DEPARTMENT OF THE AIR FORCE

WASHINGTON DC

OFFICE OF THE SECRETARY

AFMAN17-1402_AFGM2018-01

9 May 2018

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 AF Pentagon
Washington DC, 20330-1800

SUBJECT: Air Force Guidance Memorandum (AFGM) to AFMAN 17-1402, Air Force Clinger-Cohen Act (CCA) Compliance Guide

By Order of the Secretary of the Air Force, this AFGM immediately changes Air Force Manual 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 24 Oct 2012. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

As a result of the publication of AF Policy Directive 17-1, Information Dominance and Cyberspace Governance and Management, which supersedes AFPD 33-4, Information Technology Governance, dated 17 Jan 2013, AFMAN 33-407, is hereby renumbered as AFMAN 17-1402. The title and content remain unchanged. I hereby direct the Office of Primary Responsibility (OPR) for AFMAN33-407 to conduct a special review in accordance with AFI33-360 to align its content with AFPD17-1. This will result in a rewrite or rescind action of AFMAN33-407.

In response to guidance changes in DoDI 5000.02, *Operations of the Defense Acquisition System* and DoDI 5000.75, *Business Systems Requirements and Acquisition*, this guidance memorandum changes the Air Force oversight process for CCA compliance, see Attachment 1.

This memorandum becomes void after one-year has elapsed from the date of this memorandum, or upon publication of an interim change or rewrite of the affected publication, whichever is earlier**.**

BRADFORD J. SHWEDO, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Attachments:
1. CCA AFMAN 17-1402 Air Force Oversight Guidance
2. CCA Assertion Memorandum Template
3. CCA Compliance Table Template

AFMAN17-1402_AFGM2018-01

Attachment 1

Paragraphs 2.4.1, 2.4.2, and paragraph 3 to include all sub-paragraphs, figures and tables are deleted from AFMAN 17-1402. SAF/CIO A6 CCA Confirmation Memorandum signature is no longer required as of the publication date of this AFGM. Roles and responsibilities are as follows:

a. SAF/CIO A6X serves as the POC for SAF/CIO A6 and SAF/FMC participation in the CCA process as it pertains to elements 6, 8, 9 and 11 of the CCA compliance table referenced in DoDI 5000.02.

b. SAF/FMC retains approval and policy responsibility for element 6 and SAF/CIO A6 retains approval and policy responsibility for elements 8, 9 and 11 of the CCA compliance table referenced in DoDI 5000.02.

c. Program Managers will sign a CCA assertion memorandum to report CCA compliance for all elements to the Milestone Decision Authority and SAF/CIO A6 or their designee, accompanied by a CCA compliance table referenced in DoDI 5000.02.

Attachment 2

CCA ASSERTION MEMORANDUM TEMPLATE

_____
(date)

MEMORANDUM FOR (Milestone Decision Authority Organization)

SUBJECT: Clinger–Cohen Act (CCA) Compliance for the (Name of Program)

Attached to this memorandum are the CCA Compliance Table and associated links to the supporting documentation for the (Name of Program) that enable the Milestone Decision Authority to assess and confirm that the (Name of Program) is being developed in accordance with Subtitle III of Title 40 U.S.C. (formerly Division E of the Clinger-Cohen Act (CCA) of 1996) and DoDI 5000.02.

I have reviewed the attached documentation and assert that it is ready for assessment and confirmation. My POC for CCA compliance is (name, e-mail, phone number).

_____
(Signature of Program Manager)
(add signature block)

Attachment 3

NAME OF PROGRAM)
CLINGER-COHEN ACT (CCA) COMPLIANCE TABLE

Required to Comply With the CCA (Subtitle III of title 40 of U.S. Code (Reference (p)))	Applicable Program Documentation
1. Make a determination that the acquisition supports core, primary functions of the DoD.	
2. Establish outcome-based performance measures (OBPM) linked to strategic goals.	
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of commercial off-the-shelf technology.	
4. Determine that no private sector or government source can better support the function.	
5. Conduct an analysis of alternatives.	
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.	
7. Develop clearly established measures and accountability for program progress.	
8. Ensure that the acquisition is consistent with the DoD Information Enterprise policies and architecture, to include relevant standards.	
9. Ensure that the program has a Cybersecurity Strategy that is consistent with DoD policies, standards and architectures, to include relevant standards	
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.	
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO.	

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-407

24 OCTOBER 2012

Communications and Information

AIR FORCE CLINGER-COHEN ACT (CCA) COMPLIANCE GUIDE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at **http://www.e-publishing.af.mil/.**

RELEASABILITY: There are no releasibility restrictions on this publication.

OPR: SAF/A6PPB

Certified by: SAF/A6PP
(Lt Col Hewett Wells)
Pages: 46

This publication implements Air Force Policy Directive (AFPD) 33-4, *Information Technology Governance*. It provides guidance for all Air Force military, civilians, and contractor personnel under contract by the Department of Defense (DoD) who are responsible for compliance and reporting for Subtitle III of Title 40 of the Clinger-Cohen Act (CCA) of 1996; Department of Defense Directive (DoDD) 5000.01, The *Defense Acquisition System*; Department of Defense Instruction (DoDI) 5000.02, *Operation of the Defense Acquisition System*; and Directive-Type Memorandum (DTM) 09-025, *Space Systems Acquisition Process*. Implementation of CCA in the Air Force is the responsibility of the Chief of Information Dominance and Chief Information Officer of the Air Force (SAF/CIO A6). This document is intended to assist in the implementation of the guidance documents mentioned above, not as a replacement for them. Specifically, this guidance is designed to clarify the application of the CCA confirmation and compliance requirements to AF programs; delineate the AF CCA compliance and reporting process with clearly defined process steps; and provide the latest CCA requirements, guidance, and techniques for achieving CCA compliance.

This manual applies to all Air Force Active Duty Commands, Reserve, and Air National Guard units. Commands may not change the basic procedures in this manual. Send recommended changes or comments to the Office of Primary Responsibility (OPR), Secretary of the Air Force, Chief of Information Dominance and Chief Information Officer, Policy and Resources Directorate, (SAF/A6PPB), 1800 Air Force Pentagon, Washington, DC 20330-1800, using AF Form 847, *Recommendation for Change of Publication*, with an information copy to SAF/A6PP. Recommended changes or comments can also be sent via e-mail to **safxcppb.business@pentagon.af.mil.** Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management

of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

1. Introduction.

1.1. This document provides guidance for compliance and reporting for Subtitle III of Title 40 of the Clinger-Cohen Act (CCA) of 1996 (also referred to as CCA or Title 40/CCA; this guidance refers to the law as CCA for the purpose of brevity), Department of Defense Directive 5000.01 (The Defense Acquisition System), DoD Instruction 5000.02 (Operation of the Defense Acquisition System), and Directive-Type Memorandum (DTM) 09-025 (Space Systems Acquisition Process, or SSAP). Implementation of CCA in the Air Force is

the responsibility of the Chief of Information Dominance and Chief Information Officer of the Air Force (SAF/CIO A6) as directed in AFPD 33-4, *Information Technology Governance.*

1.2. This document is intended to assist in the implementation of the guidance documents mentioned above, not as a replacement for them. Specifically, this guidance is designed to:

1.2.1. Clarify the application of the CCA confirmation/compliance requirements to AF programs.

1.2.2. Delineate an AF CCA compliance and reporting process with clearly defined process steps.

1.2.3. Provide the latest CCA requirements, guidance, and techniques for achieving CCA compliance.

1.3. CCA is the principal federal law on information technology (IT). Originally enacted as the Information Technology Management Reform Act, Division E of Public Law 104-106, the law's primary purpose is to provide a framework for the role of the CIO in federal agencies and how the CIO should be involved in IT investments or IT acquisitions that support an agency's mission. (The term "investment" is used here to identify an AF activity related to the acquisition, procurement, development, management, operation, or closure of IT. Investment is used in the broadest sense, i.e., to include programs, projects, systems, business systems, family of systems, system of systems, and any other expenditures for IT or IT-related activities.) In accordance with the Foreword to the DoD publication "Clinger Cohen Act of 1996 And Related Documents," May 2000 (also referred to as the "Purple Book"), the Chief Information Officer (CIO) should ensure that IT investments:

1.3.1. Support core mission functions, be undertaken because no alternative private sector or other government source can effectively support the function, and support work processes that have been redesigned or otherwise improved;

1.3.2. Are consistent with the Agency's architecture that integrates work processes and information flows with technology to achieve the Agency's mission and strategic plan;

1.3.3. Reflect a portfolio management approach where decisions on whether to invest in IT are based on potential return, and decisions to terminate or make additional investments are based on performance – much like an investment broker is measured and rewarded based on managing risk and achieving results; and

1.3.4. Reduce risk and enhance manageability by discouraging "grand" information system projects, and encouraging incremental, phased approaches.

1.4. The importance of sections 1.3.1 through 1.3.4 indicates that CCA compliance reporting is more than checking items off of a list. CCA compliance reporting provides an opportunity for Program Managers or Project Managers to demonstrate that their programs are aligned with the Air Force's mission and programmatic objectives, and that the IT investment or acquisition is being implemented according to sound IT and business principles.

2. CCA Coverage of IT Programs.

2.1. CCA defines IT as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement,

control, display, switching, interchange, transmission, or reception of data or information by the executive agency. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. This definition is also applied to National Security Systems (NSS). It does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

2.2. CCA is implemented through, and its requirements are codified in, DoDI 5000.02, Enclosure 5 (see Attachment 2). Enclosure 5 explains that it and CCA apply to all IT investments, i.e., "...all programs that acquire IT, including an NSS, at any Acquisition Category (ACAT) level." Enclosure 5 also limits the authority of the Milestone Decision Authority (MDA) and the DoD Component, stating that "...the MDA shall not initiate a program or an increment of a program, or approve entry into any phase of the acquisition process; and the DoD Component shall not award a contract until" two conditions take place: "(1) the sponsoring DoD Component or PM has satisfied the requirements of Title 40/CCA; and (2) the DoD Component CIO, or designee, confirms Title 40/CCA compliance."

2.3. The CCA approval requirements for Major Defense Automation Programs (MDAP) and Major Automation Information Systems (MAIS) Programs was modified by the DoD-CIO on May 18, 2012 in a memorandum titled "Delegation of Title 40/CCA Confirmations for MDAP/MAIS Programs." Per that memorandum, the DoD-CIO will participate in selected CCA activities to ensure compliance with DoD policies but the Service CIOs will provide the final CCA confirmation/approval on ACAT I programs.

2.4. SAF/CIO A6 exercises its CCA oversight responsibility during four types of formal events:

2.4.1. A MAIS or MDAP submits a Clinger-Cohen Act Compliance Report to SAF/CIO A6 for review and approval prior to a Milestone decision or a major contract award;

2.4.2. During the regular acquisition review process for MAIS or MDAP programs conducted by the Office of Acquisition (SAF/AQ) for Air Force Space and Non-Space programs (in Air Force Review Boards (AFRBs) or Acquisition Strategy Panels (ASPs)).

2.4.3. Concurrent with Defense Business Systems (DBS) certification reviews for AF business systems conducted by SAF/CIO A6 for non-MAIS, non-MDAP programs/systems.

2.4.4. In response to inquiries or under other processes through which a program acquires IT.

2.5. Although the CCA definition of IT cited in section 2.1 is critical in determining the application of DoDI 5000.02 to Air Force IT and other programs, SAF/CIO A6 applies a more focused approach to assist weapon system programs in meeting their CCA compliance and reporting requirements. In looking at weapon systems, we are looking at the way in which IT is incorporated or integrated into warfighting tools to increase mission readiness and enhance organizational effectiveness and efficiency. We are focused on ensuring that the best, most up-to-date, and accurate information is available in a communications network from those who send information to those who receive it. We are looking at how the weapon system (i.e., platform) sends and receives information (e.g., communications systems, data links, messaging, etc.). At some point, that communications capability might connect with

an IP-based network, a GPS satellite, or some other platform although that is not a necessary precondition for CCA review.

2.6. CCA does not distinguish among NSS, weapon systems, DBSs, non-space weapon systems acquisition programs, space acquisition programs, infrastructure, or intelligence systems. No exceptions are made for MAIS Programs, MDAPs, or for tiered systems.

