Department of the Army
Pamphlet 25–2–14

Information Management: Army Cybersecurity

Risk Management Framework for Army Information Technology

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–14
Risk Management Framework for Army Information Technology

This new Department of the Army pamphlet, dated 8 April 2019—

- o Amplifies procedures and guidance found in AR 25–2 regarding the process for obtaining and maintaining the Risk Management Framework authorizations necessary for operations of Army information technology (throughout).

- o Supports the Department of Defense transition from the Department of Defense Information Assurance Certification and Accreditation Process to Risk Management Framework process (throughout).

- o Includes roles, duties, instructions, and procedures for the Army's implementation of the Risk Management Framework (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army
Pamphlet 25–2–14

Information Management : Army Cybersecurity

Risk Management Framework for Army Information Technology

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller
KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet provides guidance for implementing the Risk Management Framework within the Department of the Army. It supports AR 25–2 and provides amplifying procedures and guidance to DODI 8500.01 and DODI 8510.01 for Department of Defense information technology.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to all Headquarters, Department of the Army staff; Army commands; Army service component commands; and direct reporting units. It applies to all Army information technology, operational technology, and information in electronic format.

Proponent and exception authority. The proponent for this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the respective policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

UNCLASSIFIED

Contents—Continued

Contents—Continued

Figure List

Chapter 1
Introduction

1–1. Purpose

This pamphlet provides guidance for implementing AR 25–2 policy, and is designed to assist in the transition process for implementing Risk Management Framework (RMF) in Army. It assists Army organizations in effectively and efficiently understanding and implementing RMF for Army information technology (IT). The cybersecurity requirements for DOD ITs are managed through the principals established in DODI 8510.01, the National Institute of Standards and Technology (NIST) Special Publication 800–37, and CNSSI 1253. AR 25–2 issues the regulation needed to ensure consistent implementation of the RMF process within the life cycle of all IT.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See glossary.

1–4. Overview

a. DOD adopted and implemented RMF to replace the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) with the issuances of DODI 8500.01 and DODI 8510.01.

b. DODI 8500.01 adopts the term cybersecurity and replaces the term information assurance (IA) associated with the DIACAP throughout DOD. The 2008 NSPD–54/HSPD–23 defines cybersecurity as “prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

c. DODI 8510.01 establishes the RMF for DOD IT for cybersecurity policies, responsibilities, and risk management within the cybersecurity life cycle for DOD IT based on DOD, NIST, and Committee on National Security Systems (CNSS) standards.

d. RMF establishes a unified information security framework for the entire Federal Government and a risk-based approach for the implementation of cybersecurity. The transition to the RMF leverages existing acquisition and systems engineering personnel, processes, and the compelling evidence (also referred to as artifacts) developed as part of systems security engineering (SSE) activities. RMF employs a catalog of security controls as a baseline and requires a determination of the likelihood of exploitation and the harm done if noncompliant security controls are exploited, enabling operational decisions concerning authorization for initial or continuing operations. RMF emphasizes integration of cybersecurity requirements in the system’s design process, resulting in a more trustworthy system that can dependably operate in the face of a capable cyber adversary. RMF also emphasizes integrating cybersecurity activities into existing processes including system security engineering (SSE), program protection planning, trusted systems and networks analysis, developmental and operational testing, financial management and cost estimating, and sustainment through decommissioning and disposal.

e. RMF is based on a set of key tenets that form the basis for the guidance in this pamphlet. The following tenets are some of the more important concepts and principles that should be followed to successfully implement the RMF process into Army IT. At a minimum:

(1) Cybersecurity is risk-based, mission-driven, and will be addressed in the requirements development phase of the Army’s acquisition process, and continually through decommissioning.

(2) Treat cybersecurity requirements like other system requirements.

(3) System security architecture and data flows are developed early and are continuously updated throughout the system life cycle as the system and environment (including threats) change to maintain the desired security posture based on risk assessments and mitigations.

(4) Implement cybersecurity to increase a system’s capability to protect, detect, react, and restore, even when under attack from an adversary.

(5) Use a modular, open systems approach to implement system and security architectures that support the rapid evolution of countermeasures to emerging threats and vulnerabilities.

(6) Conduct cybersecurity risk assessments early and often, and integrate risk assessments with other risk management activities.

(7) As developmental systems mature and security controls are selected, implemented, assessed, and continuously monitored, continue alignment of cybersecurity with mission, technical baselines, system security architecture, data flows, and design.

(8) Promote reciprocity to the maximum extent possible through ease of sharing risk information of test and assessment results and authorization documentation.

(9) Leverage inheritance whenever possible to reduce duplication of effort and to provide authoritative source for test results and compliance status.

f. The DOD RMF Knowledge Service, available at https://rmfks.osd.mil, is DOD's official site and authoritative source for enterprise RMF policy and implementation guidelines. The RMF Knowledge Service provides cybersecurity practitioners and managers with a single authorized source for execution and implementation guidance, community forums, and the latest information and developments in RMF. The RMF Knowledge Service also hosts a library of tools, diagrams, process maps, documents, and so forth, to support and aid in the execution of RMF.

g. Army adopted Enterprise Mission Assurance Support System (eMASS) as the tool to automate the RMF process. eMASS is available at https://emass-army.csd.disa.mil.

1–5. Who should use this document

Any Army capability or system owner having or seeking to acquire, develop, integrate, deploy, or decommission IT on Army infrastructure.

1–6. Applicability and scope

a. This pamphlet contains a synopsis of RMF policy mandates, unique terms and concepts, roles and duties, and documentation requirements to assist Army personnel. DODI 8510.01 requires all DOD IT (referred to in this document as IT) be assessed, and all information systems (ISs) (consisting of major applications and enclaves) and platform information technology (PIT) systems be assessed and authorized.

b. The information in this pamphlet provides IS owners, IT staff, and security certification officials with a baseline for measuring security design effectiveness and managing design changes that affect cybersecurity throughout the system's life cycle. System standard operating procedures (SOPs) and policies will be used as additional confirmation of compliance with DOD security controls. The term IT refers not only to ISs, which require RMF assessment and authorization (A&A), but also to IT that requires assess only (see chap 6).

Chapter 2
Army Risk Management Framework Process

2–1. Risk Management Framework overview

RMF introduced the following:

a. RMF replaced mission assurance categories with classification of systems, using security levels per the Federal Information Security Modernization Act (FISMA) of 2014 assigning impact values (low, moderate, high) and security objectives (confidentiality, integrity, and availability (CIA)).

b. Confidentiality is no longer associated with classification level in the RMF. There can be unclassified information that requires a high level of protection.

c. Though RMF is primarily applicable at the tier 3 system level, risk assessment considerations include tiers 1 and 2 at the mission and organization level.

2–2. Army governance structure

The Army Cybersecurity Program leverages the multi-tiered organization-wide risk management approach defined in NIST Special Publication 800–39 and shown in figure 2–1.

a. Tier 1–Organization. Risk management at this tier is performed through cybersecurity governance bodies at the Army enterprise level.

b. Tier 2–Mission/Business Process. Risk management at this tier is performed by mission owner (MO) level and is informed by the risk context, risk decisions, and risk activities at tier 1.

c. Tier 3–Information System. Risk management at this tier is performed by individuals responsible for the management of individual IT and is guided by the risk context, risk decisions and risk activities at tiers 1 and 2.

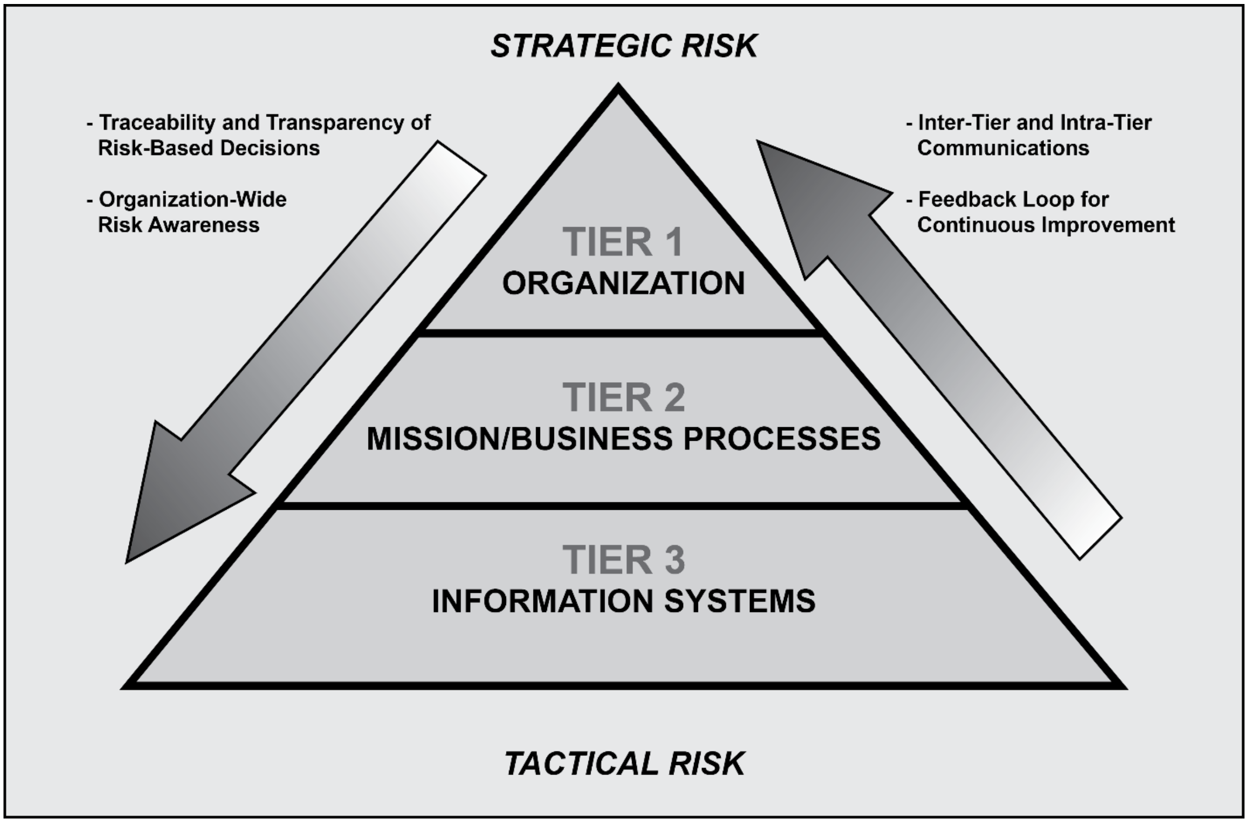

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION/BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Figure 2–1. Army tiered risk management approach

2–3. Army cybersecurity governance

The Army cybersecurity governance structure establishes the framework for how the Army manages cybersecurity risk with respect to the existing Army and DOD corporate boards and processes. The intention is to ensure cybersecurity is addressed in the appropriate forums for both mission/business risk and IT investment/portfolio management. Current governance forums do not regularly discuss cybersecurity nor the risk management process on a regular basis. These new forums ensure these topics are raised to the appropriate level and informed decisions can be made while engaging the cybersecurity community of interest (COI) at all levels (see fig 2–2).

