14.4.2.3.F1. Performance Management



- **KPIs:** The few essential performance results that leadership will use to assess performance.
- **Process Measures:** What performance metrics will process stakeholders use to determine if their areas of responsibility are meeting standards? Make sure they link to specific PWS performance tasks.
- **Sub-Process Measures:** What results metrics will sub-process stakeholders or office chiefs use to asses performance in their areas of responsibility and how

well current performance is supporting the process stakeholder?

14.4.2.3.1. Monitor Contract Performance

How you capture and report performance information is critical for two reasons. First, it keeps your stakeholders well informed based on actual performance results as measured by your CORs. Second, it provides the documented performance trends and results to have an open and honest discussion with your contractor concerning the results being achieved. Performance reviews should be held on a regular basis with both your stakeholders and your contractor. The frequency of stakeholder reviews is often dictated by the importance or complexity of the service under contract. Quarterly performance reviews with stakeholders should be a minimum. More complex acquisitions may require monthly reviews.

Fact based communication is an essential element in developing a trusting relationship with your contractor. These routine reviews are focused on keeping performance on course, reporting performance results, and making adjustments as necessary. For most contracts, monthly contractor performance reviews would be appropriate. For contracts of extreme importance or contracts in performance trouble, more frequent meetings may be required. During this review, the acquisition team should be asking these questions:

- Is the contractor performance meeting or exceeding the contract's performance standards?
- Are there problems or issues that we can address to mitigate risk?

There should be time in each meeting where the agency asks, "Is there anything we are requiring that is affecting your performance in terms of quality, cost, or schedule?" Actions discussed should be recorded for the convenience of all parties, with responsibilities and due dates assigned. At each review point the QASP should be reviewed to see if the approach to the inspection should be changed or revamped. If an objective or standard needs to be changed, then it is appropriate that both parties agree to any modification, however, the change may have a cost impact.

14.4.2.3.2. CPARS Report and Past Performance Information Retrieval System (PPIRS)

A CPARS report is an annual requirement on contracts valued over the simplified acquisition threshold. CPARS should be an objective report of the contractors performance during a period against the contract performance standards. Your CPARS report goes into the PPIRS database which collects past performance information (PPI). PPI is one of the tools used to communicate contractor strengths and weaknesses to source selection officials and contracting officers. Communication between the government and contractor during the performance period is essential. The contractor performance evaluation contained in the PPIRS is a method of *recording* contractor

performance and should not be the sole method for reporting it to the contractor.

If you've been conducting regular performance reviews with your contractor there should be no surprises at the end of the performance period about what rating the contractor will receive. These ratings are very important to a contractor; they can affect future business opportunities. That's why you need to have the facts and data to support ratings above or below satisfactory.

Consult the DoD PPIRS guide for more information.

14.4.2.4. Conduct Quarterly Supplier and Key Stakeholders Performance Reviews

A best practice concerning service contracts is to schedule regular reviews with your key stakeholders and contractor. Your communication plan should now reflect the schedule for these reviews. As has been mentioned several times already, good communication is absolutely essential. That's why a regularly scheduled review is important. It provides an opportunity to discuss current performance with the stakeholder. It also offers a chance to gain insight on projected changes that might require a change to the current contract. Being proactive is better than the best reactive strategy.

14.4.2.5. Evaluate Effectiveness of Strategy

As performance periods advance, the acquisition team should assess the effectiveness of the strategy that was originally developed to see if it is still achieving the required mission results. What should be changed or modified during the next acquisition cycle to improve mission results? Keep a record of what improvements could be made the next time because before you know it, it will be time to start the acquisition process all over again.

14.4.2.6. Develop Plan for Managing Continuous Improvement

Service contracts tend to have performance periods lasting several years. Continuous improvement should be one of the acquisition teams goals. For example, plan on regular meetings with the contractor to identify actions both parties can take to improve efficiency. This might include the identification of significant "cost drivers and what improvement actions could be taken. Sometimes agencies require management reporting based on policy without considering what the cost of the requirement is. For example, in one contract, an agency required that certain reports be delivered regularly on Friday. When asked to recommend changes, the contractor suggested that report due date be shifted to Monday because weekend processing time costs less. This type of collaborative action will set the stage for the contractor and government to work together to identify more effective and efficient ways to measure and manage the performance results over the life of the contract.