2.7. Legacy programs, i.e., programs that were initiated before the passage of CCA in 1996 or the initiation of the 5000 series, are not exempt from CCA compliance. CCA does not include any provisions to grandfather programs that existed prior to the law's enactment. The Office of Management and Budget (OMB) issued several memoranda contemporaneously with the passage of CCA that applied CCA principles to IT systems that predated passage of CCA. In accordance with OMB Memorandum M-97-02 on "Funding Information Systems Investments" (dated October 25, 1996), agencies that were in the middle of ongoing projects initiated prior to enactment of CCA and were not able immediately to satisfy the eight investment criteria set out in that memorandum, could request future years funding to support the redesign of work processes, the evaluation of investment alternatives, the development of information architectures, and the use and evaluation of prototypes. OMB Memorandum M-97-16 on "Information Technology Architectures" (June 18, 1997) directed legacy systems to focus on their interfaces with new systems, permitting the new and the old to interoperate in a cost-effective manner that does not compromise the ability of the new system to conform completely with the target architecture and standards. If the user interface of an older system does not conform to the architecture, a decision whether to change, replace, or terminate would turn on cost, operational, or functional effectiveness criteria. CCA compliance will not be exercised retroactively; however, modernizations undertaken in those older programs or new acquisitions undertaken within those programs are subject to CCA compliance.

3. CCA Compliance Reporting and Review.

3.1. **Compliance and Reporting.** This section describes the different CCA compliance reporting methodologies for use by Air Force programs. The AF utilizes two different types of CCA compliance reporting methodologies and processes, depending upon the type of program, as presented in Table 3.1 and described in detail in the sections below: (1) a CCA Compliance Report that incorporates the CCA Compliance Table from DoDI 5000.02, Table 8, and a corresponding narrative that describes an ACAT Program's compliance with CCA; and (2) a stand-alone CCA Compliance Table that lists the documents used to demonstrate a program's compliance with CCA.

Table 3.1. CCA Compliance Reporting and Approval.

TYPE OF PROGRAM	REPORTING METHODOLOGY	APPROVING OFFICE
ACAT IAM, ACAT IAC: Major Automated Information Systems (MAIS)	CCA Compliance Report	SAF/CIO A6
ACAT ID, ACAT IC: Major Defense Acquisition Programs (MDAP)		
ACAT II Programs		
ACAT III Programs in WMA, EIEMA, and DIMA		
Joint Programs – AF-owned		
ACAT III Programs in BMA, including traditional Tier 1, Tier 2, Tier 3 programs	CCA Compliance Table	SAF/CIO A6
TIER 4	CCA Compliance Table	Functional Level
TIER 5	Registration in EITDR	N/A
Joint Programs – Non-AF-owned	Discretion of Owner CIO	Owner CIO
Any IT project/program or project/program that acquires IT, selected as an IT Special Interest Program by SAF/A6 CIO, regardless of where that program is in its program lifecycle (including technology projects, service contracts, or supply contracts that have not been designated as ACATs and are considered acquisition programs).	CCA Compliance Report or CCA Compliance Table (depending upon SAF/CIO A6 discretion)	

3.2. **CCA Compliance Review Process for Air Force ACAT I, ACAT II, and Selected ACAT III Programs.** This section addresses the process steps for the preparation, scheduling, submission, review, and approval of the CCA Compliance Report. The CCA Compliance Report is used to ensure that all ACAT I (MAISs and MDAPs), ACAT II, and selected ACAT III programs are in compliance with CCA (see Attachment 3 for the definitions of the acquisition categories). This requirement also applies to any Tier system that is also assigned as an ACAT program. Confirmation of compliance with CCA has been defined by DoD as verifying compliance with the 11 key elements that are identified in DoDI 5000.02 (Enclosure 5). CCA compliance approval in the AF is the responsibility of the SAF/CIO A6.

3.2.1. **CCA Compliance Report.** A template for the CCA Compliance Report is presented in Figure 3.1. The report should be no longer than 20 pages and should be accompanied by a transmittal e-mail or memorandum to SAF/A6PP from the appropriate Command. As the CCA Compliance Report is intended to be a stand-alone document, a

narrative that only refers the reader to a source document without addressing the element is a non-compliant response. DoD has been using the Clinger-Cohen Act Compliance Report or some variation of it as a way of demonstrating program compliance with CCA since the passage of the law. DoD provided guidance on the preparation of CCA Compliance Reports as far back as 1996, usually in memoranda that direct compliance in response to DoD appropriations or authorization laws. The report format and contents have evolved over the years but the basic content has been pretty much the same.

Figure 3.1. CCA Compliance Report Template.

Title Page/Cover Sheet

Program Name
Date of Report
Issuing organization

Signature Page

Contains the required signatures, including the Program Manager, Wing Commander, MAJCOM or Functional CIO (if applicable), and Program Executive Officer (PEO).

1. **Introduction.** This section should begin with the following two paragraphs:

This report contains information required for the Air Force Chief Information Officer (AF CIO) to assess and confirm that (Name of Program) is being developed in accordance with Subtitle III of Title 40 U.S.C. (formerly Division E of the Clinger-Cohen Act (CCA) of 1996). (Name of Program) and its CCA program documentation have been reviewed by the Program Manager and are ready for assessment and confirmation of Title 40/CCA compliance. The results of that review are reported in the following pages. This report also contains information on the funding baseline and milestone schedule for (Name of Program).

(Name of Program) supports the Air Force's and DoD's ability to (provide brief description of the mission benefit(s)).

2. Overview. Provide a three or four-paragraph description of the mission need; key requirements, objectives, goals, and priorities; and a description of program governance. Include the Program's Acquisition category (ACAT) designation, the status of the program (including management and milestone reviews completed), recent MDA approvals, current program activities, and expected date of next Milestone Review or contract award.

3. CCA Compliance Table. Complete Table 8 from DoDI 5000.02, Enclosure 5. Please number (1-11) rather than letter (a-k) the CCA elements.

4. CCA Narrative. Describe program actions on the 11 CCA elements. The narrative for each element only needs to be a few summary paragraphs that address how the program complies with that element; the use of tables, figures, or other exhibit is allowed. The responses to the 11 CCA elements should be numbered 4.1 through 4.11.

Appendices

I. Funding baseline - prior year and current year through next five years, including Operations and Maintenance, Procurement, Research Development Test and Evaluation.

II. Milestone schedule denoting each program milestone, the dates for milestones already attained, and the dates for future milestones.

3.2.2. **CCA Compliance Table.** The second form of reporting is a completed CCA Compliance Table (also referred to as the CCA Compliance Matrix). As noted above, CCA reporting for most ACATs require the CCA Compliance Table and the narrative. The stand-alone CCA Compliance Table is used by Tier programs. As developed by the Business Transformation Agency (BTA), the Modernization Investment Tiers for Information Resources Board (IRB) certification are Tier 1: equivalent to MAIS/MDAP programs; Tier 2: exceeding $10 million, but not designated MAIS or MDAP: Tier 3: exceeding $1 million to $10 million; Tier 4: Investment funding required, up to $1 million; and Tier 5: programs in sustainment or steady state.

A compliance reporting submission to SAF/CIO A6 requires a completed Table 8 (from DoDI 5000.02 and replicated below in Table 3.2 that contains the 11 CCA requirements and a corresponding list of original source documents that are used as proof of CCA compliance. Table 3.2 contains an added column that presents applicable milestones for each CCA element (do not include this column in CCA reporting submission). All milestone reporting requirements must be met. Therefore, if a program reports on its CCA compliance for the first time prior to IOC, it must still report on the elements on which it missed reporting at previous milestones. A comparable table for the Business Capability Lifecycle (BCL) approach to CCA governance is presented in Attachment 8 and a discussion on BCL in section 3.4.1.

Table 3.2. CCA Compliance Table.

CCA COMPLIANCE TABLE **(Table 8 from DoDI 5000.02, amended with Milestone Requirements)**		
Actions Required to Comply with Subtitle III/CCA (Reference (v))	**Applicable Program Documentation** [1]	**Applicable Milestone**
1. Make a determination that the acquisition supports core, primary functions of the Department. [2]	ICD Approval	A
2. Establish outcome-based performance measures linked to strategic goals. [2, 3]	ICD, CDD, CPD, and APB approval	A, B, C
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [2, 3]	Approval of the ICD, Concept of Operations, AoA, CDD, and CPD	A, B
4. Determine that no Private Sector or Government source can better support the function. [4]	Acquisition Strategy, page XX, para XX AoA, page XX	A, B
5. Conduct an analysis of alternatives. [3,4]	AOA	A, B (updated as necessary), C (updated as necessary)

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). [3,4]	Program LCCE Program Economic Analysis for MAIS	For MAIS: A & B, FRPDR (or their equivalent) For non-MAIS: B / contract award
7. Develop clearly established measures and accountability for program progress	Acquisition Strategy, page XX, APB	B
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)	B & C
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards. [3]	Acquisition Information Assurance Strategy	A, B, C, FRPDR
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	B or contract award
11. Register Mission-Critical and Mission-Essential systems with the DoD CIO. [3,5]	DoD IT Portfolio Repository	B, Update as required

[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 and Control Systems that are not themselves IT systems.
[3] These actions are also required to comply with section 811 of Reference (ag).
[4] For NSS, these requirements apply to the extent practicable (section 11103 of Reference (v))
[5] Definitions:
Mission-Critical Information System. A system that meets the definitions of "information system" and "national security system" in the CCA (Reference (v)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (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 (v), that the acquiring Component Head or designee determines is basic and necessary for the accomplishment of the organizational mission. (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."

3.2.2.1. The foundation of CCA compliance is built upon the use of existing documents, most of which were prepared at earlier stages of the program lifecycle development process. The supporting documents that a program lists in the Applicable Program Documentation (APD) column should be supplemented by information about where to find the particular paragraph(s), section(s), figure(s), and/or table(s) in the referenced document. Source documents should be provided to SAF/A6PP.

3.2.2.2. If a program did not utilize a document cited as a proof of compliance in the Applicable Program Documentation column, it may cite other documents, actions, or events as proof of compliance. Examples of additional documents that may be used to confirm CCA compliance are listed in Attachment 4. Documents in draft form are acceptable at the start of the CCA reporting process but they should be finalized by the time the CCA Compliance Report is submitted for final approval.

3.2.2.3. New documentation may also be needed when the (1) information in the original documentation needs to be updated or (2) original document did not

adequately address the CCA requirement. If certification testing for certain CCA elements becomes available in the future, PMs should retain the certification certificates as proof of CCA compliance for such elements

3.2.3. **Report Preparation.** In support of the Milestone Decision Authority (MDA), the Program Sponsor and the Program Manager (PM) shall ensure that the program has met the requirements of CCA. PMs or those responsible for preparing CCA Compliance Reports should become familiar with the statutory, regulatory, and milestone requirements for IT programs and IT-related investments in DoDI 5000.02, Enclosure 4. That enclosure lists the information requirements (statutory and regulatory) for all milestones and phases, for MAIS and MDAP acquisition programs, as well as those for ACAT II and below acquisition programs.

3.2.3.1. MAJCOMs and HQ Functionals are encouraged to work with Program PMOs together to implement an efficient CCA reporting process to meet AF and DoD requirements. The MAJCOMs and HQ Functionals should follow the processes, procedures, and requirements described in this guidance document to assure that there is commonality among procedures and to ensure accurate and timely CCA reporting by their respective programs. Under such an approach, the MAJCOMs and HQ Functionals might be responsible for providing CCA reports and status to SAF/CIO A6. Formal staffing by the PMO, i.e., obtaining command signatures, is not required until a final version of the CCA Compliance Report is approved by SAF/A6PP. The MAJCOM should designate a CCA OPR as the single point of contact for coordination with SAF/A6PP. The MAJCOM CIOs will be a required signatory on all CCA final compliance report submissions to SAF/CIO A6.

3.2.4. **Scheduling.** The PM should take into consideration the time required to obtain CCA confirmation of compliance when developing the project schedule, preparing program documentation, and approaching program milestones to ensure that obtaining CCA confirmation from the AF CIO's office does not negatively impact program schedules. PMs and PMOs are encouraged to contact the CCA POC in SAF/A6P as early in the process as is possible before the next milestone review. In that way, the Program and SAF/A6P can develop an ongoing dialogue, increase and improve the opportunities for early feedback, and facilitate access to SAF/A6P's SMEs for assistance in architecture and other areas. Programs are then encouraged to submit drafts of the CCA Compliance Report and supporting documentation to SAF/A6PP at least four months before the milestone review is scheduled to allow sufficient time for review and revisions. Submissions may be made by e-mail or CD-ROM to the SAF/A6PP CCA POC. A schedule should also be developed for the preparation of documents that directly support CCA compliance, such as the Information Assurance Strategy (IAS) and the Information Support Plan (ISP). Those documents often take much longer to prepare than four months so an appropriate amount of time should be set aside for their preparation. Although the IAS may be submitted for review at the same time as the CCA Compliance Report, the ISP should be submitted earlier as the ISP review process takes longer than the IAS or CCA Compliance Report review process. A program or system should be registered in Enterprise Information Technology Data Repository (EITDR) before the CCA Compliance Report and IAS are submitted to SAF/A6PP.