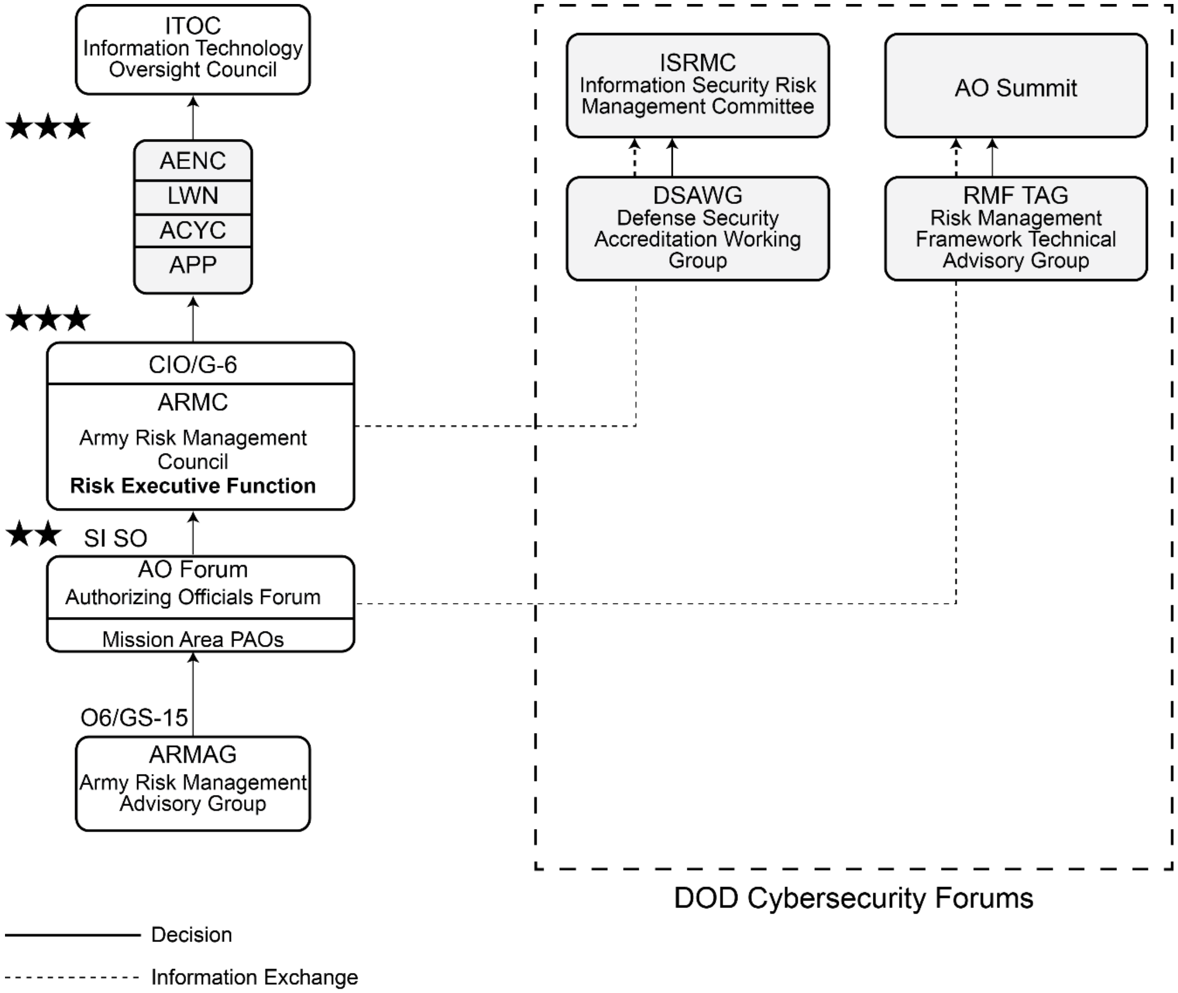

ITOC
Information Technology Oversight Council
★★★
AENC
LWN
ACYC
APP
★★★
CIO/G-6
ARMC
Army Risk Management Council
Risk Executive Function
★★
SI SO
AO Forum
Authorizing Officials Forum
Mission Area PAOs
O6/GS-15
ARMAG
Army Risk Management Advisory Group
ISRMC
Information Security Risk Management Committee
AO Summit
DSAWG
Defense Security Accreditation Working Group
RMF TAG
Risk Management Framework Technical Advisory Group
DOD Cybersecurity Forums
Decision
Information Exchange

Figure 2–2 Army cybersecurity governance

a. The Army leverages existing Army and DOD governance bodies to discuss cybersecurity risk topics and make organizational and mission/business area risk decisions (see fig 2–2 list under Information Technology Oversight Council (ITOC)). These governing bodies are already established and their roles and responsibilities are defined in their corresponding charters. This pamphlet focuses on establishing the cybersecurity bodies at tiers 1 through 3.

b. The following governance groups provide focused management and oversight of the Army Cybersecurity Program. Charters and process guides for each of these organizations will be developed after the publication of this pamphlet. Army cybersecurity funding requirements and prioritization will be coordinated between the risk executive function (REF), the Chief Information Officer (CIO)/G–6 and the senior level governing bodies. This governance will establish the mission area principal authorizing officials (PAOs).

(1) *Information Technology Oversight Council.* The ITOC is a senior review group established by Headquarters, Department of the Army co-chaired by the Under Secretary of the Army and the Vice Chief of Staff Army. The ITOC integrates activities and assessments across the four IT mission areas in order to provide guidance and direction, prioritize investment, allocate resources, and resolve conflicts.

(2) *Army Risk Management Council.* The Army Risk Management Council identifies risk tolerance, accepts risk impacting the Army's mission, and recommends funding prioritization to minimize risk to the Army's mission. It will be co-chaired by CIO/G–6 and U.S. Army Cyber Command (ARCYBER), and will advise the CIO/G–6. Members include representatives from Deputy Under Secretary of the Army, mission area PAOs, the Army Senior Information Security Officer (SISO), and the intelligence community represented by Deputy Chief of Staff (DCS), G–2; DCS, G–8; and DCS, G–3/5/7.

(3) *Authorizing Official Forum.* The Authorizing Official (AO) Forum provides strategic guidance and direction to the Army appointed AOs related to their authorities and responsibilities under the RMF per the direction of the CIO/G–6 and within the terms of the risk management strategy developed by the REF and DODI 8510.01. Chaired by the Army SISO appointed by the CIO/G–6. Members are the Army AOs.

(4) *Army Risk Management Advisory Group.* The Risk Management Advisory Group (RMAG) provides policy clarification to support the implementation of the RMF for DOD IT within the Army and issues Army specific cybersecurity policies to further implement this process supporting the Army mission. The RMAG coordinates issue resolution with the COI and elevates issues as necessary to the AO Forum, issues additional policies associated with security control baselines and overlays, advises established Army forums on how to resolve RMF priorities and cross cutting issues, and develops policy and guidance for facilitating reciprocity within the Army. The chair is an O6/GS–15 in the CIO/G–6 appointed by the SISO and is the Army's representative to the DOD RMF Technical Advisory Group. Members of the RMAG are the appointed program information system security managers (P–ISSMs) and authorizing official designated representatives (AODRs).

2–4. Department of Defense information technology type definition

a. System categorization is within step one of the six RMF process steps for DOD IT Systems, which parallels the system life cycle. The system is categorized in accordance with CNSSI 1253 and the results are documented in the security plan (SP).

b. There are different IT types defined by DOD. Further guidance on defining DOD IT types can be located on the RMF Knowledge Service, under the tabs RMF General, IT, Define DOD IT Type.

c. IT identified on the right side in figure 2–3 needs to be assessed for security risk but not formally authorized.

d. PIT, IT services, and IT products do not need an authorization but must be securely configured in accordance with applicable DOD policies and security controls and undergo special assessment of their functional and security-related capabilities and deficiencies. Conversely, systems that are defined on the left side in figure 2–3 require a full A&A and receive an authorization to operate (ATO) before being authorized to operate on Army networks. The forms of DOD/Army IT, as shown in figure 2–3, range in size and complexity from individual hardware and software products to stand-alone systems to massive computing environments, enclaves, and networks.

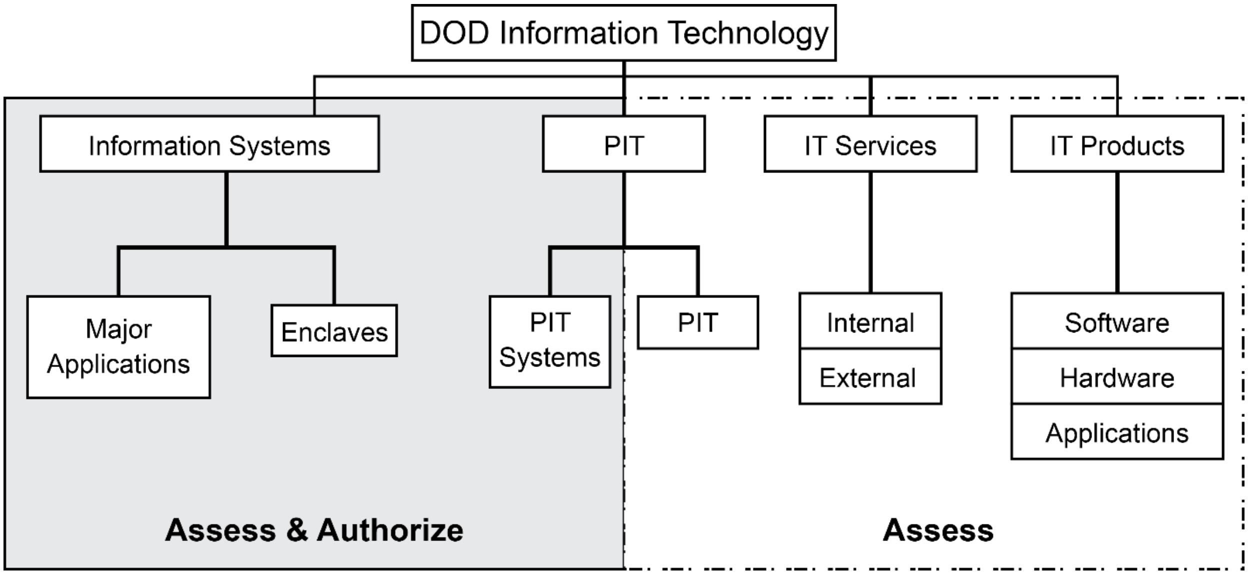


Figure 2–3. Department of Defense information technology types

2–5. Department of Defense information technology types requiring assess and authorize

a. Platform information technology system. A PIT system is a collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. Owners of PIT, in consultation with an AO, may determine that a collection of PITs rise to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support. PIT systems must be designated as such by the responsible agency heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

b. Major application. A major application may be a single software application (for example, Integrated Consumable Items Support), multiple software applications that are related to a single mission (for example, payroll or personnel), or a combination of software and hardware performing a specific support function across a range of missions (for example, Global Command and Control System, Defense Travel System (DTS), and Defense Enrollment Eligibility Reporting System (DEERS)). Major applications include any application that is a product or deliverable of an acquisition category I through III program as defined in DODI 5000.02. Defense Business Systems are mandated under DODI 5000.75, which covers big business major automated information systems (for example, Integrated Personnel and Pay System–Army (IPPS–A) and Logistics Modernization Program (LMP)).

c. Enclave. An enclave is a collection of computing environments connected by one or more internal networks under the control of a single approval and security policy, including personnel and physical security. Enclaves provide standard network cybersecurity and functionality such as boundary defense, incident detection and response, key management, office automation, and electronic mail.