Appendix A -- REQUIREMENTS ROADMAP WORKSHEET

Requirements Roadmap Worksheet Sample

Appendix B -- SERVICE ACQUISITION PROJECT PLAN

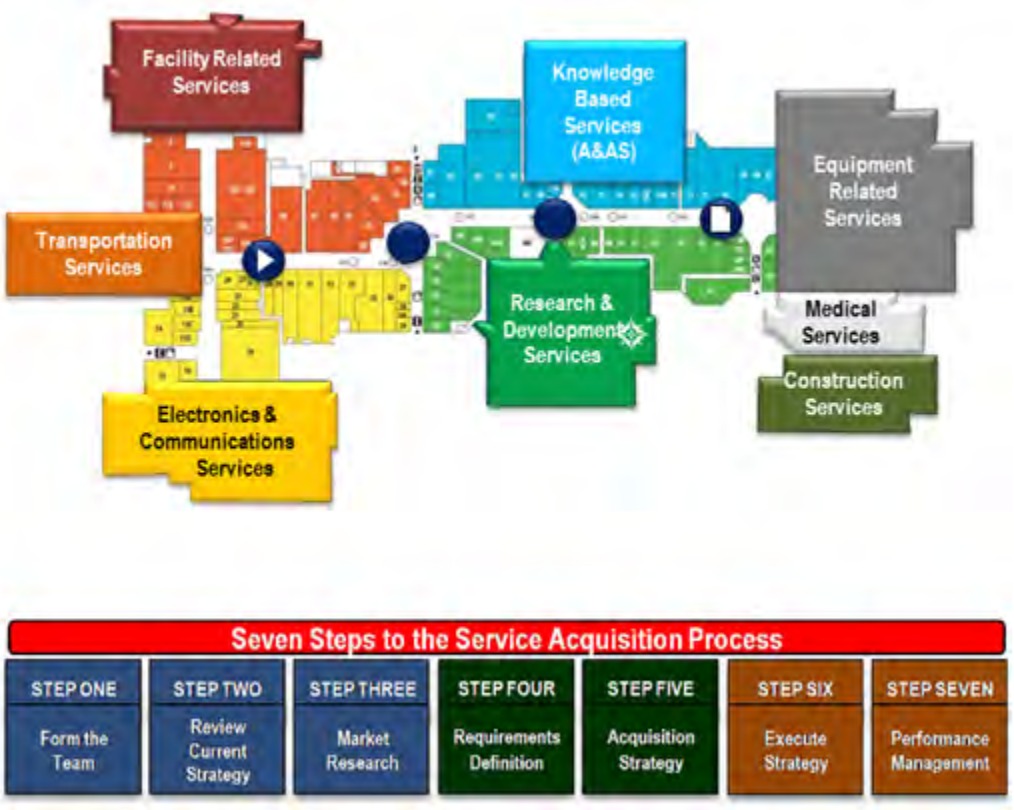
Service Acquisition Project Plan Sample

Appendix C -- SERVICE ACQUISITION MALL (SAM)

Welcome to SAM, DAUs Service Acquisition Mall .

SAM is intended to help you get your job done by providing usable tools and templates to create your performance-based service acquisition requirements. Each of the Wings on the mall map below contains information related to a category of services. Move your mouse over the elements of the mall map to discover what is available in SAM. Enter the Wing by simply clicking on the appropriate space.

Figure 14.Appendix C.1. Model of SAM



Appendix D -- MARKET RESEARCH RESOURCES

You may find this list of sources helpful when conducting your market research:

Central Contractor Registration, http://sam.gov

Commercial Advocates Forum, http://www.acq.osd.mil/

Federal Information Exchange, http://www.ssa.gov/gix/

Acquisition Reform Net, http://www.acquisition.gov/

Thomas Register, http://www.thomasnet.com

Department of Commerce, http://www.commerce.gov/

GSA eLibrary, http://www.gsaelibrary.gsa.gov/

Small Business Administration, http://www.sbaonline.sba.gov

SBA-Dynamic Small Business Search, http://dsbs.sba.gov/dsbs/search/dsp_dsbs.cfm

Consumer Reports, http://www.consumerreports.com

National Contract Management Association, http://www.ncmahq.org

Dow Jones Business Information Services, http://www.dowjones.com

Standard & Poor's Research Reports, http://www.standardandpoors.com/home/en/us

Manufacturers Information Network, http://www.manufacturing.net

National Association of Purchasing Managers, http://www.ism.ws/

National Yellow Pages, http://www.yellowpages.com

Federal Business Opportunities, http://www.fbo.gov

Government Contracts Directory, http://www.contractdirectory.gov /contractdirectory/

DoD market research, http://acc.dau.mil/CommunityBrowser.aspx?id=18892

Other Helpful Web Sites:

http://www.imart.org/ : A collection of search engines, directories, and databases to aid

in market research

http://superpages.com : Yellow pages of 16 million U.S. businesses

http://switchboard.com : Business search engine

http://www.techweb.com : More than 100 links to industry, focused on electronics

Appendix E -- GLOSSARY

A&AS	Advisory and Assistance Services
AQL	Acceptable Quality Level
CDRL	Contract Data Requirements List
CLM	Continuous Learning Module
CO	Contracting Officer
CONUS	Continental United States
COR	Contracting Officers Representative
CPARS	Contractor Performance Assessment Reporting System
CPFF	Cost Plus Fixed Fee
DAU	Defense Acquisition University
DoD	Department of Defense
DFARS	Defense Federal Acquisition Regulation
DPAP	Defense Procurement and Acquisition Policy
FAR	Federal Acquisition Regulation
FFP	Firm-Fixed-Price
FTE	Full-Time Equivalent
GFE	Government Furnished Equipment
GFM	Government Furnished Material
GFP	Government Furnished Property
GPS	Global Positioning System
HQ	Headquarters
IGE	Independent Government Estimate
KPI	Key Performance Indicators
LPTA	Low Price Technically Acceptable

MIPR	Military Interdepartmental Purchase Request
MOU	Memorandum Of Understanding
OCONUS	Outside Continental United States
OSD	Office of the Secretary of Defense
PBA	Performance-Based Acquisition
PM	Program Manager
PPI	Past Performance Information
PPIRS	Past Performance Information Retrieval System
PRS	Performance Requirement Summary
PWS	Performance Work Statement
QAE	Quality Assurance Evaluator
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
R&D	Research and Development
RFI	Request for Information
RFP	Request for Proposal
SAM	Service Acquisition Mall
SAT	Simplified Acquisition Threshold
SAW	Service Acquisition Workshop
SBA	Small Business Administration
SBS	Small Business Specialist
SOO	Statement of Objectives
SOW	Statement of Work
SSA	Source Selection Authority