3.2.5. **SAF/CIO A6 CCA Review Process.** A single point of contact has been established in SAF/A6PP for CCA compliance and to facilitate the CCA review and avoid multiple taskings on the same documents. When a program's draft CCA Compliance Report is ready for review, the program's PM should notify SAF/A6PP POC that a draft CCA Compliance Report will be forthcoming and send the draft report to SAF/A6PP at the CCA Workflow box (SAF/A6P **Clinger-CohenWorkflow@pentagon.af.mil**).

3.2.5.1. After the program's draft CCA Compliance Report and supporting documentation are received by SAF/A6PP, they will be reviewed by the Subject Matter Experts (SMEs) in architecture, finance, information assurance, and other areas. SAF/A6PP will consolidate the SMEs comments and send them to the PM if there are issues that require resolution. SAF/A6PP employs a rigorous, consistent, and repeatable review protocol that is conducted as quickly and comprehensively as possible. This process usually takes about two to three weeks for the review of a first draft CCA Compliance Report.

3.2.5.2. SAF/A6PP will separately notify the program's CCA POC when the IAS is approved. SAF/A6PP will provide the PM with a memorandum indicating SAF/CIO A6's approval of the IAS. For MAIS and MDAP programs, the PM should send that approval memorandum and the approved IAS to DoD-CIO/NII in order to receive that office's approval of the IAS.

3.2.5.3. The desired outcome of the SAF/A6PP CCA review and approval process is a recommendation to the AF CIO that the program under review should be confirmed as CCA compliant. Therefore, SAF/A6PP will conduct as many reviews of the draft CCA Compliance Report as necessary until the document is ready for submission to the AF CIO. When SAF/A6PP has determined that the program is CCA compliant, it will request that the PMO formally resubmit the completed CCA Compliance Report to SAF/A6PP accompanied by a signature page that contains the required signatures (please see Figure 3.1, CCA Compliance Report Template).

3.2.6. **Notice of AF CIO Approval.** SAF/A6PP will send the completed CCA Compliance Report, incorporating the signature page, to the AF CIO. If approved, the AF CIO will sign a memorandum confirming that the program is being developed in accordance with Subtitle III of Title 40/CCA and DoDI 5000.02. The signed approval memorandum will be sent to the Program's PM or POC, regardless of ACAT, for submission to the MDA for milestone decisions or contract awards. As noted previously, DoD-CIO approval is not required.

3.3. **CCA Compliance Review Process for Air Force ACAT III Programs.** CCA applies to all programs and systems in the three Mission Area Portfolios: Business Mission Area (BMA), Warfighting Mission Area (WMA), and Enterprise Information Environment Mission Area (EIEMA). As AF business systems in the BMA domain have undergone most of the non-ACAT CCA reviews among the three domains during the past two years, the discussion below utilizes those BMA programs for the purpose of clarity. WMA and EIEMA programs will undergo similar reviews in the near future.

3.3.1. When DBSs (including those that are legacy systems; are in sustainment; or are characterized as mixed life-cycle by OMB, regardless of their initiation date) spend new

monies on development, modernization, and enhancement (DME), the modernization activity is required to be CCA compliant. According to DoD Financial Management Regulation, Chapter 18, DME refers to any change or modification to an existing Information System (IS), program, and/or initiative that results in improved capability or performance of the baseline activity. Development/Modernization includes: (1) program costs for new applications and infrastructure capabilities that are planned or under development; (2) any change or modification to existing applications and infrastructure capabilities which is intended to result in improved capability or performance of the activity (these changes include (a) all modifications to existing operational software (other than corrective software maintenance); and (b) expansion of existing capabilities to new users); (3) changes mandated by Congress or the Office of the Secretary of Defense; and (4) personnel costs for Project Management." For the purposes of CCA compliance, we focus on the use of any funds that are used for DME.

3.3.2. Program Managers developing a new DBS should recognize that its program may be an ACAT program that needs to comply with the DBS certification review process contained within Enclosure 11; CCA compliance reporting as defined in Enclosure 5, DoDI 5000.02; other sections of DoDI 5000.02; and this guidance. It is expected that this will improve program development and management applications under the 5000 series.

3.3.3. ACAT III business systems will report their CCA compliance to SAF/A6PP in conjunction with their certification/recertification reporting under the DBS certification review process. To demonstrate CCA compliance, business systems will report on their use of selected documents in the CCA Compliance Table (DoDI 5000.02, Enclosure 5, Table 8). These systems may use any of the documents cited in the Applicable Program Documentation column of the CCA Compliance Table as proof of compliance; if they did not use the documents listed in that column, they should cite the documents that were used to support the CCA element. Original reports, memoranda, spreadsheets, and architectural drawings may be used but the citation should be an original document, not a secondary source. For example, an answer to a question in EITDR is not an acceptable response. The supporting documents that a program lists in the Applicable Program Documentation column should be provided to SAF/A6PP. The CCA compliance table submitted by the business systems will be approved by SAF/A6PP.

3.3.4. Although systems will not generally be asked to prepare new analyses, new drawings, or new documents, there may be some exceptions to that rule. In some of the areas where new documentation may be required, A6P has tried to develop requirements and templates that are more flexible than those imposed on ACAT I and II programs. For development of an Information Assurance Strategy (IAS) for programs that are modernizing, A6P provides a new IAS template that relies heavily on DoD Information Assurance Certification and Accreditation Process (DIACAP) information. Systems will probably need to prepare an economic analysis similar to that discussed in section 4.7. SAF/FMC is developing a scaled down approach for systems under $1million; regardless, the National Defense Authorization Act (NDAA) Economic Viability Tool (EVT) does not meet the EA requirement as it only contains a small subset of the information that is required in an EA (the EVT compares the net present value of the selected alternative against status quo and provides associated financial metrics but does not address the non-monetary impacts or provide the documentation that would be required for an economic

analysis). For programs that do not need to prepare an ISP but need to demonstrate alignment to the Global Information Grid (GIG) and the use of proper architecture where existing architectural drawings are not compliant with policy, section 4.9.2. provides an alternate compliance approach.

3.3.5. Tier 4 business systems are reviewed by appropriate authorities at the Functional levels for CCA and other governance requirements under the tiered accountability model utilized by the Air Force. In light of tiered accountability and to ensure consistency with CCA compliance for Tier 1, 2, and 3 business systems, the Functional Levels will have a new responsibility for assessing CCA compliance for Tier 4 business systems using the CCA Compliance Table in DoDI 5000.02, Enclosure 5. Functional Levels will report annually (at the end of each calendar year) to SAF/CIO A6 on the Tier 4 business systems that they reviewed and approved or disapproved as CCA compliant.

3.3.6. A system or program in sustainment is one that spends O&M funds for continuing operations and current services, or sustainment-only activities. This type of system is not allocating or spending any funds on DME or for new capabilities, i.e., an activity that results in improved capability or performance of the baseline activity. OMB refers to these systems or programs as steady-state. The only reporting requirement for business systems in sustainment (usually Tier 5 systems) is that they be registered in EITDR.

3.4. **Streamlining Approaches.** Although some CCA supporting documents can be subsumed into alternate acquisition documentation, the CCA Compliance Report, the IAS, and the ISP (or alternate documentation such as the section 4.9.2. report) must be provided to SAF/A6 CIO as stand-alone documents prepared in accordance with this guidance document and other specialized guidance documents. SAF/CIO A6 will accept nontraditional documentation under the following circumstances (a) the program is undergoing an officially sanctioned streamlining approach; (b) the program has defined criteria or requirements for what will be included specifically in the streamlined document; and (c) SAF/CIO A6's compliance criteria for a particular compliance element (where such criteria exists) must be met.

3.4.1. Business Capability Lifecycle (BCL). On June 23, 2011, DoD-ATL issued "Directive-Type Memorandum 11-009, Acquisition Policy for Defense Business Systems (DBS)." Those guidelines formally established the BCL model as the acquisition process for defense business systems. The BCL guidance provides the framework for structuring the definition, development, testing, production, deployment, and support of DBS. In most cases for DBSs, the BCL acquisition business model and guidance take precedence over applicable sections of DoDI 5000.02. DBS PMs are encouraged to read the BCL guidance, as it also addresses roles and responsibilities and issues related to document submission and oversight process. The BCL requirements in Table 4 (Attachment 8) are almost identical to those in Table 8 in DoDI 5000.02, Enclosure 5. Please pay particular attention to Attachments 3 and 4 in the BCL guidance memorandum. Attachment 3 describes the statutory and regulatory requirements for DBSs. Attachment 8 addresses the IT considerations associated with DBSs.

4. CCA Compliance Elements.

4.1. **Describing the CCA Compliance Elements.** This section provides guidance on how to address the 11 CCA compliance elements in the CCA Compliance Table (DoDI 5000.02, Enclosure 5, Table 8). Presented after the statement of each element are issues to be

considered in complying with each element and likely sources of information and documentation for CCA compliance reporting. The same review standards are applied whether SAF/CIO A6 is reviewing a CCA Compliance Report or, for example, documents submitted in support of an AFRB and ASP.

4.1.1. Three of the CCA elements in Table 8 are referenced with a footnote that states, "These requirements are presumed to be satisfied for Weapons Systems with embedded IT and for Command and Control Systems that are not themselves IT systems." Those words have been misinterpreted by some as meaning that the program under consideration could omit evidence of compliance. The footnote refers to an assumption that the CCA element for the subject system was addressed in an approved Joint Capabilities Integration and Development System (JCIDS) or acquisition document. Experience has shown that it is often the case that, especially with respect to outcome-based performance measures, the JCIDS or acquisition document was approved without addressing the CCA element. In those cases, the program may have to address that CCA element in order to be CCA compliant.

4.1.2. There are several guidance documents and tools that will be of assistance in writing the compliance discussion for the 11 CCA elements:

4.1.2.1. *Defense Acquisition Guidebook* (**http://akss.dau.mil/DAG/welcome.asp**) is helpful in addressing all 11 CCA elements and in providing specific information on CCA (**https://akss.dau.mil/dag/DoD5000.asp?view=document&rf=GuideBook\IG_c7.8.asp**).

4.1.2.2. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01C, *Operation of the Joint Capabilities Integration and Development System.*

4.1.2.3. CJCSI 3170.01G, *Joint Capabilities Integration and Development System* (CCA elements 1, 2, 3, 4, and 5).

4.1.2.4. CJCSI 6212.01E *Interoperability and Supportability of IT and National Security Systems*.

4.1.2.5. Air Force Instruction (AFI) 10-601, *Capabilities-Based Requirements Development* (CCA elements 1, 2, 3, 4, 5, 6, and 7).

4.1.2.6. AFI 63-101, *Operation of Capabilities Based Acquisition System* (CCA elements 2, 3, 4, 5, 6, 7, and 10).

4.1.2.7. Clinger-Cohen Act Compliance/Certification Community of Practice (CoP) site (**https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-AQ-AF-01**) (contains authoritative sources and templates to aid in preparing a CCA Compliance Report).

4.2. **CCA Compliance Element 1. Make a determination that the acquisition supports core, priority functions of the Department.**

4.2.1. Summarize the results of the core mission analysis of the acquisition program. The summary will validate and document the rationale supporting the relationship between the AF's mission (i.e., core/priority functions) as documented in AF mission and strategy documents, and the function supported by the acquisition. Is the function that the proposed IT acquisition will support something the Federal government actually

needs to perform; i.e., for the Department of Defense, is the function one that the Department of Defense and/or its Components must perform to accomplish the military missions or business processes of the Department?