2–6. Department of Defense information technology types eligible for assess only

IT identified on the right side in figure 2–3 needs to be assessed for security risk but not formally authorized.

a. Information technology product. Products are defined by DOD as individual IT hardware or software items. They can be commercial or government-provided and include, but are not limited to, operating systems, office productivity software, firewalls, and routers. IT products do not require authorizations under RMF. However, products must be securely configured in accordance with applicable DOD policies and security controls, such as security technical implementation guides (STIGs) designed by the Defense Information Systems Agency (DISA). Site cybersecurity personnel are responsible for ensuring all products have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

b. Platform information technology. PIT may consist of both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems (in other words, platforms). PIT differs from products in that it is integral to a specific platform type as opposed to being used independently or to support a range of capabilities (for example, major applications, enclaves, or PIT systems). A group of PITs acting in concert with one another may be identified as a PIT system.

c. Information technology service. IT services are outside the service user organization's authorization boundary, and the user's organization has no direct control over the application or assessment of required security controls. DOD organizations that use IT services are typically not responsible for issuing authorization decisions for those services. However, organizations contracting for IT services generally do perform security assessments and sign formal service level agreements (SLAs) enforcing agreed upon cybersecurity standards.

Chapter 3
Roles and Duties

3–1. Risk Management Framework team

a. The RMF team is responsible for implementing the RMF for a specific DOD IS or PIT system. Personnel filling RMF roles must be assigned and qualified for those positions and are listed in the SP. The RMF team includes:

(1) Component CIO.
(2) Army SISO.
(3) AO.
(4) AODR.
(5) Security control assessor (SCA).
(6) Information system owner (ISO).
(7) Program manager (PM) or system manager (SM).
(8) Information system security manager (ISSM).
(9) Information system security officer (ISSO).
(10) Information system security engineer (ISSE).
(11) DOD information system user representative (UR).

b. Cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with this pamphlet and DODM 5200.02, and qualified in accordance with DOD 8570.01–M, DODD 8140.01, and supporting issuances.

c. Specific officials within the Army are assigned responsibility for conducting activities in the RMF authorization and monitoring cycle. Reference NIST Special Publication 800–53 and NIST Special Publication 800–37 with additional input from DODI 8510.01 in cases where roles are defined differently in the two publications.

d. It is important to note that an individual may fill one or more roles in the RMF process. Army sites are not obligated to name different people to each position and may assign multiple roles to the same person if doing so does not violate conflict of interest and enhances organizational efficiency.

e. RMF personnel assigned to perform tasks throughout the RMF accreditation process should be a diverse community of subject matter experts with the knowledge to adequately answer and/or enter test results during self-assessments of systems. The team should consist of network administrators, system administrators, cybersecurity managers, traditional security personnel, and others. The RMF process is not intended to be solely the responsibility of the organizational ISSM.

3–2. Army Chief Information Officer/G–6

In addition to the CIO/G–6 cybersecurity responsibilities listed in DODI 8500.01, DODI 8510.01, AR 25–2, and DA Pam 25–2–12, the CIO/G–6 duties are as follows:

a. Administers the RMF within the Army Cybersecurity Program.

b. Maintain visibility of A&A status of Army ISs and PIT systems through eMASS and Army Portfolio Management Solution (APMS). Verify that an ISO/PM/SM is appointed for each Army IS and PIT system, and the appointment is recorded in Army Training and Certification Tracking System (ATCTS) and APMS.

c. Establish and maintain processes and procedures to manage DOD component plans of action and milestones (POA&Ms).

d. Review and document concurrence on all ATOs issued for Army ISs with a level of risk of very high or high.

e. Oversee modification of ATCTS and APMS to support roles and terminology required for compliance with RMF and AR 25–2.

f. Develop and maintain the Army workspace, landing page, and policy tab within the RMF Knowledge Service.

3–3. Army senior information security officer

The SISO is the official responsible for directing Army's Cybersecurity Program on behalf of the organization's CIO. In addition to the SISO responsibilities documented in DODI 8510.01 and AR 25–2, the Army SISO duties are as follows:

a. Appoint AOs on behalf of the CIO/G–6 in accordance with CIO/G–6 policy and standards.

b. Develop, maintain, and publish the list of approved AOs in the Policy tab of the RMF Knowledge Service.

c. Track the A&A status of IS and PIT systems governed by the DOD component cybersecurity program.

d. Assess the quality, capacity, visibility, and effectiveness of security assessments, and direct modifications as necessary.

e. Ensure AOs integrate cybersecurity concepts in the DOD acquisition program implementation of cybersecurity requirements.

f. Support development of ARCYBER/Network Enterprise Technology Command (NETCOM) RMF operations orders, and tactics, techniques, and procedures (TTP) to ensure compliance with Army and DOD policy.

3–4. Authorizing official

The AO is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. The AO renders authorization decisions for DOD ISs and PIT systems under their purview in accordance with DODI 8510.01. AO duties and requirements are documented in DA Pam 25–2–12.

3–5. Authorizing official designated representative

The AODR is an organizational official that acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process in accordance with NIST Special Publication 800–37. The only activity that cannot be delegated to the AODR by the AO is the authorization decision and signing of the associated authorization decision document. The AODR duties are documented in DA Pam 25–2–12.

3–6. Security control assessor

a. The SCA is the official having the authority and responsibility for the assessment of all ISs and PIT systems governed by an Army Cybersecurity Program. The SCA has the authority to formally evaluate the cybersecurity capabilities and services of a DOD IS and PIT system and issue an authorization recommendation to the authorizing AO. This recommendation accompanies the RMF security authorization package for review towards an authorization decision.

b. The SCA continuously assesses and guides the quality and completeness of RMF activities and tasks and the resulting artifacts. The authority and accountability for security control assessments is vested in the Army SISO.

c. The Army SCA structure has been further divided into four distinct roles to better serve and perform their tasks efficiently:

(1) SCA–Army.

(2) SCA–representative.

(3) SCA–validator.

(4) SCA–organization.

d. CIO/G–6 delegated the responsibility for the RMF SCA activities to ARCYBER who further delegated the SCA responsibilities to NETCOM.

e. SCA–Army duties are as follows:

(1) Perform the IS (tier III) SCA activities for Army IT as documented in DODI 8510.01 and AR 25–2.

(2) Conduct assessments of security controls, quantify the residual risk, and make recommendations to Army AOs.

(3) Recommend remediation actions for noncompliant security controls based on assessment findings, and reassess remediated controls as appropriate.

(4) Prior to publication, coordinate all RMF operations orders and TTPs with the CIO/G–6 appointed SISO to ensure compliance with RMF policies and DA Pams.

(5) Verify that an ISO is identified in APMS and appointment orders are filed in ATCTS for each Army IT prior to performing assessment activities.

(6) Provide RMF status reports associated with SCA activities and the Army RMF process to the Army SISO monthly, or sooner if requested.

(7) Develop and manage the RMF process and eMASS training and scheduling to ensure that the Army cybersecurity community is sufficiently trained.

(8) Manage the Army Nonclassified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) instances of eMASS, and serve as the Army voting member on the eMASS configuration control board (CCB). Coordinate changes with the SISO to ensure that security issues are not introduced.

(9) Appoint SCA–validator leads in accordance with CIO/G–6 policy and standards.

(10) Provide a copy of SCA–validator lead appointments signed by the SCA–Army (or, if digital, public key infrastructure (PKI) certified digitally signed) to the Army SISO.

(11) Develop, maintain, and publish the list of Army-authorized assessors and SCA–validators on the NETCOM's operations tab of the Army workspace on the RMF Knowledge Service.

(12) Develop and maintain the NETCOM operations tab within the Army workspace of the RMF Knowledge Service.

3–7. Security control assessor–representative

a. The SCA–representative acts on behalf of the SCA and assists with the review of system documentation to ensure implementation of security controls has been performed correctly. The SCA–representative also participates in independent assessments and provides technical and managerial support to the SCA–Army, AO, AODR, P–ISSM, and ISO as needed.

Note. This is not an official position under RMF or DOD, but one created based on the current Army organizational structure.

b. SCA–representative duties are as follows:

(1) Work under the direct management of the SCA–Army.

(2) Be assigned to the IS throughout the accreditation process and provide the final risk assessment to the SCA–Army.

(3) Be organized into theater and functional command teams led by a government civilian certified at the information assurance management (IAM) III level.

(4) The SCA–representative civilian command team leads serve as single points of contact for process users.

(5) Be government civilians or contract support and have at least an IAM II certification.

c. Organizing along these lines facilitates building institutional knowledge for theater/functional command missions and operational/threat environments.

3–8. Security control assessor–validator

a. The SCA–validator coordinates with system owner sites to prepare for, schedule, and conduct an independent verification and validation visit. The SCA–validator maintains the authorization timeline, develops a detailed security assessment plan, compiles a list of vulnerabilities discovered during testing, answers technical questions as needed, and provides significant input into the production and approval of A&A packages.

b. The SCA–validator lead is an individual appointed in writing by the SCA–Army, who meets the Army SISO standards, to act on behalf of the SCA–Army to conduct security control assessments. The individual appointed as an SCA–

validator lead must be an accountable military or Department of the Army (DA) Civilian. This standard applies only to the SCA–validator lead; the SCA–validator lead team members may be a mix of government civilians and/or contract support personnel. Government and contract support personnel will be documented during the SCA–validator application process and updated with the SCA–Army as personnel changes occur. Most SCA–validator activities are a reimbursable function.

c. SCA–validator lead duties are as follows:

(1) Ensure continuity (sustain a learning environment that drives continuous improvement in performance and provides a means to share critical knowledge across the organization) within the government of knowledge of Army IS and cybersecurity status and issues.

(2) Ensure the highest level of integrity within the SCA–validator organization and the RMF process.

(3) Be, along with appointed alternate(s), the only individuals authorized to sign or sign on behalf as the SCA–validator lead.

(4) Be accountable to the SCA–Army to include their team and the validation findings.

(5) Attend all NETCOM SCA–validator working focus groups.

(6) Complete a minimum of four evaluation assessments per calendar year (one per quarter).

d. In order to be appointed as the SCA–validator lead, the individual must—

(1) Be a government employee.

(2) Be a U.S. citizen.

(3) Be at least a lieutenant colonel, GS–14 DA Civilian, or equivalent.

(4) Hold a U.S. government security clearance and formal access approvals commensurate with the level of information processed by the IS under his or her purview as an SCA–validator, or a Secret clearance, whichever is higher.

(5) Obtain the current DOD approved certifications for Information Assurance Technical (IAT) II or IAT III and Computer Network Defense–Auditor (CND–AU), such as Global Information Assurance Certification Security Essentials (GSEC), Security Certified Network Professional (SCNP), Security+, Systems Security Certified Practitioner (SSCP), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP) (or Associate), Global Information Assurance Certification Certified Incident Handler (GCIH), Government Sponsored Enterprise (GSE), Security Certified Network Architect (SCNA) and Certified Ethical Hacker (CEH), Global Information Assurance Certification Systems and Network Auditor (GSNA), or other technical certifications associated with security evaluation and/or auditing functions.

(6) At a minimum, have 8 years of high-level (enterprise-level preferred) IT experience, with a minimum of 5 years of senior level experience in cybersecurity in DA, or commensurate experience. This must be demonstrated through submission of applicant's written resume. In addition to the years of experience, the following must be discernable from the resume:

(a) A comprehensive understanding of DOD and DA cybersecurity policy.

(b) Practical application of cybersecurity through security engineering, security test and evaluation (T&E), or major command or project cybersecurity positions.

(c) Knowledge and judgment necessary for making proper evaluations of vulnerabilities and understanding them in the context of their likelihood of exploitation.

(7) Support of the goals and needs of the Army SISO, ARCYBER/NETCOM, and the Army at large; that is, a defense-in-depth view that combines cybersecurity with technological best practices in the best interests of the Army. While there is room for many specialties within the cybersecurity field, the SCA–validator must demonstrate a mature, holistic view of cybersecurity that blends an understanding of the nature of technology, security, the enterprise, and operational needs.

(8) The SCA–validator may be the leader of a larger team that has the technical and subject matter expertise to properly evaluate whether a given IS has met its RMF controls and requirements. There is no minimum or maximum size of the SCA–validator's organization. The amount and type of work the SCA–validator is capable of handling is left to the professional judgment of the SCA–validator lead. Some SCA–validators may specialize in certain technical fields, and thereby be more efficient than others with a more general focus. However, SCA–validators and their teams are not authorized to perform assessments on any systems that they are responsible for under other titles, such as P–ISSM, organization information system security manager (O–ISSM), ISO, PM, system/security engineering, and so forth.

e. Personnel must be appointed prior to personal or organizational representation as an SCA–validator.

f. The SCA–Army publishes the list of authorized SCA–validator leads on the NETCOM operation's page of the Army workspace on the RMF Knowledge Service.

g. The SCA–validator lead immediately notifies the SCA–Army of any changes to the information upon which their appointment decision was made or which adversely affects their ability to perform the SCA–validator mission. Those changes include, but are not limited to:

(1) Changes in the supporting organization that significantly changes the technical or cybersecurity qualifications of the supporting team.

(2) Changes in the duties of the SCA–validator lead within the SCA–validator's organization that might impact their ability to perform SCA–validator duties.

(3) Conflicts of interest associated with specific ISs or projects that should disqualify the SCA–validator from certain functions.

(4) For additional guidance, refer to the ARCYBER/NETCOM SCA–validator TTP located in the Army workspace on the RMF Knowledge Service.

3–9. Security control assessor–organization

a. The SCA–organization is a new Army RMF concept under the purview of the SCA. The SCA–organization is currently only used in the closed restricted network (CRN)/stand-alone information system (SIS) process. The ARCYBER/NETCOM TTPs identify when the SCA–organization can be used in place of other SCA functions.

b. SCA–organization duties are as follows:

(1) Be formally designated in writing by the P–ISSM with the approval of the AO.

(2) Perform all activities reserved for the SCA–Army as described in this pamphlet.

(3) Act on behalf of the SCA–Army for the systems which minimally affect organizations or personnel outside of the program which creates the SIS or CRN.

(4) Act in each of the roles of the SCA–Army, SCA–validator, and SCA–representative.

(5) Perform step two of the RMF control approval chain and the creation of the security assessment report (SAR) within eMASS.

(6) Perform the SCA–representative and SCA–Army roles in the RMF package approval chain.

(7) Be assigned to the organization that is authorizing a SIS or CRN.

(8) Not be the ISO/PM for the system but may be the O–ISSM or P–ISSM for the system.

(9) Not be responsible for the design, operation, or maintenance of the system in their assigned duties.

3–10. Information system owner/program/system manager

a. All DOD ISs and PIT systems must have an appointed ISO or a PM/SM. The ISO/SM is responsible for the procurement, development, integration, modification, operation, maintenance, life cycle management, and disposal of an IS. The ISO/PM is responsible for ensuring the appropriate operational security posture is maintained for the component IS or PIT system.

b. ISO/PM duties are as follows:

(1) Manage system development, operations, and maintenance at the program level.

(2) Ensure the appointment of an O–ISSM and ISSO for each IT system to implement and maintain cybersecurity and satisfy the RMF program's requirements.

(3) Collaborate with AOs, P–ISSMs, ISSOs, and PMs to ensure compliance for all assigned systems.

(4) Collaborate with the ISSO and O–ISSM to identify information types stored or processed with an IT system and assign CIA impact levels for each in accordance with CNSSI 1253, and document the system security categorization in the appropriate Joint Capabilities Integration and Development System capabilities document (for example, capabilities development document).

(5) Appoint a UR for assigned IS's and PIT systems.

(6) Determine the security impact of proposed or actual changes to the IS and its environment of operation.

(7) Conduct remediation actions within specified timelines based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M.

(8) Update the SP, and POA&M based on the results of the continuous monitoring process.

(9) Report the security status of the IS (including the effectiveness of security controls employed within and inherited by the system) to the AO and other appropriate organizational officials on an ongoing basis, in accordance with the monitoring strategy.

(10) Implement an IS decommissioning strategy, when needed, which executes required actions when a system is removed from service.

(11) Obtain AO approval for the SP which specifies the categorization and set of security controls required to meet security requirements for the system.

(12) Accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.

(13) Serve as the focal point for the integration of cybersecurity into and throughout the system life cycle of an assigned DOD IS and PIT system.

(14) Ensure each program acquiring an IS or PIT system has an assigned IS security engineer and that they are fully integrated into the systems engineering process.

(15) Ensure that the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

(16) Enforce AO authorization decisions for hosted or interconnected IS and PIT systems.

(17) Implement and assist the ISSO in the maintenance and tracking of the SP for assigned IS and PIT systems.

(18) Ensure POA&M development, tracking, and resolution.

(19) Ensure periodic reviews, testing, and assessment of assigned IS and PIT systems are conducted no less than annually.

(20) Provide the IS or PIT system description.

(21) Register the IS or PIT system in APMS and eMASS.

(22) Ensure T&E of assigned IS and IT system is planned, resourced, and documented in the program T&E master plan per DODI 5000.02.

(23) Enforce Army and regional cybersecurity policy, developing command-unique procedures as needed.

(24) Ensure cybersecurity personnel implement vulnerability remediation alerts, bulletins, and advisories that protect the security of their ISs.

(25) Ensure that all cybersecurity personnel receive the necessary technical and security training to carry out their duties and maintain certifications.

(26) Serve as the primary point of contact for cybersecurity-related actions for his or her respective IT systems.

3–11. Program executive officers and direct reporting program/project managers

a. This section applies to program executive officers (PEOs) and PMs to include the PMs that are outside the PEO structure, but are responsible for fielding systems to multiple Army organizations.

b. PEO/PMs duties are as follows:

(1) Acquire, operate, and support systems within their command or activity in accordance with AR 25–2 and its associated DA Pams.

(2) Embed cybersecurity engineering and capabilities in all system research, development, and T&E activities.

(3) Ensure that designated pre-deployed ISSOs effect continuous coordination with the organizational cybersecurity personnel for which the systems are demonstrated, tested, or fielded.

(4) Ensure that the ISO makes the authorization package available to the Army command/Army service component commands and NETCOM 30 days before initial operational T&E and before deployment of the system.

(5) Integrate cybersecurity, communications security, and Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions (TEMPEST) into entire system life cycle design, development, and deployment.

(6) Address and include the addition of any IT/cybersecurity personnel (such as system administrator or network security managers needed to operate the new or expanded system or network) or any additional access requirements and responsibilities for patch management and system administration as part of the development cost of stated system or network.

(7) Integrate cybersecurity practices into pre-milestone A activities and events.

(8) Perform acquisition and life cycle management of materiel in support of the cybersecurity strategy.

(9) Accomplish all intelligence and threat support requirements outlined in AR 381–11 and AR 25–2.

(10) Enforce cybersecurity standards and maintain/report an inventory of IS products, equipment, locations, and contact information.

(11) Enforce information assurance vulnerability management (IAVM) compliance measures as required by ARCYBER as the Army tier II cybersecurity service provider.

3–12. Information system security manager

a. ISSMs act as technical advisors and support the AO and ISO/PM. ISSMs are also in charge of the continuous monitoring of systems within their purview to ensure compliance with cybersecurity policies.

b. The Army identified an operational need to break down the ISSM role into two distinct roles in order to delineate roles and responsibilities within the ISSM functions. The two distinct roles are the P–ISSM and O–ISSM and are described in paragraphs 3–13 and 3–14.

3–13. Program information system security manager

a. The P–ISSM operates at the command level, where the AO resides. P–ISSMs are primarily responsible for maintaining the overall security posture of the systems within their organization and are accountable for the implementation in accordance with DODI 8510.01. The organization's cybersecurity program is developed by P–ISSMs that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.

b. P–ISSM duties are as follows:

(1) Ensure ISO and stewards associated with Army information (received, processed, stored, displayed, and/or transmitted) on each Army IS are appointed in order to establish accountability, access approvals, and special handling requirements.

(2) Function as the primary cybersecurity technical advisor to the AO and managerial lead for RMF throughout the command.

(3) Ensure cybersecurity-related events or configuration changes that may impact Army IS authorizations or security postures are formally reported to the AO and other stakeholders such as information owners (IOs) and stewards, as well as AOs of interconnected DOD ISs.

(4) Ensure the secure configuration and approval of IT below the system level (that is, products, IT services, and PIT) in accordance with applicable guidance prior to acceptance into or connection to an Army IS.

(5) Ensure ISSOs are appointed in writing and provide oversight ensuring established cybersecurity policies and procedures are followed.

(6) Monitor compliance with cybersecurity policies, as appropriate, and review the results of such monitoring.

(7) Ensure cybersecurity inspections, tests, and reviews are synchronized and coordinated with stakeholders.

(8) Ensure implementation of IS security measures and procedures, including reporting incidents to the AO and appropriate reporting chains, while coordinating system-level responses to unauthorized disclosures in accordance with DODI 8500.01.

(9) Ensure the handling of possible or actual data spills of classified sensitive information resident in ISs are conducted in accordance with DODI 8500.01.

(10) Implement, manage, and administer the organization’s structure and workflow within eMASS.

(11) Coordinate with PM/SM, ISO, IO, ISSM, MO, AO, or designated representative for the categorization of all systems within the command’s scope.

(12) Establish and ensure training for all RMF roles throughout the command.

(13) Enforce the use of Army-approved procedures for clearing, purging, reusing, and releasing system memory, media, output, and devices.

(14) Program, manage, execute, and report management decision evaluation packages MS4X and MX5T resource requirements.

(15) Administer a cybersecurity management control evaluation program separate from, or in support of, force protection assessment teams.

(16) Serve as a member of the configuration management board (CMB) or CCB.

(17) In coordination with the DCS, G–3/5/7; DCS, G–2; and CIO/G–6, provide technical and nontechnical information to support a commander’s information operations condition program.