4.2.2. For the WMA and Enterprise Information Environment functions, this question is usually answered in the JCIDS process. At this time, the Program Sponsor should conduct a series of analyses (i.e., the Functional Area Analysis, Functional Needs Analysis, and Functional Solution Analysis). These analyses are normally completed before preparing an Initial Capabilities Document (ICD). The JCIDS analyses should demonstrate that the acquisition supports core/priority functions that should be performed by the Federal Government. Examples of a valid mission need include a combat or weapon system or an integral part of a weapons system, Joint operations in support of the warfighter, or designation as an NSS. The analysis should also establish linkages among the mission, the function supported, the capability gap, and potential solutions.

4.2.3. The supporting documentation for this element is generally found in an approved ICD. DoD core/primary functions are documented in national strategies and DoD mission and strategy documents like the Quadrennial Defense Review, Strategic Planning Guidance, Joint Operating Concepts, Joint Functional Concepts, Integrated Architectures, the Business Enterprise Architecture, the Universal Joint Task List, mission area statements, or Service mission statements. Other potential sources include the Mission Need Statement (MNS), Operational Requirements Document (ORD) or Capability Development Document (CDD), and Analysis of Alternatives (AoA).

4.3. **CCA Compliance Element 2. Establish outcome-based performance measures linked to strategic goals.**

4.3.1. Outcome-based performance measures (OBPMs) assess the actual results, effects, contributions, accomplishments, or impacts of a program compared to its intended purpose. According to CJCSI 3170.01C, OBPMs are "measures designed to correspond to accomplishment of mission objectives and achievement of desired effects." In other words, OBPMs represent the mission outcomes that would fill the functional gap identified as the need for the program and would be used in justifying the program. They measure the ability of the delivered system to achieve a need, requirement, or capability previously identified by the user.

4.3.2. OBPMs for capabilities needed by the WMA and EIEMA programs and would be developed during a Capabilities-based Assessment (CBA) and recorded in a validated ICD. In older programs, the OBPMs related to the achievement of a needed capability (rather than actual system performance) might be found in a MNS or an equivalent 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.

4.3.3. The effective measurement of an IT investment’s contribution to agency accomplishments begins during the investment’s planning stage. There should be a statement in the program documentation about the desired outcome and how the program would develop and deploy the solution to achieve that outcome (an outcome is the resulting effect of an IT investment on an organization). The OBPMs should measure the value-added contribution of the IT investment to missions, goals, and objectives and

provide a clear basis for assessing accomplishment and aiding decision-making. They are a measure of operational success that must be closely related to the objective of the mission or operation being evaluated.

4.3.4. OBPMs for IT investments and processes should:

4.3.4.1. Measure the capabilities that the system provides, not system performance.

4.3.4.2. Be outcome-oriented and measurable (i.e., quantifiable), demonstrating the results (or lack thereof) for a particular system based on an established baseline.

4.3.4.3. Be linked to the mission of the IT investment that they support.

4.3.4.4. Be limited to a vital few, i.e., to only those absolutely necessary to provide the required data (If there are too many measures, organizations may become too intent on measurement and lose focus on improving results. A guiding principle may be to measure that which matters most.).

4.3.4.5. Be determined prior to the selection of a particular alternative approach or contractor, be independent of any solution, and not specify system performance or criteria (i.e., the OBPM should be established before the Concept Decision that starts the acquisition process or at the pre-Milestone A stage and validated at Milestone A). If that has not occurred in an existing program, the OBPMs should be developed before Milestone B.

4.3.4.6. Be measured by collecting performance data and comparing actual to projected performance from carrying out a program or activity, thereby determining an investment's efficiency and effectiveness in meeting cost, benefit, schedule, risk, mission, documentation, and performance objectives.

4.3.4.7. Be supported by data that can be accurately and reliably collected.

4.3.4.8. Be inclusive of both AF and enterprise performance benefits.

4.3.5. Several examples of OBPMs might be helpful.

4.3.5.1. Measuring the number of enemy submarines sunk or enemy tanks destroyed may be satisfactory OBPMs if the objective is to destroy such weapons systems.

4.3.5.2. Measuring the reduction in operating or manpower costs or the replacement of multiple legacy systems with a new single system, or facilitating command decision-making.

4.3.5.3. An outcome measure for a tornado warning system would be the number of lives saved and property damage averted.

4.3.5.4. An outcome measure for a learning management system could be the increased competency of employees and increased mission readiness of an organization from its use.

4.3.6. It is easy to confuse OBPMs with output measures. Outputs are defined as “the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity.” The differences between OBPMs and output measures can be demonstrated using some of the earlier examples. In the case of tornado warning system, an output measure could be the

measure of time between the warning and the tornado strike with a goal of increasing the warning time and reducing the number of false alarms. In the case of the learning management system, output measures could be the number of courses delivered on relevant topics, the number of those who pass the courses, or the number of instructors hired.

4.3.7. When formulating OBPMs, it is important to differentiate between OBPMs, Key Performance Parameters (KPPs), and acquisition performance measures. KPPs are those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability and those attributes that make a significant contribution to the key characteristics as defined in the Joint Operations Concept. KPPs of the ORD/CDD/Capability Production Document (CPD) or the measures of performance found in a system Test and Evaluation Master Plan (TEMP) are generally not OBPMs. These are derivatives of the mission/capability. Similarly, OBPMs are not acquisition performance measures that are found in the acquisition program baseline (APB) containing cost, schedule, and system-level performance goals and thresholds; Development Test and Evaluation Measures (measure conformance to contract); Operational Test and Evaluation (OT&E) Measures Title 10 USC Section 2399 (or simulated employment, by typical users, of a system under realistic operational conditions); or Follow-on OT&E (verification of correction of deficiencies discovered earlier, tactics development, OT&E of block upgrades to the system, completion of OT&E of system support materiel (pubs, equipment, etc.), OT&E against emerging threat, and completion of deferred OT&E (other climates, unique modes of operation, etc.)). Those measures may be use to satisfy CCA Element #7.

4.3.8. The OBPMs serve as the basis for developing the program's Post-Implementation Report (see section 5.0).

4.3.9. The best document to use to answer element #2 is an approved ICD. Other potential sources include the CDD; CPD; APB; Performance Measurement Plan; MNS; ORD; TEMP; Organizational Strategic Plan; Mission Area Performance Plan; *Guide for Developing and Using IT Performance Measurements*, Department of the Navy, Chief Information Officer (October 2001); and *Capabilities-Based Assessment Users Guide, Version 2*, Force Structure, Resources, and Assessments Directorate, JCS J8, December 2006.

4.4. **CCA Compliance Element 3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology.**

4.4.1. As information systems and networks have become more sophisticated and widespread, it has become imperative to ensure that those systems are maximized for cost reduction and performance improvement. Has the business process or mission function supported by the proposed acquisition has been designed (or redesigned) for optimum effectiveness and efficiency? The Program should revise its mission-related processes and administrative processes as appropriate before making significant investments in IT.

4.4.2. Describe the actions taken to streamline, reengineer, or redesign existing processes to reduce costs, improve effectiveness, and maximize the use of Commercial Off-The-Shelf (COTS) technology that better support the organization's mission. If the acquisition program supports a newly developed process, describe the development of the

process (i.e., describe the current process, the need for change, and the benefits associated with that change). Among the items that should be considered are whether (a) the business process or mission function supported by the proposed acquisition has been designed for optimum effectiveness and efficiency; (b) if the work is done in a way that improves performance in meeting the program's mission while reducing costs; and (c) the process be accomplished more efficiently by another federal organization, e.g., another Major Command (MAJCOM) or even another organization within the same MAJCOM? (this is similar to the question asked in CCA element #4).

4.4.3. Describe the extent to which COTS/Government Off-the-Shelf (GOTS) hardware and software will be used to satisfy the system requirements. Programs should maximize the use of COTS/GOTS technologies or tailored versions of GOTS/COTS technologies in an effort to reduce cost, risk, and development time. In addition, in the absence of a total COTS solution, the program should endeavor to utilize COTS technology as part of an overall solution and approach to reducing costs, etc., while maintaining vision on any operational risks or second-order effects of using a product from a commercial vendor.

4.4.4. The best document to use to answer element #3 is an approved ICD. Other major sources include the General Accountability Office (GAO) *Business Process Reengineering Assessment Guide* (GAO/AIMD-10.1.15, April 1997); and the following documents: Concept of Operations, AoA (FSA), CDD, CPD Acquisition Plan (AP), Business Case Analysis (BCA), MNS, and ORD.

4.5. **CCA Compliance Element 4. Determine that no Private Sector or Government source can better support the function.**

4.5.1. Must the acquisition be undertaken by the AF because it requires unique capabilities that are not found in the private sector or elsewhere in the public sector in a way that can support the function more effectively or at less cost? Identify sourcing determination and rationale; consider commercial, small business, and other Government agencies as potential sources.

4.5.2. Depending on the project's current milestone review, some questions to be considered are:

4.5.2.1. Does the proposed investment in IT support core mission or inherently governmental functions that need to be or must be performed by the Government?

4.5.2.2. Can the functions be accomplished more efficiently (reduced cost and/or improved effectiveness) by another federal organization?

4.5.2.3. Does the proposed IT investment fall under OMB Circular A-76, *Performance of Commercial Activities*? (Outsourcing policy)

4.5.3. Include in the narrative for this section a statement that clarifies whether there are other Federal Government, DoD, or AF entities performing the proposed function, or if the proposed function duplicates or overlaps with an existing function.

4.5.4. The best document to use to answer element #4 is an approved Acquisition Strategy (AS), supported by an approved AoA. Another potential source is the Market Survey (if one has been performed).

4.6. **CCA Compliance Element 5. Conduct an analysis of alternatives.**

4.6.1. Summarize the discussion in the AoA that was conducted for the program. The AoA discussion should address the following:

4.6.1.1. Whether the program prepared a thorough AoA and considered enough reasonable alternatives (at least two viable alternatives in addition to the current baseline [i.e., status quo])?

4.6.1.2. The alternatives examined (including the pros and cons of each alternative). Discuss the methodology and criteria used to evaluate alternatives, and the risk-adjusted lifecycle cost/benefits estimates.

4.6.1.3. Why the selected alternative was chosen and why the remaining alternatives were not chosen.

4.6.2. A frequent question is whether an AoA should be updated prior to the program going through the milestone process. The answer depends upon whether the AoA was general enough to cover changes to the program occurring after the AoA was issued. An update is not required if the AoA was general enough; however, the PM should consider revising the AoA if it specified, for example, the use of software ABC V.1.0 and the contemplated contract and/or Milestone decision brief intends to procure software XYZ V.5.0.

4.6.3. The best document to use to answer element #5 is an approved AoA. Use OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, to determine the criteria to be used in the AoA and benefit/cost analysis. Another useful document is OMB's *Capital Planning Guide*, especially Part 7, Section 300, *Planning, budgeting, acquisition, and management of capital assets*, and the Part 7 Supplement. Other potential sources include the Business Case Analysis, Trade Survey, and Cost and Operational Effectiveness Analysis (COEA).

4.7. **CCA Compliance Element 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).**

4.7.1. An Economic Analysis (EA) consists of a life-cycle cost and a benefits analysis and is a systematic approach to selecting the most efficient and cost effective strategy for satisfying a program's need. The EA also supports the AoA by examining the monetary (costs, financial metrics) and non-monetary (benefits, risks) impacts of selecting an alternative. When supporting the AoA, the EA is a stand-alone document that describes the background behind the decision at hand, the expected requirements and performance for each alternative, and the rationale behind the analysis. An EA is required whenever a functional user or program office is procuring, modernizing, or upgrading a material solution.

4.7.2. For AIS programs, briefly describe the economic analysis to include a calculation of the Return on Investment (ROI). Provide the current projected ROI for the preferred alternative. Does the ROI support the investment in the preferred alternative? Identify the elements that were considered in the ROI including mission improvements, resource

savings, and qualitative mission benefits. If possible, for an incremental or evolutionary acquisition, provide an overall ROI for each increment.

4.7.3. For non-AIS programs, briefly describe the program LCCE. The LCCE provides a structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a particular program. This entails identifying all cost elements that pertain to the program from initial concept all the way through operations, support, and disposal. The LCCE encompasses all past (or sunk), present, and future costs for every aspect of the program, regardless of funding source. The LCCE should represent a realistic appraisal of the level of cost most likely to be realized. The numbers, explanation, and justification associated with the Cost Analysis Requirements Descriptions (CARD) and other economic analyses should be sufficiently detailed and the calculations should be replicable based upon the information provided.