(18) Ensure that program controls are in place to confirm user access requirements.

3–14. Organization information system security manager

a. The O–ISSM operates at the organization level, where the AO does not reside, and performs similar duties to the P–ISSM at all appropriate levels of command, including subordinate commands, posts, installations, and tactical units. The O–ISSM performs duties as needed for those Army activities responsible for project development, deployment, and management of command-acquired software, operating systems, and networks.

b. O–ISSM duties are as follows:

(1) Be appointed by the organizational commander or the director.

(2) Be military or a government civilian when appointed at the major subordinate command, installation, or post level.

(3) Be a U.S. citizen.

(4) Hold a U.S. Government security clearance and access approval commensurate with the level of information processed by the system.

(5) Have and maintain DOD 8570.01–M IAM II or IAM III certification, depending on the scope of responsibilities.

(6) Obtain and maintain cybersecurity training and certification.

(7) Complete the Army Cybersecurity Fundamentals training within six months of appointment.

(8) Complete applicable DOD baseline management certification.

(9) Implement and support the organization’s RMF activities at the respective local level and below (for example, brigade, battalion, or garrison level).

(10) Support the ISO/PM in his or her role to ensure assigned IT capabilities are properly identified, evaluated, configured, and authorized to operate at the approved level of risk.

(11) Assign ISSO’s for IT owned by the organization within the scope of the O–ISSM.

(12) Ensure hardware connected to any system or network has the express written consent of the O–ISSM and the CMB or CCB.

(13) Establish procedures to scan their networks quarterly to identify assets; application, network, and operating system vulnerabilities; configuration errors; and points of unauthorized access.

(14) Be appointed senior O–ISSM for those commands, activities, or organizations with multiple O–ISSMs. In installations with multiple O–ISSMs, the installation O–ISSM is the senior O–ISSM.

3–15. Information system security officer

The ISSO is responsible for ensuring the appropriate operational security posture is maintained for the component DOD IS or PIT system. In addition to the ISSO responsibilities documents in DODI 8510.01, DODI 8500.01, and AR 25–2, the ISSO duties are as follows:

a. Effect continuous coordination with the organizational cybersecurity personnel for which the systems are demonstrated, tested, or fielded.

b. Meet the training and certification requirements of DA Pam 25–2–6 for IAM I, IAM II, or IAM III, if also working as the ISSM for the organization. The category and level depend on the functions performed, per DOD 8570.01–M.

c. Ensure the appropriate organizational operational security posture is maintained for the assigned Army IS.

d. Maintain organizational situational awareness and initiate actions to improve or restore cybersecurity posture of assigned Army IS.

e. Assist the ISSMs in meeting their duties and responsibilities and initiate protective measures for cybersecurity incidents.

f. Implement and enforce assigned Army IS cybersecurity policies and procedures, as defined by cybersecurity-related documentation.

g. Ensure users for Army ISs under the ISSO's purview have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities before being granted access to those systems.

h. In coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered or reported.

i. Ensure Army IS cybersecurity-related documentation is current and accessible to properly authorized individuals.

j. Ensure implementation of IAVM dissemination, reporting, and compliance procedures.

k. Ensure users receive initial and annual cybersecurity awareness training.

l. Prepare, distribute, and maintain plans, instructions, and SOPs concerning system security.

m. Review and evaluate the effects on security of system changes, including interfaces with other ISs and documents all changes.

n. Ensure that all ISs within their area of responsibility have received a current ATO.

Chapter 4
Risk Management Framework

RMF is a disciplined and structured process that combines IS security and risk management activities into the system development life cycle and authorizes their use within DOD. The RMF consists of six steps.

4–1. Six primary steps of the Risk Management Framework process

a. The RMF is a disciplined and structured process that combines IS security and risk management activities into the system development life cycle and authorizes their use within DOD. The RMF consists of six steps:

(1) Categorize a system's security requirements.

(2) Select applicable security controls.

(3) Implement security controls.

(4) Assess security controls.

(5) Authorize a system.

(6) Monitor security controls.

b. The complete workflow a system must go through to obtain an ATO is depicted in figure 4–1. Army specific guidance on performing each of the steps is provided in paragraphs 4–2 through 4–8.

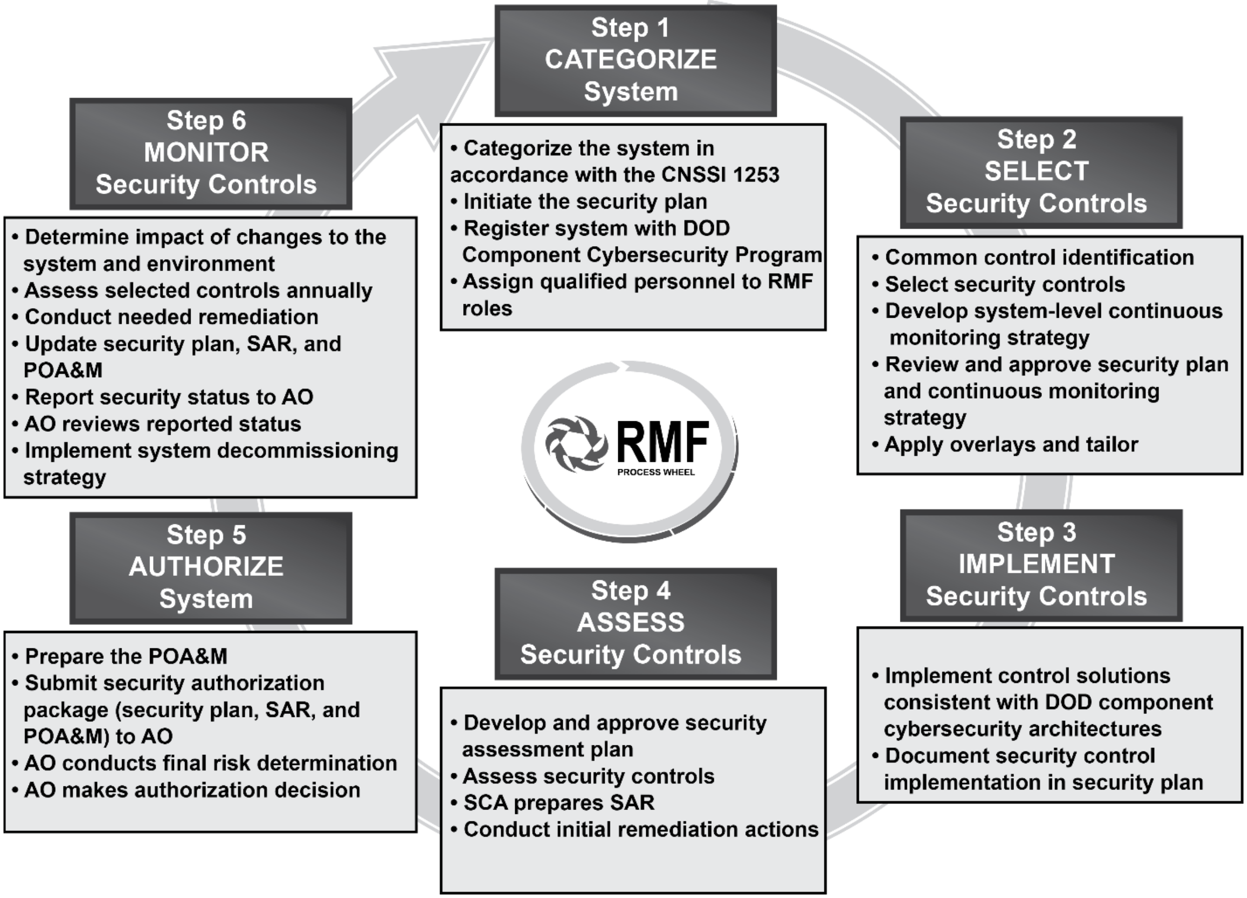

Step 1
CATEGORIZE
System
• Categorize the system in accordance with the CNSSI 1253
• Initiate the security plan
• Register system with DOD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common control identification
• Select security controls
• Develop system-level continuous monitoring strategy
• Review and approve security plan and continuous monitoring strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DOD component cybersecurity architectures
• Document security control implementation in security plan
Step 4
ASSESS
Security Controls
• Develop and approve security assessment plan
• Assess security controls
• SCA prepares SAR
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare the POA&M
• Submit security authorization package (security plan, SAR, and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to the system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR, and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF
PROCESS WHEEL

Figure 4–1. Risk Management Framework six-step process

c. DOD guidance indicates that annual assessments will be performed to maintain a constant and accurate understanding of a system's security posture. DOD is in the process of developing further guidance about the performance of annual assessments in an RMF environment.

d. The RMF is designed to be implemented at each stage of the system development life cycle.

4–2. Step 1: Categorize the information system

a. The first step in the RMF process is to categorize the system in accordance with CNSSI 1253 and document the results in the SP. Categorization of IS and PIT systems is a coordinated effort between the PM/SM, ISO, IO, MOs, ISSM, AO, or their designated representatives. In the categorization process, the IO identifies the potential impact (low, moderate, or high) resulting from loss of CIA if a security breach occurs. Specific guidance on determining the security category for information types and ISs is include in the RMF Knowledge Service.

b. ISOs should consciously document achievements and coordinate with other RMF participants as they build their SP.

c. The security categorization and security control selection of Army IT is a coordinated effort between the PM/SM, ISO, IO, MOs, P–ISSM, O–ISSM and the AO. The ISO/PM/SM, IO, and MOs, with the help of the P–ISSM, categorize Army IT. If necessary, in response to increased risk from changes in threats, vulnerabilities, and variations in risk tolerance based on the sensitivity of information processed on individual systems, the ISSO is permitted to modify recommended categorization levels as appropriate. On behalf of the AO, the AODR can approve the categorization. There are data type surveys that can assist in the CIA determination. In addition, the system owner can select the applicable data types within eMASS and eMASS will recommend CIA levels based on the selected data types.

d. Per DODI 8510.01, all DOD IS and PIT systems must be categorized in accordance with CNSSI 1253 and the corresponding controls from NIST Special Publication 800–53. Controls determined to be not applicable based on the system's categorization or operational environment can be marked "not applicable" in eMASS with compelling artifacts provided to demonstrate why the control is not applicable. A sufficient reason as to why or how the security control is managed must be provided for all remaining security controls that are identified as not applicable.