4.7.4. The best documents to use to answer element #6 are an approved Economic Analysis with Return on Investment (EA w/ ROI) and the Program LCCE. Depending on the capability, an approved LCCE may be substituted. Please see DoDD 5000.4, Cost Analysis Improvement Group. The FM Center of Expertise also has a lot of good information on its website (**www.saffm.hq.af.mil/coe**).

4.8. **CCA Compliance Element 7. Develop clearly established measures and accountability for program progress.**

4.8.1. Describe the process reporting, tools, and metrics for measuring program progress and post-deployment evaluation to include cost, schedule, and technical performance. Are there clearly established measures and accountability for program progress? Are these measures linked to strategic goals? Describe how the performance measures are being applied for evaluation of mission accomplishment. Demonstrate how program control and MDA-level directions are being achieved.

4.8.2. At milestone reviews, comparisons are made between the expected costs, risks, and benefits of earlier phases with the actual costs incurred, risks encountered, and benefits realized to date. Cost and schedule measures should be used as performance measures of program progress.

4.8.2.1. Cost figures should reflect realistic cost estimates of the total program and/or increment. Budgeted amounts should never exceed the total cost thresholds (i.e., maximum costs) in the APB.

4.8.2.2. Schedule parameters should include, as a minimum, the projected dates for program initiation, other major decision points, and IOC.

4.8.2.3. KPPs that measure program performance should be identified and linked to strategic DoD and AF goals, periodic program management reviews, and quarterly metrics reviews.

4.8.3. Describe how the established roles and responsibilities for the organizations involved in the program ensure accountability for program progress. In that context, describe how the PMO manages to achieve its cost objectives and how contractors manage to achieve cost objectives.

4.8.4. The best document to use to answer element #7 is an approved AS. Other potential sources are an approved APB and an Earned Value Management System (EVMS).

4.9. **CCA Compliance Element 8. Ensure that the acquisition is consistent with the Global Information Grid policies and architecture, to include relevant standards.**

4.9.1. Information Support Plan (ISPs) will be presented at appropriate Milestone decision reviews as part of the approval to proceed. The ISP is defined in DoDI 4630.8 and CJCSI 6212.01F, both of which require that an ISP be developed for all IT and NSS regardless of ACAT level to ensure net-centricity and compliance with the GIG. The ISP must also be developed for legacy systems undergoing a major modification. Additional guidance on ISP preparation and requirements at each milestone and review protocols may be found at the Information Support Plan CoP. The ISP provides graphic views that show the major elements/subsystems that make up the system being acquired, and how they fit together. The ISP describes the system's function, dependencies and interfaces with other IT and NSS systems.

4.9.2. The PM should address the timing of ISP preparation early in the program development process. For a small program with few interfaces, it takes approximately six months to prepare an ISP for a Stage I (or initial) review. For most programs, ISP preparation for Stage 1 review can take up to one year. For very complex programs, such as a major fighter aircraft, it can take significantly longer to prepare the ISP.

4.9.3. DoD has adopted a new Enhanced Information Support Plan (EISP) process focuses on ISP data as opposed to the ISP document. The ISP developer will no longer have to write a document that may or may not be consistent with the Defense Acquisition Guidebook (DAG). Instead, they will be asked to enter data into an EISP template that focuses on the core informational aspects of the program. The data will be entered into the EISP template via the Enhanced ISP Tool. Detailed information on the EISP Tool can be found on the ISP CoP. Under this new process, the responsibility of the Program Manager / Submitter is to create a program profile, build and/or modify an ISP using EISP Enterprise Service Version (ESV), declare GIG Technical Profiles (GTPs), create all required architectural views, and submit it as a data package for assessment/Interoperability and Supportability (I&S) certification.

4.9.4. Existing ACAT I and II programs and new programs of any ACAT that do not have an ISP waiver must transmit information about the program’s compliance with GIG policies, interoperability and architecture through the ISP. The ISP should be summarized in this section of the CCA Compliance Report. Those programs must be compliant with GIG and AF policies on net-centricity when acquiring IT-enabled capabilities that must interoperate with other systems for mission success. Compliance with the GIG means that an IT-based initiative or an acquisition program throughout its lifecycle should:

4.9.4.1. Meet the DoD Architecture Framework (DoDAF) requirements in producing integrated architectural products;

4.9.4.2. Meet the GIG Technical Guidance (GTG) or DoD Information Technology Standards Registry (DISR) requirements in selecting technologies and standards;

4.9.4.3. Meet the DoD Net-Centric Data Strategy requirements and intent;

4.9.4.4. Explicitly address net-centricity and determine the program's net-centric correspondence to key net-centric criteria (e.g., concepts, processes, services, technologies, standards, and taxonomy from the DoD Information Enterprise Architecture [DoD IEA] in a description of which principles and rules from the DOD IEA were used in the design of the systems concept of operations for external interfaces.

4.9.4.5. Describe the concept of operations that the system will use to exchange information using the DoD IEA's activities and concepts. This is driven by the CCA requirement to demonstrate that the IT elements of a system are aligned to the agency's IT architecture (the DoD IEA is the surrogate for the GIG) and that business process reengineering (BPR) has been done to promote improvements in communications processes. Net-centric operations and warfare are the way the AF is facilitating BPR and the use of the DoD IEA principles and terminology demonstrates that concept. These practices must be demonstrated in a way that is defensible to OMB. At an OV level this concept of operations typically identifies the four ways to exchange information – person to person, point to point, linked, and networked or combination. If an internet protocol network like the Internet is used, then the architecture needs to address data repositories, services, etc. (i.e., the principles of the DoD IEA). This is typically in the Operational View-5 (OV-5) from architecture developed with DoDAF 1.5 or earlier and the OV-5b in DoDAF 2.0)(the system may use it own terminology for the concept of operations as long as they provide the mapping to the DOD IEA); and

4.9.4.6. Use the Joint Common Systems Functional List (JCSFL) to describe the system's high level functions so that they can be traceable to the Joint Capabilities Areas (JCAs), a requirement of JCIDS and link to missions for CCA.

4.9.5. Existing ACAT III programs that have an existing interface or plan to have an interface but do not have an ISP or were granted an ISP waiver, and new programs that were granted an ISP waiver, must demonstrate their compliance with GIG policies and architecture by answering the 11 questions listed in Table 4.1 below and by providing all of the architectural views listed on the table. The answers to those questions need to define how well (a) others have to be able to get information to the system; (b) the system has been able to get the data to those that need it; and (c) how well the transport mechanisms for these exchanges need to perform. This should reflect joint operations in a net-centric environment. A complete listing of the architectural views required by JCIDS and the ISP can be found in the current CJCSI 6212.01.

Table 4. 1 Architectural questions to be answered in the ISP

Questions to be Addressed	Architecture Standard Employed	
	Under DODAF 1.0 and 1.5	Under DODAF 2.0
1. What does the system need to do?	OV-5	OV-5b
2. Who has the information needed by the system and to whom does the system need to give information?	OV-2 and OV-4	OV-2 and OV-4
3. How well do those exchanges need to be performed?	OV-3	OV-3
4. When does the system need to have those communications?	OV-6c	OV-6c
5. Can the system understand those communications?	OV-7	DIV-2
6. What systems have the information in them?	SV-1	SV-1
7. How is the system going to move the information?	SV-2	SV-2
8. What system characteristics are needed to support the communications and what does the system need to do?	SV-4b and SV-5	SV/SvcV-4 and SV/SvcV-5
9. What are the testable characteristics of those communications between systems at an Operational Test (OT) level?	SV-6	SV-6
10. What are the data formats of the systems with which the system needs to exchange information?	SV-11	DIV-3
11. What specs and standards is the system using to assure the systems can interoperate?	TV-1 and TV-2	StdV-1 and StdV-2

4.9.6. The data is independent of the framework in which it is presented. If a program does not have architecture or Net-Ready–Key Performance Parameters (NR-KPPs), the same questions in Table 4.1 need to be answered in order for SAF/CIO A6 to determine CCA and interoperability compliance. SAF/CIO A6P will utilize the checklist in Attachment 5 to assess the architecture for CCA compliance.

4.10. **CCA Compliance Element 9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.**

4.10.1. An IAS is required to address how IA will be implemented in an IT program. The IAS is appended to the Program Protection Plan (Document Streamlining - Program Protection Plan (PPP), July 18, 2011, Memorandum from Frank Kendall) after its approval by the Component CIO and DoD CIO. PMs should be aware that some sections previously contained in an IAS (e.g., IA threats, MAC level) were moved to the body of the PPP for document streamlining. The template for an IAS for programs other than ACAT III and Tier DBSs undergoing modernization, enhancement, or development is presented in Attachment 6. That IAS template also describes the information that is required on a milestone-by-milestone basis. A modified IAS template for ACAT III and

Tier DBSs undergoing modernization, enhancement, or development is presented in Attachment 7.

4.10.2. An IAS is not required for Material Development Decisions (MDD). An IAS developed in preparation for Milestone A will be more general and contain a lesser level of detail than an IAS submitted to support subsequent Milestone decisions. In consideration of the different levels of maturity relative to acquisition phases, and to encourage brevity and focus, the following page limitations are imposed for IA Strategies: Milestone A – 7 pages; Milestone B or C – 15 pages, Full Rate Production (FRP) or Full Deployment Decision (FDD) – 15 pages. Tables of contents, acronym lists, signature sheets and executive summaries are not required, but if included do not count against the page limitations.

4.10.3. The PM in accordance with DoDI 8510.01 must assemble a Certification and Accreditation Team consisting of a Designated Accrediting Authority (DAA), Certifying Authority (CA), CA Representative, CA Agent, IA Manager (IAM), and User Representative. Roles and responsibilities are outlined in AFI 33-210, Air Force Certification and Accreditation Program. All systems except Space and Special-Access Program/Special Access Required (SAP/SAR) systems are certified by the Air Force Senior Information Assurance Officer. Space systems are certified and accredited by the AFSPC DAA and SAP/SAR systems are certified and accredited by SAF/AAZ.

4.10.4. PMs should pay attention to IA issues in the early stage of a program. Examine program and system characteristics to determine whether compliance with DoDD 8500.1 is recommended or required and whether an IAS is required. Programs that do not involve the use of IT in any form have no IA requirements. However, PMs should examine programs carefully because many programs have IT embedded in the product or its supporting equipment, such as automatic test equipment. Programs that include IT always have IA requirements, but these IA requirements may be satisfied through the normal system design and test regimen but are required to comply with DoDD 8500.01E if they are categorized as Automated Information System Application, Platform IT Interconnection, Enclave, Outsourced Based IT, or stand-alone system.

4.10.5. Acquisitions that include Platform IT with no communications interconnection are not required to comply with DoDD 8500.1; however, such programs require an IAS if they are designated Mission Critical or Mission Essential. Acquisitions of platforms with network interconnections must comply with the IA requirements of DoDD 8500.1 and DoDI 8500.2. Programs that include IT and are designated Mission Critical or Mission Essential require an IAS without regard to the applicability of DoDD 8500.1. Whether an investment is categorized as a system or as Platform IT, both require an IA strategy. In accordance with DoDI 8500.2, the IAS for Platform IT with interconnection to an external system or network must specifically address IA protection for the interconnection points. Program Managers responsible for Platform IT with no interconnection to an external system or network should implement the IA guidance in DoDD 8500.1 and DoDI 8500.2.

4.10.6. In the case of Family of Systems Acquisition Programs, the IASs for these programs may be written at a capstone level, focusing on the integration of IA

requirements and controls, coordination of System Security boundaries, and ensuring IA resourcing for own and subordinate systems.

4.10.7. The IA section of the CCA Compliance Report itself should describe how the program's IA features comply with applicable DoD and AF policies, standards, and architectures, describe the program's certification and accreditation approach, and include the dates that the IAS was approved by the AF CIO and the DoD CIO. Describe the security features, practices, procedures, and architecture of the system that mediate and enforce the DoD Information Assurance Certification and Accreditation Process (DIACAP). IA requirements should be addressed throughout the program life cycle and incorporated into program design activities.

4.10.8. The requirements for an IAS (including NSS), appear in:

1. DoDD 8500.1, *Information Assurance (IA).*

2. DoDI 8500.2, *Information Assurance (IA) Implementation.*

3. DoDI 8580.1, *Information Assurance in the Defense Acquisition System.*

4. DoDD 8100.01, *Global Information Grid (GIG).*

5. Chairman of the Joint Chiefs of Staff (CJCSM) 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND).*

6. *DoD Acquisition Guidebook* (The IA section of the Defense Acquisition Guidebook includes an "IA Compliance Decision Tree" and an "IA Compliance by Acquisition Program Type" table to help determine if an IAS is required.).