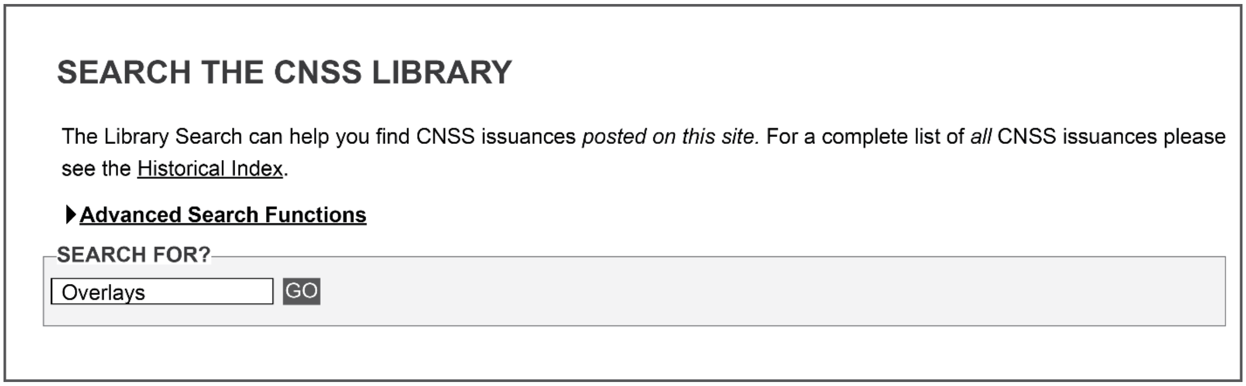
e. Prior to categorization, ensure DD Form 2930 (Privacy Impact Assessment (PIA)) is completed for IT that process and/or store personally identifiable information (PII)/protected health information.

f. DOD designates IS and PIT systems as national security systems (NSS). The high water mark concept described in FIPS PUB 200 does not apply to national security systems. Therefore, per CNSSI 1253, "retaining the discrete impact levels for each of the three security objectives is done to provide a better granularity in allocating security controls to baselines, and should thereby reduce the need for subsequent tailoring of controls."

4–3. Security control overlays

a. Identifying applicable overlays is part of the security categorization process and applied during security control selection. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process that is intended to complement and further refine security control baselines. For example, the controls for classified information are located in the classified information overlay. Protection for the Health Insurance Portability and Accountability Act and PII are located in the privacy overlay.

b. DOD RMF overlays are developed, reviewed, approved, and published in accordance with the DOD RMF Overlay Developmental Guidance. Downloadable copies of the approved and published overlays are located on the CNSS website https://www.cnss.gov/cnss/index.cfm, the official source for NSS overlays. Overlays can be found using the following path https://www.cnss.gov/cnss/searchform.cfm. Once the Library Search opens, enter "Overlays" and select Go to display a list of the current overlays as shown in figure 4–2. Access to the overlays, and guidance regarding how to determine which overlays may apply, are included on the RMF Knowledge Service.



SEARCH THE CNSS LIBRARY

The Library Search can help you find CNSS issuances *posted on this site.* For a complete list of *all* CNSS issuances please see the Historical Index.

Figure 4–2. Committee on National Security Systems library search for overlays

c. ISOs should analyze each overlay document, as well as any forthcoming overlays, and determine if their system meets the definition of any overlay control set. When registering a system in eMASS, ISOs will be prompted to review existing overlay sets to determine applicability to the system being registered. Some controls included in an overlay set may duplicate those already in the baseline set. In such a situation, duplicate controls may be ignored, while unique controls located in the overlay should be automatically added in eMASS.

d. The following information pertains to the tailoring process through which an ISSO identifies all controls that match the system's CIA level; determines which are applicable or not applicable based on system function; applies overlays as appropriate; and identifies common controls.

(1) Tailoring decisions must be aligned with operational considerations and the environment of the IS or PIT system and should be coordinated with MOs and URs. Security controls should be added or marked as not applicable only as a function of specified, risk-based determinations.

(2) Tailoring decisions, including the specific rationale (in other words, mapping to risk tolerance) for those decisions are documented in the SP for the system.

(3) Every selected control must be accounted for either by the organization or the ISO or PM/SM. If a selected control is not implemented, then the rationale for not implementing the controls must be documented in the SP and POA&M.

4–4. Step 2: Select security controls

a. Located on the RMF Knowledge Service website is an automated control selection process that translates CIA values into a baseline control list.

b. DISA has decomposed all discrete tasks within each security control to individual measurable statements. Meaning or intent of the security control is not changed. Controls are simply a breakdown of each requirement within the security control. Each statement is called a control correlation identifier (CCI). CCIs are also used to map to STIGs.

c. NIST Special Publication 800–53 organizes security controls into 19 subject families, indicating the major subject or focus areas to which an individual security control is assigned as shown in figure 4–3. The NIST Special Publication 800–53 also contains a set of privacy controls organized into the following eight subject families:

(1) AP – authority and purpose.

(2) AR – accountability, audit, and risk management.

(3) DI – data quality and integrity.

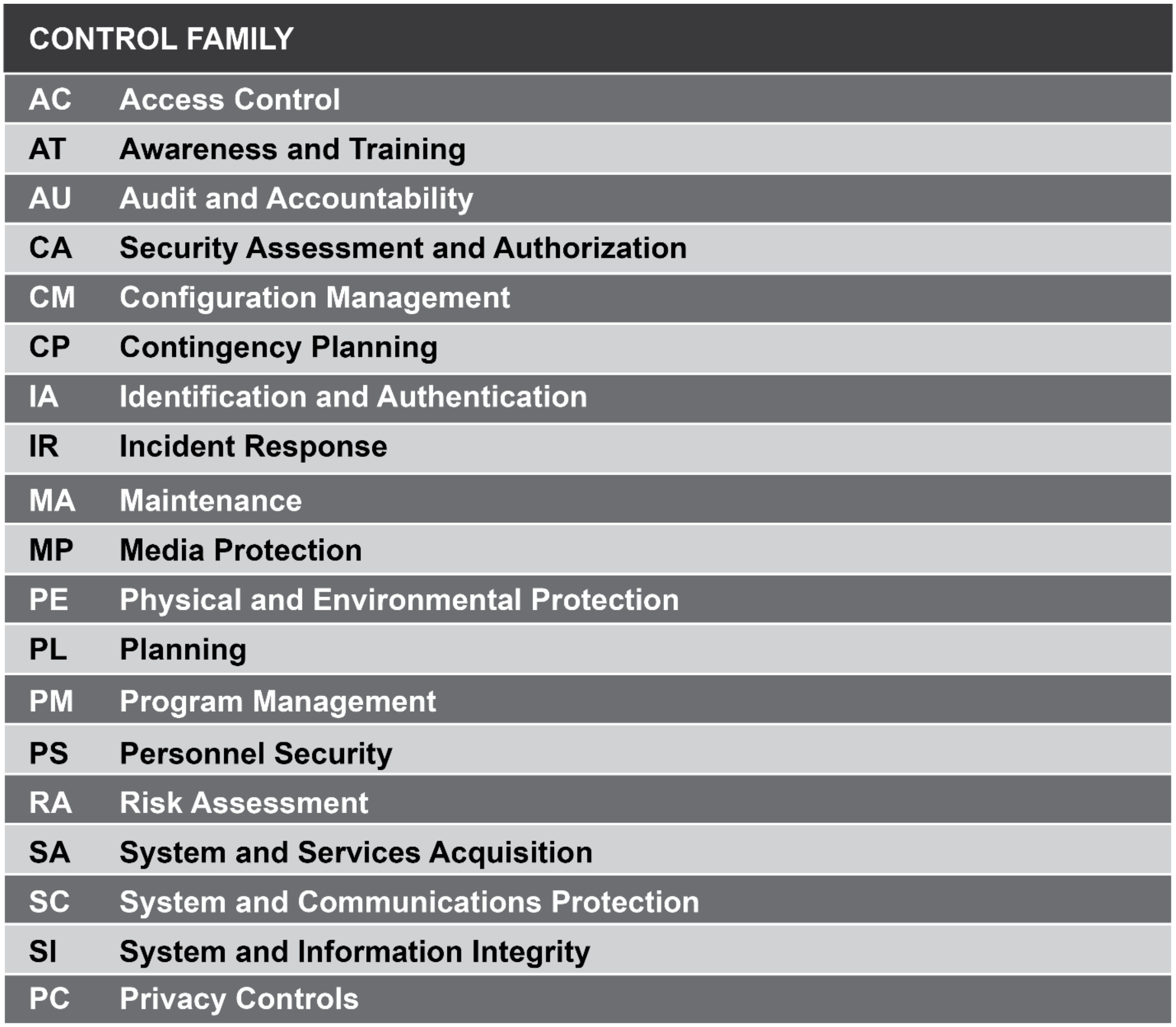
(4) DM – data minimization and retention.

(5) IP – individual participation and redress.

(6) SE – security.

(7) TR – transparency.

(8) UL – use limitation.



CONTROL FAMILY	
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PC	Privacy Controls

Figure 4–3. Security control families

d. Security controls have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into 19 families, as referenced in figure 4–3. Each family contains security controls related to the general security topic of the family. A two-character code uniquely identifies security control families, for example, personnel security. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by ISs/devices.

e. There are three distinct types of designations related to controls that define the scope of applicability for the control; the shared nature of the control; and the responsibility for control development, implementation, assessment, and authorization. These designations include common controls, system-specific controls, and hybrid controls.

(1) Security controls not designated as common controls are considered system-specific or hybrid controls. System-specific controls are the primary responsibility of ISOs and their respective AOs.

(2) Security controls are deemed inheritable by ISs or information system components when the systems or components receive protection from the implemented controls but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components—entities internal or external to the organizations where the systems or components reside.

(3) Organizations assign a hybrid status to security controls when one part of the control is common and another part of the control is system-specific.

f. Common controls can be derived from any of the control families that make up the complete set of RMF controls, however several types may be excellent candidates for common control status. These include controls that require the creation of organization-wide plans and activities, like those detailing incident response processes or providing security awareness training. DODI 8510.01 also highlights organization-wide technical policies, such as a mandate to use PKI security, as examples of common controls.

g. CNSSI 1253 explicitly identifies controls that may be inheritable; not all controls meet that standard, as some will be required for individual systems at all times. The final determination of which controls to implement as common controls varies depending on the organization, mission/business process, or IS and its intended environment/deployment.

4–5. Step 3: Implement security controls

a. The ISO/PM implements the assigned security controls, creating necessary documentation and associated artifacts that support security control implementation.

b. The ISO/PM records the results of the security control implementation as test results associated with the implementation procedures in eMASS. The DOD has created implementation and assessment procedures.

4–6. Step 4: Assess security controls and conduct remediation

In the fourth step, the validation team assesses the security controls using appropriate assessment procedures to determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The ISO/PM creates POA&M vulnerabilities identified, any existing mitigations, and identifies milestones to address all vulnerabilities.

4–7. Step 5: Authorize information system

a. The AO reviews the security authorization package (containing the risk assessment, SAR, and POA&M).

b. The official reviews the package, the AO issues an authorization decision document granting or rejecting the authorization requested and describing the level of risk the organization is accepting by permitting the system’s operation.

4–8. Step 6: Monitor security controls

a. Continuous monitoring begins once an authorization has been granted for operations, and the activities in this plan are performed continuously throughout the life cycle of the IS. Continuous monitoring is a critical part of the RMF. DOD has adopted NIST Special Publication 800–137 for monitoring security controls.

b. Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISs are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an IS or its environment of operation is an essential element of an effective security control monitoring program.

c. The security controls in the IS are monitored continuously. This includes assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. Monitoring actively supports the complementary goals of FISMA compliance and maintains ongoing system security.

d. The following tasks are a breakdown of the RMF monitor security controls per NIST Special Publication 800–37:

(1) Information system and environment changes.
(2) Ongoing security control assessments.
(3) Ongoing remediation actions.
(4) Key updates.
(5) Security status reporting.
(6) Ongoing risk determination and acceptance.
(7) Information system removal and disposal.

4–9. System changes

System changes require a CCB review. A CCB is a group that plays an essential role in an organization's overall cybersecurity strategy. The overall goal of a CCB is to provide a structured process by which changes to an IS are requested and approved, while ensuring the overall cybersecurity posture of the system is maintained and continuing to support the business posture or mission of the organization. Security is an integral part to the CCB process, and members should take every opportunity to address security concerns during every phase of configuration management. The configuration control method focuses on enforcing current operational policies and developing operational guidelines. A CCB should concentrate on two main duties: controlling the baseline and evaluating and approving proposed changes.

4–10. Reauthorization

The ISO initiates a new authorization process via the RMF team prior to the expiration of the existing ATO. Moreover, new overlays may have been developed and new threats may have emerged since the system's initial authorization, further justifying a need to begin the A&A process at RMF step one in the case of a reauthorization (see para 4–2).

4–11. Decommission

The RMF requires organizations to implement an IS decommissioning strategy during the disposal phase of the system development life cycle. Disposal is the process of reusing, transferring, donating, selling destroying, or other disposal of excess surplus property. Decommission information is located on the RMF Knowledge Service at https://rmfks.osd.mil/rmf/rmfimplementation/monitor/pages/decommission.aspx.

4–12. Risk Management Framework security authorization package requirements and contents

a. RMF includes requirements for specific types of compelling evidence (also referred to artifacts) to support an AO's initial and continued operational risk acceptance decision.

b. The security authorization documentation consists of all artifacts developed through RMF activity. Security authorization documentation is maintained throughout a system's life cycle. The security authorization package consists of the SP, SAR, POA&M, and authorization decision document, but are not limited to the components depicted in figure 4–4. It is the minimum information necessary for the acceptance of an IS or PIT system by a receiving organization. Detailed information on the content of the security authorization package is available on the RMF Knowledge Service.

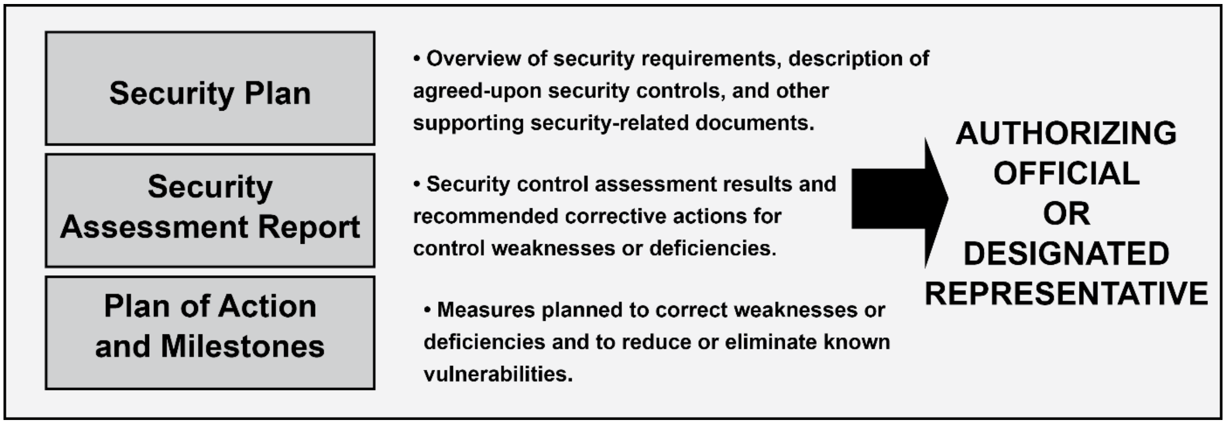

Security Plan
• Overview of security requirements, description of agreed-upon security controls, and other supporting security-related documents.
Security Assessment Report
• Security control assessment results and recommended corrective actions for control weaknesses or deficiencies.
Plan of Action and Milestones
• Measures planned to correct weaknesses or deficiencies and to reduce or eliminate known vulnerabilities.
AUTHORIZING OFFICIAL OR DESIGNATED REPRESENTATIVE

Figure 4–4. Risk Management Framework security authorization package

(1) *Security plan.*

(a) The SP is a formal document that provides an overview of the security requirements for an IS or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) Contains supporting appendixes or, as references, other key security-related documents such as risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

(c) The O–ISSM/ISSO/ISO/common control provider (CCP) are responsible for preparing and submitting the SP. The SP is generated in eMASS.

(2) *Security assessment report.*

(a) The SAR provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.

(b) A SAR is always required before an authorization decision. If a compelling mission or business need requires the rapid introduction of a new IS or PIT system, assessment activity and a SAR are still required. SARs should be updated regularly following the granting of an ATO as site cybersecurity personnel make changes to system security settings. This encourages "near-real-time" risk management, a core tenet of RMF.

(c) The SCA–validator is responsible for preparing the SAR, which is generated in eMASS.

(3) *Plan of action and milestones.*

(a) A POA&M is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The POA&M addresses:

1. Identification of vulnerabilities and impact of noncompliance.
2. All applied mitigations that reduce the overall residual risk for an identified vulnerability.
3. Specific corrective actions for previously identified vulnerabilities that are now compliant.
4. The agreed upon timeline for completing and validating corrective actions.
5. The resources necessary and available to properly complete the corrective actions.
6. Requests for AO risk acceptance for vulnerabilities due to operational or resource requirements.

(b) POA&M items are closely monitored to justify a system authorization and to maintain a valid authorization, as some authorizations are granted under the condition that POA&M items will be addressed by a specified point in time. The ISO/PM/SM/ISSO are responsible for implementing the corrective actions identified in the POA&M and providing visibility and status to the AO.

(c) The O–ISSM/ISSO is responsible for preparing the POA&M, which is generated in eMASS.

(4) *Authorization decision document.*

(a) An authorization decision document is the official management decision given by a senior organizational official to authorize operation of an IS and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls. The document contains the following information:

1. Authorization decision (approval or denial of the requested authorization).
2. Terms and conditions for the authorization, if any.
3. Authorization termination date (ATD).

(b) The security authorization decision indicates to the ISO/O–ISSM whether the system is—

1. Authorized to operate (ATO).
2. Authorized to operate with conditions.
3. Authorized to test.
4. Not authorized to operate.

(c) The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the IS or inherited controls that must be followed by the system owner or CCP.

(d) The ATD, established by the AO, indicates when the security authorization expires. ATDs are written to expire within a 3-year period. OMB A–130 objectives are to move to the ongoing authorization concept, but robust continuous monitoring is necessary to achieve this objective. Until such time as the DOD CIO determines the DOD ISCM program is mature and robust enough to support ongoing authorization, DOD and the Army will continue to require a 3 year authorization.

(5) *Risk Assessment Report.* The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.

4–13. Tools that support the Army Risk Management Framework process

The following tools and systems, many of them web-based and accessible only with a valid common access card (CAC), are crucial to performing the activities that comprise the RMF process. There are several tools available to help with the implementation of the RMF; they include, but are not limited to:

a. The Risk Management Factor Knowledge Service. This is DOD's official site for overarching RMF policy and implementation guidelines. The U.S. Army component workspace on the RMF Knowledge Service contains Army RMF pertinent information for the dissemination and sharing of Army specific RMF information, located at https://rmfks.osd.mil.

(1) The security controls explorer can be accessed at https://rmfks.osd.mil/rmf/general/securitycontrols/pages/controlsexplorer.aspx.

(2) The RMF Knowledge Service provides a mapping spreadsheet that correlates DIACAP and RMF controls. The RMF Knowledge Service link is https://rmfks.osd.mil/rmf/general/securitycontrols/pages/comparisonof85002and800-53.aspx.

b. Enterprise Mission Assurance Support Service. eMASS is the tool for the implementation and management of the RMF process. NETCOM manages the Army instances of eMASS. The Army NIPRNET eMASS instance is located at https://emass-army.csd.disa.mil. The Army SIPRNET eMASS instance is located at https://emass-army.csd.disa.smil.mil.

(1) eMASS is designed to allow members of the Army community to track authorization of their component systems and provide the status of their system vulnerabilities to controlling authorities. The application allows users to enter system information and track the progress of cybersecurity activities including execution of assessment procedures, compliance

statuses, attachments, progress of the POA&M, authorization process decisions, and associated action plans for the purpose of sharing system security information and compliance status.

(2) eMASS is an ongoing DOD effort to automate a broad range of services for comprehensive, fully integrated cybersecurity management for DOD components. eMASS facilitates robust, measurable cybersecurity program management through the following capabilities:

(a) Security-process management and reporting based on compliance with security controls.

(b) Standardized information exchange to facilitate dynamic connection decisions.

(c) Workflow automation.

(d) Simplified management of the entire authorization process from security authorization package submission through completion.

(e) Traceable systems security engineering across the entire system development life cycle.

(f) Facilitation of regulatory and cybersecurity management-reporting requirements, such as those contained in FISMA of 2014.

(3) Access to Army NIPRNET eMASS, at https://emass-army.csd.disa.mil, requires a user to have an eMASS account, connection via a .mil domain and CAC with current DOD PKI certificates.

(4) A significant amount of information about a system must be compiled before it can be registered in eMASS. This includes knowledge of RMF controls that apply to the system. The following data is needed to complete registration:

(a) Basic system information, such as system version.

(b) Ports, protocols, and service.

(c) Encryption requirements.

(d) Locations.

(e) Authorization information (if a system has previously been authorized).

(f) FISMA mandates associated with the system.

(g) Business function details, such as mission criticality.

(h) External security services, if any are in use.

(i) Categorized CIA values, which will be used to derive a baseline control set, apply overlays, and tailor controls.

(j) A listing of common controls that may be inherited.

(k) An assignment of roles and responsibilities within eMASS.

4–14. Reciprocity

a. Documentation regarding the security posture of DOD IS and PIT systems will be made available to promote reciprocity as described in DODI 8510.01 and to assist AOs from other organizations in making credible, risk-based decisions regarding the acceptance and use of systems and the information that they process, store, or transmit.

b. Reciprocity is defined as the mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IS resources and/or to accept each other's assessed security posture in order to share information. Cybersecurity reciprocity is essential in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DOD Information Enterprise. Reuse reduces the requirement for redundant testing, assessment, documentation, and the associated costs in time and resources. Reciprocity is ultimately about trust that the required process was followed to support an authorization decision by the deploying organization prior to providing to any other organization under reciprocity.

c. To facilitate reciprocity, the following concepts are fundamental to a common understanding and must be adhered to:

(1) The DOD RMF presumes acceptance of existing test and assessment results and authorization documentation.

(2) Under the RMF there is only a single valid authorization for an IS. Multiple authorizations indicate multiple systems under separate ownership and configuration control.

(3) Deploying systems with valid authorizations (from a DOD organization or other federal agency) are intended to be accepted into receiving organizations without adversely affecting the authorizations of either the deployed system or the receiving enclave or site (that is, the system accepted under reciprocity should do no harm to the receiving organization, its systems, its people, and/or its mission).

(4) When Army is the deploying agency, the Army ISO must complete the RMF process and provide the results in eMASS to the receiving organization.