7. Federal Information Security Management Act *(*FISMA) Public Law (PL) 107-347.

8. Information Assurance Technical Forum (IATF).

9. AFPD 33-2, *Information Assurance.*

10. AFI 33-200, *Information Assurance (IA) Management.*

4.10.9. All AF IASs must be approved by SAF/CIO A6. Upon approving the IAS, SAF/CIO A6 will take two actions: it will send to the program POC a memorandum indicating that the program's IAS is approved by SAF/CIO A6 and direct the program's POC to forward the memorandum and approved IAS to NII/DoD-CIO for its review and approval. NII/DoD-CIO approves IASs for all MAISs and MDAPs. The IASs for space programs must be approved by the AFSPC CIO prior to submission to SAF/CIO A6.

4.10.10. The best document to use to answer element #9 is an approved IAS. Other potential sources include DIACAP guidance; CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*; System Security Authorization Agreement (SSAA), Program Protection Plan, System Security Policy document, and System Security Plan.

4.11. **CCA Compliance Element 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.**

4.11.1. Describe the extent to which modular contracting principles are adhered. Under modular contracting, a system is acquired in successive acquisitions of interoperable increments that allow for the following: easier to manage, address complex IT objectives, not dependent of subsequent increments, take advantage of technology advancements and reduces risk through avoidance of custom-designed components. Describe the relationship between each increment and the mission need and benefit associated with that increment. CCA 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 or systems.

4.11.2. Program schedule and milestones reflect phased successive implementation approaches. Each increment results in stand-alone functional capability; development in iterations or spiral development methodology, phased implementations, use of multiple contracts, and identification of "usable assets."

4.11.3. OMB Memoranda M-10-26 ("Immediate Review of Financial Systems IT Projects"June 28, 2010) recommends that agencies split projects into smaller, simpler segments with clear deliverables. Project segments should generally take no longer than 90 -120 days to achieve specific project milestones. Although all specific milestones may not deliver functionality, all such milestones must support the delivery of well defined functionality. This approach simplifies planning, development, project management and oversight, and training. It reduces risk and allows changes in technology to be incorporated into later phases at lower costs.

4.11.4. For the AS, please identify the following items:

4.11.4.1. Was the contract competitively awarded? If not, please explain why with ample justification. How has the government ensured a "full and open" competition process as part of the AS? If a sole source or limited competition is utilized, has the project conducted or made available the studies, reviews, and documents that provide ample documentation that full and open is not viable? Would the justification provided by the project meet any criteria set down by the Air Force's Competition Advocate (such as the acquisition of critical intellectual property or data rights)?

4.11.4.2. Is the contract performance-based?

4.11.4.3. Is earned value management built into the contract? If not, why not?

4.11.4.4. Does the contract include the required security and privacy clauses (e.g., Privacy Act of 1974, 5 USC Section 552a and OMB Circular No. A-130, Attachment I)?

4.11.4.5. Is there an acquisition plan that has been approved in accordance with Air Force requirements? If yes, when was it approved? If not approved, why has it not been approved?

4.11.5. The best document to use to answer element #10 is an approved AS. Other potential sources of information include the AP and the ORD.

4.12. **CCA Compliance Element 11. Register Mission-Critical and Mission-Essential systems with the DoD CIO.**

4.12.1. EITDR is the AF system of record for IT management data, and it serves as the single AF repository for AF IT initiative/system information to share data across all AF IT management processes. EITDR is migrated to the DoD Information Technology Portfolio Repository (DITPR) as its system of record.

4.12.2. PMs are responsible for ensuring that their program is registered in EITDR and that the information in EITDR is complete, current, and accurate. In order to register an IT program in EITDR, user access must first be established. To obtain access to EITDR, IT program personnel must complete DD Form 2875. The required forms, user guides, and additional information on the registration process may be found on the EITDR CoP located at **https://afkm.wpafb.af.mil/asps/DocMan/DOCMain.asp?Tab=0&FolderID=OO-TR-MC-16-34-1&Filter=OO-TR-MC-16**.

4.12.3. Once access is established and the registration process begins, there are several basic sets of registration and reporting requirements that must be followed. All programs must follow the "Basic Registration" filter that addresses basic program information such as name of the program, certification and accreditation (C&A) Status, and project description in order to be assigned an EITDR Registration Number. Depending upon the nature of the program being registered, one might have to address other filters such as FISMA, ISP, and Section 508.

4.12.4. Completion of questions in the CCA filter documents basic information about a program including "Does this investment acquire Information Technology (IT)?", "What Acquisition Category or Tier is your program?", and "Please identify the milestone schedule for your program, denoting current milestones and the dates for the milestones already attained and for future milestones."

4.12.5. After a program has been approved as CCA compliant, SAF/A6PP will enter the approved CCA memorandum or e-mail into EITDR.

5. Post-Implementation Reviews.

5.1. There are multiple statutory and regulatory requirements for a performance and results-based management and reporting. At present, DoD Instruction 5000.02 (Enclosure 4, Tables 2-1 and 2-2) requires a Post-Implementation Review (PIR) for MAIS, MDAP, and ACAT II and below acquisition programs at the Full-Rate Production Decision Review/Full-Deployment Decision Review (FRPDR/FDDR). The tables cite the following as their justification: Paragraph (a)(5) of Section 1115 of title 31, U.S.C., and Section 11313 of Title 40 (formerly the Clinger-Cohen Act of 1996). The rewrite of DoDI 5000.02 may limit PIR reviews to MAIS programs only.

5.2. Additional regulatory requirements are found in OMB rules as well. OMB Circular No.A-11, Part 7 requires that agencies "conduct post-implementation or post-occupancy reviews of capital programming and acquisition processes, and projects to validate estimated

benefits and costs, and document effective management practices, i.e., lessons learned, for broader use." OMB Circular A-130 (Revised) that requires agencies, as part of their evaluation of their capital planning process, to "conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use." OMB Circular A-130 also directs agencies to "document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge."

5.3. The development of OBPMs is a first step towards development of the PIR (see section 4.3). After a program is deployed, a PIR is conducted to assess whether the needed mission effects were met and whether the functional gap was filled by the materiel solution selected by the capability/mission/program owner. The PIR should answer the question, "Did we (i.e., the Service or program) get what it needed and, if not, what should be done?" It is conducted to determine how accurately the program met its performance and cost objectives, expected benefits, and strategic goals of the Air Force. It is an important diagnostic tool for measuring the success of a particular acquisition or investment.

5.4. The PIR looks at the contribution made by all the elements of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) toward achievement of the needed capability, including return on investment. For example, the system may be fully functional but if the doctrine does not reflect the capability, or the leadership has not been educated in the exploitation of the capability, then the selected OBPMs should reveal such shortcomings.

5.5. The PIR compares actual system performance to program expectations and mission realities based upon the operational environment and the Concept of Operations (CONOPS). The PIR evaluates the project's benefit-cost and risk analyses, and the projected benefits to mission accomplishment and the proposed performance measures for comparing expected versus actual results.

5.6. The PIR should identify the gaps that current investments are not meeting and thereby influence future investment decisions or adjustments to the next increment of the program being analyzed. If the expected benefits are not being achieved, AF management must decide whether to terminate the project; initiate any changes or modifications to the project that may be needed; or leave the project unchanged.

5.7. After the OBPMs have been developed, there are four activities that are part of a successful PIR implementation.

5.7.1. Plan the PIR. A draft PIR plan is developed and then submitted to the Title 40/CCA Action Officer at MS B, and a final PIR plan is due at the last acquisition milestone – FRPDR/FDDR. When planning the PIR, consider topics such as timing, identification of scope and stakeholders, and identification of information sources.

5.7.2. Conduct the PIR. The PIR should be carried out according to the PIR planning that was reviewed and approved at the FRPDR/FDDR. This activity involves collecting measurement data, performing measurement analysis, and presenting the results so that the results of the PIR can be used to make decisions. Analysis, in the form of quantitative and qualitative indicators against the OBPMs, should be based on answering

the question, "Did we get what we needed?" Data collection techniques will vary according to circumstance, but may include surveys, interviews, observations document analysis, and focus groups. Background material can include feasibility studies, value management reports, cost plans, field reports, etc.

5.7.3. Analyze the Results. The PIR should assess the extent to which the DoD's investment decision-making processes were able to capture the warfighter's initial intent. The PIR should also address, if possible, whether the warfighter's 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.

5.7.4. 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. The results of the PIR can 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 OBPMs can be developed to enhance the assessment of future spirals or similar IT investment projects.

5.8. A draft PIR plan should be submitted for review at milestone B, and a final PIR plan is due at the last acquisition milestone – Milestone C, Full Rate Production Decision Review (FRPDR), and Full Deployment Decision Review (FDDR). Programs should prepare the PIR if they are in the post-milestone C phase for a MAIS or MDAP program, assuming that the program has been fielded and is operational in its intended environment and does not have a future milestone. Such programs are in the sustainment phase, meaning they are not spending any funds on enhancement, development, or modernization. The PIR itself is held after Initial Operational Capability (IOC) but prior to Full Operational Capability (FOC). The PIR is also referred to as a Post-Deployment Review (PDR) in DoD and Department of the Navy (DoN) CIO documents.

5.9. When planning the PIR, consider the following factors: timing of the PIR, identification of scope and stakeholders, team composition, and identification of information sources. The different PIR documents may be submitted separately from the CCA Compliance Report.

5.10. The PIR does not have to be a single event or test. It is a sequence of activities that when combined, provide the necessary information to successfully compare actual system performance to program expectations. In some cases, these activities can take place over a long period of time. Some activities measurable for the PIR may be accomplished in the context of typical program acquisition activities or system operational processes.

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-1, *Cyberspace Support*, 9 August 2012

AFPD 33-2, *Information Assurance (IA) Program,* 3 August 2011

AFI 10-601, *Operational Capability Requirements Development,* 12 July 2010

AFI 33-200, *Information Assurance (IA) Management,* 23 December 2008

AFI 33-210, *Air Force Certification and Accreditation Program,* 23 December 2008

AFI 63-101, *Acquisition and Sustainment Life Cycle Management,* 17 April 2009

CJCSI 3170.01C, *Operation of the Joint Capabilities Integration and Development System,* 1 May 2007

CJCSI 3170.01G, *Joint Capabilities Integration and Development System (JCIDS),* 1 March 2009

CJCSI 6212.01E *Interoperability and Supportability of IT and National Security Systems*, 15 December 2008

Clinger-Cohen Act Compliance/Certification Community of Practice (CoP) site

Clinger Cohen Act of 1996 and Related Documents, DoD, May 2000 (the "Purple Book")

Defense Acquisition Guidebook

DoD Chief Information Officer – Laws, Regulations, and Policies, 2009 Edition

DoDD 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security System (NSS),* 5 May 2004

Department of Defense Directive (DoDD) 5000.01, *The Defense Acquisition System,* 12 May 2003

DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008

DoDD 8000.01, *Management of the Department of Defense Information Enterprise,* 10 February 2009

DoDD 8100.01, *Global Information Grid (GIG*), 8 February 2009

DoDD 8500.1, *Information Assurance (IA), 24 October 2002*

DoDD 8500.01E, *Information Assurance (IA),* 24 October 2002

DoDI 8500.2, *Information Assurance (IA) Implementation,* 6 February 2003

DoDI 8580.1, *Information Assurance in the Defense Acquisition System*;

DTM 09-025, *Space Systems Acquisition Process*

DTM 11-009, *Acquisition Policy for Defense Business Systems (DBS),* June 23, 2011

Federal Information Security Management Act (FISMA), PL 107-347

Information Technology Management Reform Act, Division E, PL 104-106

Information Technology: Additional Responsibilities of Chief Information Officers, 10 USC Section 2223

National Defense Authorization Act (NDAA), multiple years

Paperwork Reduction Act, PL 104-13 (as amended)

Abbreviations and Acronyms

ACAT—Acquisition Category

AFRB—Air Force Review Board

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Document

AoA—Analysis of Alternatives

AP—Acquisition Plan

APB—Acquisition Program Baseline

APD—Applicable Program Documentation

AS—Acquisition Strategy

ASP—Acquisition Strategy Panel

ATO—Authority to Operate

BCA—Business Case Analysis

BCL—Business Capability Lifecycle

BMA—Business Mission Area

BPR—Business Process Reengineering

BTA—Business Transformation Agency

C&A—Certification and Accreditation

CA—Certifying Authority

CAIG—Cost Analysis Improvement Group

CARD—Cost Analysis Requirements Descriptions

CBA—Capabilities Based Assessment

CCA—Clinger-Cohen Act of 1996

CCACR—Clinger-Cohen Act Compliance Report

CD—ROM—Compact Disk-Read Only Memory

CDD—Capability Development Document

CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CJCSM—Chairman of the Joint Chiefs of Staff Manual

CND—Computer Network Defense

CONOPS—Concepts of Operations

COTS—Commercial-Off-the-Shelf

CPD—Capability Production Document

DAA—Designated Accreditation Authority

DBS—Defense Business System

DBSMC—Defense Business Systems Management Committee

DIACAP—DoD Information Assurance Certification and Accreditation Process

DIMA—Defense Intelligence Mission Area

DISR—DoD Information Technology Standards Registry

DITPR—DoD Information Technology Portfolio Repository

DME—development, modernization and enhancement

DoD—Department of Defense

DOD IEA—DOD Information Enterprise Architecture

DoDAF—DoD Architecture Framework

DoDD—DoD Directive

DoDI—DoD Instruction

DoN—Department of the Navy

DOTMLPF—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities

DTM—Directive-Type Memorandum

EA—Economic Analysis

EIEMA—Enterprise Information Environment Mission Area

EITDR—Enterprise Information Technology Data Repository

EVMS—Earned Value Management System

EVT—Economic Viability Tool

FISMA—Federal Information Security Management Act

FOC—Full Operating Capability

FDD—Full Deployment Decision

FDDR—Full Deployment Decision Review

FRPD—Full Rate Production Decision

FRPDR—Full Rate Production Decision Review

GAO—General Accountability Office

GIG—Global Information Grid

GOTS—Government Off-the-Shelf

GTG—GIG Technical Guidance

IAS—Information Assurance Strategy

IAM—Information Assurance Manager

IATF—Information Assurance Technical Forum

IATO—Interim Authority to Operate

ICD—Initial Capabilities Document

IER—Information Exchange Requirements

IOC—Initial Operational Capability

IRB—Investment Review Board

IS—Information System

ISP—Information Support Plan

IT—Information Technology

ITA—Information Technology Architecture

JCA—Joint Capabilities Areas

JCIDS—Joint Capabilities Integration and Development System

JCSFL—Joint Common Systems Functional List

KPP—Key Performance Parameter

LCCE—Life-Cycle Cost Estimate

LCMP—Life Cycle Management Plan

MAC—Mission Assurance Category

MAIS—Major Automated Information Systems

MAJCOM——Major Command

MDA—Milestone Decision Authority

MDAP—Major Defense Acquisition Programs

MDD—Material Development Decision

MNS—Mission Need Statement

MOE—Measures of Effectiveness

NCOW-RM—Net-Centric Operations and Warfare Reference Model

NDAA—National Defense Authorization Act

NR-KPP—Net-Ready–Key Performance Parameter

NSS—National Security Systems

OBPM—Outcome-Based Performance Measures

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

ORD—Operational Requirements Document

OT&E—Operational Test and Evaluation

OV—Operational View

PDR—Post-Deployment Review

PEO—Program Executive Officer

PIR—Post-Implementation Review

PM—Program Manager

PMO—Program Management Office

PPP—Program Protection Plan

RDS—Records Disposition Schedule

ROI—Return on Investment

SAF—Secretary of the Air Force

SAP/SAR—Special Access Program/Special Access Required

SME—Subject Matter Expert

SSAA—System Security Authorization Agreement

SSAP—Space Systems Acquisition Process

TEMP—Test and Evaluation Master Plan

USAF—United States Air Force

WMA—Warfighting Mission Area

Terms

Defense Business System—An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and IA infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (National Defense Authorization Act (NDAA) of 2012, as amended, 10 USC 2222(j)(1).

Global Information Grid—The 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, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems (NSS). (DoDD 8100.01).

National Security System—Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system, is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (DoDD 8000.01, February 10, 2009).

Net-Ready Key Performance Parameters—Assess the information needs, information timelines, information assurance, 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 is comprised of the following elements: compliance with the NCOW-RM; compliance with applicable GIG key interface profiles; verification of compliance with the DoD IEA requirements; and supporting integrated architecture products required to assess information exchange for a given capability. (CJCSI 3170.01E).

Attachment 2

EXCERPT FROM DODI 5000.02,
ENCLOSURE 5, SECTIONS 1 – 3

IT CONSIDERATIONS

1. CLINGER-COHEN ACT (CCA) COMPLIANCE. Subtitle III of Reference (v) (formerly known as Division E of CCA) (hereinafter referred to as "Title 40/CCA") applies to all IT investments, including NSS.
a. For all programs that acquire IT, including an NSS, at any ACAT level, the MDA shall not initiate a program or an increment of a program, or approve entry into any phase of the acquisition process; and the DoD Component shall not award a contract until:

(1) The sponsoring DoD Component or PM has satisfied the requirements of Title 40/CCA;

(2) The DoD Component CIO, or designee, confirms Title 40/CCA compliance; and

(3) For MDAPs and MAIS programs only, the DoD CIO also confirms Title 40/CCA compliance.

b. The Title 40/CCA requirements identified in Table 8 of this enclosure shall be satisfied to the maximum extent practicable through documentation developed under the JCIDS and the Defense Acquisition System. The DoD Component Requirements Authority, in conjunction with the Acquisition Community, is accountable for actions 1-5 in Table 8; the PM is accountable for actions 6-11. The PM shall prepare a table similar to Table 8 to indicate which documents (including page and paragraph) correspond to the Title 40/CCA requirements. CIOs shall use the documents cited in the table prepared by the PM to assess and confirm Title 40/CCA compliance.

c. The OIPT shall resolve issues related to compliance for MAIS programs and MDAPs. The IRB shall resolve issues related to compliance for MAIS and MDAP defense business systems. Reference (f) has more information supporting Title 40/CCA compliance.

2. TIME-CERTAIN ACQUISITION OF AN IT BUSINESS SYSTEM. Before providing Milestone A approval for an IT business system, the MDA shall determine that the system will achieve IOC within five years (section 811 of P.L. 109-364 (Reference (az))). This MDA determination is not required for NSS, but is required for AIS defense business systems, including those that are also MAIS or MDAP.

3. DEFENSE BUSINESS SYSTEMS MANAGEMENT COMMITTEE (DBSMC) CERTIFICATION APPROVAL. For defense business system acquisition programs that have modernization funding exceeding $1,000,000, the MDA shall not grant any milestone or full-rate production approval or their equivalent, and the authority to obligate funding shall not be granted until the certification under paragraph (a) of section 2222 of Reference (k) has been approved by the DBSMC (see Enclosure 11).

Attachment 3

DESCRIPTION AND DECISION AUTHORITY FOR ACAT I – III PROGRAMS

(DODI 5000.02, Enclosure 3, Table 1)

Acquisition Category	Reason for ACAT Designation	Decision Authority
ACAT I	1. MDAP (section 2430 of Reference (k)) 1. Dollar value: estimated by the USD(AT&L) to require an eventual total expenditure for research, development, test and evaluation (RDT&E) of more than $365 million in fiscal year (FY) 2000 constant dollars or, for procurement, of more than $2.190 billion in FY 2000 constant dollars 2. MDA designation 1. MDA designation as special interest	ACAT ID: USD(AT&L) ACAT IC: Head of the DoD Component or, if delegated, the CAE (not further delegable)
ACAT IA[1, 2]	1. MAIS (Chapter 144A of Reference (k)): A DoD acquisition program for an Automated Information System[3] (either as a product or a service) that is either: 1. Designated by the MDA as a MAIS; or 2. Estimated to exceed: a. $32 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 in any single fiscal year; or b. $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 c. $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. 3. MDA designation as special interest	ACAT IAM: USD(AT&L) or designee ACAT IAC: Head of the DoD Component or, if delegated, the CAE (not further delegable)
ACAT II	1. Does not meet criteria for ACAT I 2. Major system a. Dollar value: estimated by the DoD Component Head to require an eventual total expenditure for RDT&E of more than $140 million in FY 2000 constant dollars, or for procurement of more than $660 million in FY 2000 constant dollars (section 2302d of Reference (k)) b. MDA designation[4] (paragraph (5) of section 2302 of Reference (k))	CAE or the individual designated by the CAE[4]
ACAT III	1. Does not meet criteria for ACAT II or above 2. AIS that is not a MAIS	Designated by the CAE[4]

1. In some cases, an ACAT IA program, as defined above, also meets the definition of an MDAP. The USD (AT&L) shall be the MDA for such programs unless delegated to a DoD Component. The statutory requirements that apply to MDAPs and MAIS shall apply to such programs.
2. The MDA (either the USD (AT&L) or, if delegated, the ASD (NII)/DoD CIO or another designee) shall designate MAIS programs as ACAT IAM or ACAT IAC. MAIS programs shall not be designated as ACAT II.
3. Automated Information System: 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:
   a. an integral part of a weapon or weapon system;
   b. used for highly sensitive classified programs (as determined by the Secretary of Defense);
   c. used for other highly sensitive information technology programs (as determined by the ASD(NII)/DoD CIO); or
   d. 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).
4. As delegated by the Secretary of Defense or Secretary of the Military Department.

Attachment 4

TYPICAL EVIDENCE OF CCA COMPLIANCE BY PROGRAM DOCUMENT

(From DoDI 5000.02, Enclosures 4 and 5)

Program Document (signed documents must be provided as evidence of compliance)	**Title 40/ CCA Elements**	**Typical Milestone**
Acquisition Program Baseline (APB) {Net-Ready KPP}	2, 7, 8	B
Acquisition Strategy (AS)	4, 7, 10	
Analysis of Alternatives (AoA)	3, 4, 5	A, B, C
Capability Development Document (CDD)	2, 3	B
Capability Production Document (CPD)	2, 3	C
Certificate of Interoperability	8	B, C
Certificate of Supportability	8	B, C
Concepts of Operations (CONOPS)	3	A, B
Economic Analysis with Return on Investment (EA w/ ROI)	6	A, B, C, FRP
Program Office Estimate (POE) or Life-cycle Cost Estimate (LCCE)	6	B, C, FRP
Independent Life-cycle Cost Estimate (N/A for AIS) Component Life-cycle Cost Estimate/Army Cost Position (MAIS and ACAT IC programs)	6 6	B, C, FRP
Cost Analysis Requirements Description (CARD) (MDAPs only)	6	B, C, FRP
EITDR number (EITDR updates into DITPR)	11	B
Information Assurance Strategy (IAS)	9	A, B, C, FRP
Information Support Plan (ISP) {Net-Ready KPP}	8	B, C
Initial Capabilities Document (ICD), {MNS, ORD}	1, 2, 3	A, B, C
Life Cycle Management Plan (LCMP)	4, 7, 10	B

Attachment 5

ARCHITECTURE ASSESSMENT CHECKLIST FOR CCA COMPLIANCE

ISSUE	EXPLANATION
1. Is the system consistent with the applicable Air Force CONOPS?	Does the system fit within the general construct of the CONOPS they say they support? Does it fit within the command and control construct of the CONOPS? For example, can the system operate from austere bases if called for, etc.?
2. Is the architecture of the system consistent with the Air Force Enterprise Architecture?	The system architecture describes the activities to be performed and an analysis is done to determine if the systems functions supports the AFEA construct. An essential element of this is whether the architecture was developed and contains the applicable portions of the DoD IEA or NCOW-RM. Net-centric operations and communications are essential elements of the AFEA and the GIG and should be reflected in the architecture.
3. Is the CONOPS of the system consistent with the Air Force CONOPS?	Is how the system will be used consistent with current USAF policy? For example, rescue systems are not supposed to deploy without top cover.
4. Is the architecture of the system consistent with the system CONOPS?	The functions the architecture outlines should be aligned with the written CONOPS of the system. For example, if the architecture describes air refueling so should the system CONOPS. This is based on an understanding of the system architecture, primarily the OV-5 from architecture developed with DoDAF 1.5 or earlier and the OV-5b in DODAF 2.0, and system CONOPS as stated in the JCIDS document or ISP.
5. Is the architecture of the system consistent with the stated/approved requirements from the Air Force Requirements for Operational Capability Council (AFROCC)?	If a change is being proposed to the system, is it within the bounds of the AFROCC approved JCIDS documents?
6. Is the architecture of the system syntactically correct?	Is the architectural functional decomposition logical? Are the architecture products logically related and traceable between views?
7. Does the architecture of the system meet the stated legal requirements of the acquisition process? Are the right architecture products available when required?	Is the architecture aligned with or use the architectural constructs of guiding higher level architectures (BEA, DoD IEA, NCOW-RM, etc.)? CJCSI 3170.01 defines the required views for each milestone. Are they there and do they contain the required data?
8. Are the Key Performance Parameters (KPPs)	The architecture is used to define the systems interface points. For architectural documents produced prior to June 2009, the

answered consistent with the architecture and CONOPS of the system? Can the key interfaces associated with the Key Interface Profiles (KIPs) be found within the architectural products?	Key Interfaces are defined by the GIG KIPs, and then they are documented in the KIP table in the Net-Ready Key Performance Parameters (NR-KPPs). For architectural products produced after June 2009, these interfaces are found in the "Technical Standards/Interfaces" element of the GTG. These interfaces should also match those in the system's CONOPS. If built properly, the architecture contains enough data to define the net-centric characteristics the system needs to achieve its required mission. This culminates in the System View-6 (SV-6) that describes the required systems interfaces and the data and quality of service need. This is used to create the development and operational test plans used by the contractor, AF testers, and the Joint Interoperability Test Command. These tests can occur months or years after the architecture was developed.
9. Is the ISP consistent with the architecture and CONOPS of the system?	All the common aspects of the ISP, JCIDs documents, and architecture are the same. One consistent data set should feed all three documents.
10. Are there any impediments to CCA confirmation of compliance?	Cost, schedule, and performance issues. Lack of documentation to confirm CCA compliance.

Attachment 6

INFORMATION ASSURANCE STRATEGY TEMPLATE
(PROGRAM NAME) Acquisition IA Strategy

I. Program and System Description.

A. Program Information (Applicable to MS A, B, C, FRP/FDD)

Identify the Acquisition Category (ACAT) of the program. Identify current acquisition life-cycle phase and next milestone decision. Include a graphic representation of the program's schedule.

B. System Description (Applicable to MS A, B, C, FRP/FDD)

Include or reference a high-level overview of the specific system being acquired. Characterize the system as to type of DoD information system (AIS application, enclave, platform IT interconnection, outsourced IT-based process), or as Platform IT without a GIG interconnection. Include or reference a graphic (block diagram) that shows the major elements/subsystems that make up the system or service being acquired, and how they fit together. Describe or reference the system's function, and summarize significant information exchange requirements and interfaces with other IT or systems, as well as primary databases supported. Identify the primary network(s) to which the system will be connected (e.g. NIPRNET, SIPRNET, JWICS, etc.). Include a description or graphic defining the system's accreditation boundary.

II. Information Assurance Requirements.

A. Sources (Applicable to MS A, B, C, FRP/FDD)

1. Mission Assurance Category and Confidentiality Level

Identify the system's MAC and Confidentiality Level as specified in the applicable capabilities document, or as determined by the system User Representative on behalf of the information owner, in accordance with DoD Instruction 8500.2. If the system architecture includes multiple segments with differing MAC and CL combinations, include a table listing all segments and their associated MAC and CL designations, as well as a brief rationale for the segmentation. If the system is a National Security System, state such and indicate question N78 has been answered in EITDR.

2. Baseline IA Control Sets

Identify the applicable sets of Baseline IA Controls from DoD Instruction 8500.2 that will be implemented. A listing of individual controls is not required.

3. ICD/CDD/CPD specified requirements

List any specific IA requirements identified in the approved governing capability documents (e.g. Initial Capabilities Document, Capability Development Document or Capability Production Document).

4. Other requirements

List any IA requirements specified by other authority (i.e. Component mandated).

B. IA Budget (scope and adequacy) (Applicable to MS A, B, C, FRP/FDD)

Describe how IA requirements for the full life cycle of the system (including costs associated with certification and accreditation activities) are included and visible in the overall program budget. Include a statement of the adequacy of the IA budget relative to requirements.

III. System IA Approach (high level): (Applicable to MS B, C, FRP/FDD)

A. System IA technical approach

Describe, at a high level, the IA technical approach that will secure the system.

B. Protections provided by external system or infrastructure

List any protection to be provided by external systems or infrastructure (i.e. inherited control solutions).

IV. Acquisition of IA Capabilities and Support: (Applicable to MS B, C, FRP/FDD)

Describe how the program's contracting/procurement approach is structured to ensure each of the following IA requirements are included in system performance and technical specifications, RFPs and contracts (as well as other agreements, such as SLAs, MOAs, etc.) early in the acquisition life cycle.

A. System IA capabilities (COTS or developmental contract)

B. GFE/GFM (external programs)

C. System IA capabilities as services (commercial or government)

D. Information Systems Security Engineering (ISSE) services

E. IA professional support services to the program (commercial or government, including C&A support)

Confirm that program contracts/agreements communicate the requirement for personnel performing IA roles to be trained and appropriately certified in IA in accordance with DoD Directive 8570.01.

V. System Certification and Accreditation:

A. Process (DIACAP; DCID 6/3, etc) (Applicable to MS A, B, C, FRP/FDD)

Identify the specific Certification and Accreditation (C&A) process to be employed (e.g., DoD Information Assurance Certification and Accreditation Process (DIACAP), NSA/CSS

Information Systems Certification and Accreditation Process (NISCAP), DoD Intelligence Information System (DODIIS)). If the system being acquired is platform IT without a GIG interconnection, describe any Component level process imposed to allocate and validate IA requirements prior to operation.

B. Key role assignments (Applicable to MS B, C, FRP/FDD)

Include the name, title, and organization of the Designated Accrediting Authority, Certification Authority, and User Representative for each separately accreditable system being acquired by the program.

C. C&A timeline (Applicable to MS B, C, FRP/FDD)

Include a timeline graphic depicting the target initiation and completion dates for the C&A process, highlighting the issuance of Interim Authorization to Test (IATT), Interim Authorization to Operate (IATO), and Authorizations to Operate (ATOs). Normally, it is expected that an ATO will be issued prior to operational test and evaluation.

D. C&A approach (Applicable to MS B, C, FRP/FDD)

If the program is pursuing an evolutionary acquisition approach, describe how each increment will be subjected to the certification and accreditation process. If the C&A process has started, identify significant activity completed, and whether an ATO or IATO was issued. If the system being acquired will process, store, or distribute Sensitive Compartmented Information, compliance with Intelligence Community Directive (ICD) 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation" is required, and the plan for compliance should be addressed. Do not include reiterations of the generic descriptions of the C&A process (e.g. general descriptions of the DIACAP activities from DoDI 8510.01 and the DIACAP Knowledge Service).

VI. IA Testing:

A. Testing Integration (Applicable to MS A, B, C, FRP/FDD)

Confirm that all IA testing and C&A activities will be/has been integrated into the program's test and evaluation planning, and incorporated into program testing documentation, such as the Test and Evaluation Strategy and Test and Evaluation Master Plan.

B. Product Evaluation (e.g. IA/IA enabled products) (Applicable to MS B, C, FRP/FDD)

List any planned incorporation of IA products/IA enabled products into the system being acquired, and address any acquisition or testing impacts stemming from compliance with NSTISSP Number 11.

C. Cryptographic Certification (Applicable to MS B, C, FRP/FDD)

List any planned incorporation of cryptographic items into the system being acquired, and address any acquisition or testing impacts stemming from the associated certification of the items by NSA or NIST prior to connection or incorporation.

VII. IA Shortfalls: (Include as classified annex if appropriate) (Applicable to MS B, C, FRP/FDD)

A. Significant IA shortfalls

Identify any significant IA shortfalls, and proposed solutions and/or mitigation strategies. Specify the impact of failure to resolve any shortfall in terms of program resources and schedule, inability to achieve threshold performance, and system or warfighter vulnerability. If applicable, identify any Acquisition Decision Memoranda that cite IA issues. If no significant issues apply, state "None".

B. Proposed solutions and/or mitigation strategies

If the solution to an identified shortfall lies outside the control of the program office, include a recommendation identifying the organization with the responsibility and authority to address the shortfall.

VIII. Policy and Guidance: (Applicable to MS A, B, C, FRP/FDD)

List the primary policy guidance employed by the program in preparing and executing the Acquisition IA Strategy, including the DoD 8500 series, and DoD Component, Major Command/Systems Command, or program-specific guidance, as applicable. The Information Assurance Support Environment web site provides an actively maintained list of relevant statutory, Federal/DoD regulatory, and DoD guidance that may be applicable. Capsule descriptions of the issuances are not required.

IX. Point of Contact: (Applicable to MS A, B, C, FRP/FDD)

Include the name and contact information for the program management office individual responsible for the Acquisition IA Strategy document. It is recommended that the system's Information Assurance Manager (as defined in DoD Instruction 8500.2) be the point of contact.

Attachment 7

INFORMATION ASSURANCE STRATEGY TEMPLATE
FOR SYSTEMS IN SUSTAINMENT UNDERGOING MODERNIZATION

PAGE 1

SYSTEM NAME - ACRONYM
VERSION
DATE

PAGE 2

1. System Registration Number: (EITDR / DITPR)
2. Mission Assurance Category: (MAC I, II, or III)
3. Confidentiality Level: Public, Sensitive, Classified
4. National Security System (NSS): Yes / No
5. NSS Category:
6. Mission Area: Warfighting, Business, Intelligence, Enterprise Information Environment
7. Mission Criticality: Essential, Critical
8. Accreditation Type: ATO, IATO
9. This is the first, second, other IATO
10. Current Accreditation Expiration Date:
11. Information System Owner:
12. Designated Accrediting Authority:
13. Program Manager: (name and phone number)
14. IAM: (name and phone number)
15. System Baseline IA Controls Set: (list)
16. IA Controls affected by the configuration change: (list)
17. Planned IA Control Testing Milestones:
    (estimated test completion date for each Control – list)

Attachment 8

EXCERPT FROM DIRECTIVE-TYPE MEMORANDUM 11-009, ACQUISITION POLICY FOR DEFENSE BUSINESS SYSTEMS (DBS), JUNE 23, 2011

TABLE 4. CCA (REFERENCE (O)) COMPLIANCE FOR DBS USING BCL

ACTIONS REQUIRED TO COMPLY WITH SUBTITLE III OF THE CCA (REFERENCE (O))	APPLICABLE PROGRAM DOCUMENTATION[1]
1. Make a determination that the acquisition supports core, priority functions of the DoD. [2]	Business Case, Program Charter
2. Establish outcome-based performance measures linked to strategic goals. [2]	Business Case, APB approval
3. Redesign the processes that the system supports to reduce costs, improve effectiveness and maximize the use of COTS technology. [2]	Business Case, Program Charter
4. Determine that no Private Sector or Government source can better support the function.	Business Case, Program Charter
5. Conduct an AoA.	Business Case (AoA)
6. Conduct an economic analysis that includes a calculation of the return on investment.	Business Case (EA)
7. Develop clearly established measures and accountability for program progress.	Business Case (APB)
8. Ensure that the acquisition is consistent with the Global Information Grid (GIG) policies and architecture, to include relevant standards (References (j) and (x)).	APB (Net-Ready KPP), Business Case (ISP (Information Exchange Requirements))
9. Ensure that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures. [2]	Acquisition Information Assurance Strategy
10. Ensure, to the maximum extent practicable, that modular contracting has been used, and that 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.	Business Case
11. Register mission-critical and mission-essential systems (see Glossary) systems with the DoD CIO. [2]	DoD IT Portfolio Repository

Notes:
1. The system documents cited are examples of the most likely but not the only references for the required information. I 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 actions are also required to comply with section 811 of Public Law 106-398 Reference (y)).
3. Definitions:
Mission-Critical Information System. A system that meets the definitions of "information system" and "National Security System (NSS)" in the CCA (Reference (0)), the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (The designation of mission-critical shall be made by a DoD Component Head. A financial management IT system shall be considered a mission-critical IT system as designated by the Under Secretary of Defense (Comptroller) (USD(C)/Chief Financial Officer (CFO), DoD.) A "mission-critical IT 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 the CCA (Reference (0)), that the acquiring DoD Component Head determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential shall be made by a DoD Component Head. A financial management IT system shall be considered a mission essential IT system as designated by the USD(C)/CFO.) A "mission-essential IT system" has the same meaning as a "mission-essential information system."