(5) When Army is the receiving organization, the appointed AO determines the acceptability of the impact for Army use.

d. If acceptable, the AO must document acceptance of the capability. A mutual agreement memorandum of understanding (MOU), memorandum of agreement (MOA), or SLA will be signed by the Army and the deploying agency. The

MOA/MOU/SLA must include, but is not limited to, agreement of responsibilities for the maintenance and monitoring of the security posture of the system.

e. If the risk is not acceptable, the AO will document their refusal to accept the IS with justification and provide the refusal to the deploying organizations.

Chapter 5
Special Considerations

5–1. Tenant enclave standards

The term tenant in this paragraph refers to an organization that is physically located on the installation, or virtually or logically connected to the installation campus area network (ICAN), also known as the backbone. A tenant enclave refers to the tenant's collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. This paragraph specifically focuses on tenant enclaves that receive their services from the ICAN.

a. A tenant enclave is not required to obtain an individual AO authorization when it meets the standards of connectivity provided by the ICAN service provider and the following are implemented:

(1) The tenant enclave is required to provide proof of meeting the security standards in order to receive and maintain connectivity to the ICAN in a tenant security plan (TSP).

(2) The tenant enclave provides the required information/documentation to the network enterprise center (NEC)/service provider for use as artifacts in the ICAN installation authorization.

(3) The NEC/service provider accepts the tenant enclave submission as sufficient and provides a tenant in good standing memorandum to the tenant enclave owner.

(4) The installation ICAN authorization package is updated to include the list of tenants.

(5) The NEC/service provider includes the accepted tenant enclave information/documentation as an artifact to the installation ICAN authorization.

b. The NEC/service provider is required to scan all tenant enclave organizations.

(1) The tenant ensures that the NEC/service provider has physical and electronic access and permissions necessary to allow compliance verification and security scans of all networked devices to determine that cybersecurity, computer network defense, and Defense-in-Depth program configurations and countermeasures are in place.

(2) Tenant enclaves that are subject to being deployed will conduct their own vulnerability scanning to remain proficient in the vulnerability assessment tools and methodology so as to conduct the scans in the deployed area of operations.

(3) The NEC may direct the frequency of vulnerability and STIG scans and the unit/organization will provide all scan results to the NEC when completed.

c. TSPs are not applicable to DOD IS, SISs, and CRNs.

5–2. Stand-alone information systems/closed restricted network

a. SISs or CRNs have no external connectivity and do not have the ability to access the network infrastructure (for example, Defense Research and Engineering Network (DREN), Department of Defense Information Network (DODIN), and the internet) or services (for example, web services, domain name server, and enterprise email). They are not externally connected to live operational networks such as the DREN, NIPRNET, SIPRNET, tactical networks, or other government or commercial networks. They may host multiple connected systems to include servers and workstations that are not interconnected to any other network or system and do not transmit, receive, route, or interchange information outside the network such as a classroom topography or network training facility. SIS and CRN, as outlined in ARCYBER/NETCOM's TTP, may be configured to process any information type but must be categorized like any other Army IS in accordance with Army, DOD, and NIST guidance. This includes applying all applicable security overlays such as Classified, National Security, or PII. SIS are identified by Type I (no media), Type II (with media), and Type III (stand-alone network) and are all physically separate from all other networks. Type IV are cryptographically isolated CRN. As SIS and CRN do not directly interact with the DODIN and/or other Army controlled networks, the Army component level role in the A&A process is significantly reduced. SIS and CRN must utilize eMASS for recording and execute. A&A process for SIS and CRN follows the same general steps as that of a normal Army system. However, the personnel assigned to the RMF control approval and package approval roles within the A&A process for SIS and CRN are different and the process can be done at a lower organizational level, making the process entirely internal to the organization for which the system and its AO belong.

b. The SCA–organization is responsible for performing all activities reserved for the SCA. For details, please refer to the tailored set of security controls following the RMF A&A process as documented in the ARCYBER/NETCOM

SIS/CRN A&A Authorization Operational TTP located on the RMF Knowledge Service under the Army workspace, NETCOM operations page.

Note. A third-party validation is not required unless requested by the AO.

5–3. Control systems

Control systems are a combination of control components (for example, electrical, mechanical, hydraulic or pneumatic, and so forth), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (for example, transport of matter or energy, maintain a secure and comfortable work environment, and so forth). Industrial control systems (ICSs) are automated control systems that act upon industrial systems and processes. ICS is used as a general term that encompasses several, but not all, types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems, such as the programmable logic controllers (PLCs) often found in the industrial sector and critical infrastructure. However, since most uses of the term ICS do not pertain to industrial systems or processes, the term control system is used herein for this general category of IT.

a. Throughout industry, and informally within DOD, the term operational technology (OT) is used to differentiate control systems from traditional ISs. Other emerging terms related to control systems include hybrid/converged systems, cyber physical systems, the internet of things, and the industrial internet of things. In any future publications or correspondence, any equipment designated as OT will be treated as DOD IT for the purposes of cybersecurity requirements.

b. Control systems have many aspects inherent to their nature that often prevent the use of standard IT security mechanisms and techniques. Aspects of control systems such as the impact of real time operating systems, extremely long life cycle replacement timelines, and limited patching opportunity require special considerations when applying security controls to control systems.

c. With the publication of DODI 8510.01, DODI 8530.01, and in consideration of Executive Order 13636, DOD control systems are DOD IT and will control cybersecurity risk through the implementation of RMF.

d. The Office of the Secretary of Defense (OSD) for Energy, Installations, and Environment (EI&E) has produced guidance to assist control system owners with step one based on the function of the control system (see para 4–2).

(1) OSD EI&E control system guidance can be found on the RMF Knowledge Service.

(2) The ISO of Army control systems use the OSD EI&E control system guidance for system categorization.

(3) Deviations from OSD EI&E recommended system categorization are approved by the AO. ISO for Army control systems will provide adequate rationale for all deviations in the SP.

e. NIST Special Publication 800–82 provides general guidance on securing control systems. This guidance includes recommended security control baselines for control systems. OSD EI&E has utilized these baselines to provide control selection guidance based on the previously established control system categorization guidance.

(1) OSD EI&E control system guidance can be found on the RMF Knowledge Service.

(2) The ISO of Army control systems use the security control baselines established by OSD EI&E.

(3) The ISO of Army control systems provide rationale for additional security control tailoring in the SP. The AO approves all further control tailoring.

(4) The SCA–Army, as delegated to implement the RMF, publishes procedural control tailoring guidance for control systems that also meet the definition of SISs or CRNs. This guidance will be approved by the SISO.

f. Any OT not rising to the level of a system and defined as IT product, IT service, or platform IT as defined in DODI 8510.01 will be processed using the assess only process previously defined when fielded into an authorized boundary.

g. While many security controls from the NIST and CNSSI security control baselines can be applied to an ICS, how and where they are implemented can vary due to technical and operational constraints. Interconnections between ICSs and organizational network and business systems expose ICSs to exploits and vulnerabilities, and any attempt to address them must be tailored to meet ICS constraints and requirements. Figure 5–1 provides a schematic architecture of ICS levels that follows the American National Standards Institute/International Society of Automation (ISA) process, augmented to include additional components/layers not shown in the ISA architecture.

h. This pamphlet does not supersede any existing standards or regulations outside of the Army that may apply to Army control systems. Examples include the North American Electric Reliability Corporation critical infrastructure protection standards, Department of Transportation Federal Motor Vehicle Safety Standards and Regulations, and the Office of the National Coordinator for Health Information Technology Health IT Certification Program.

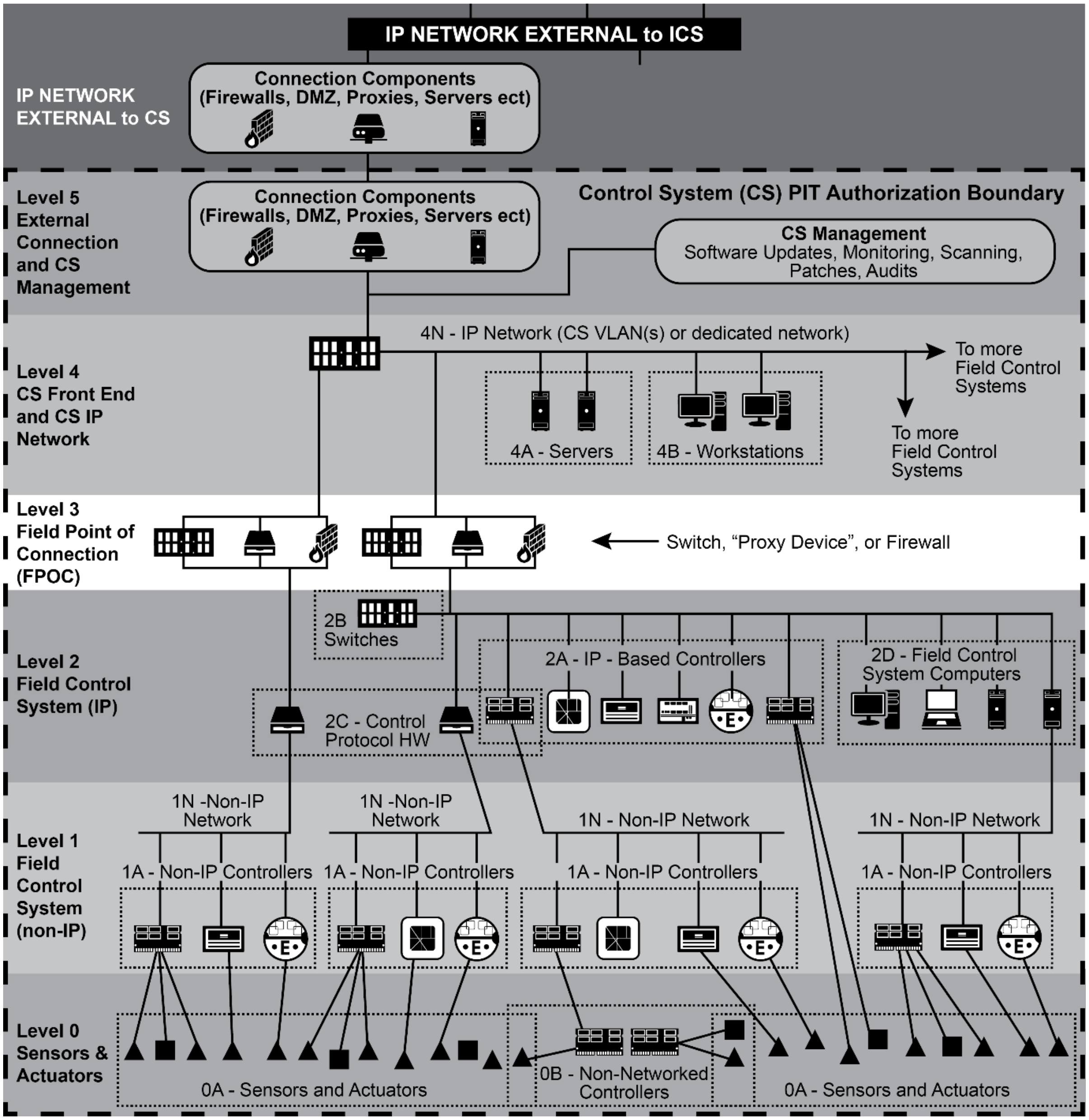

IP NETWORK EXTERNAL to ICS
IP NETWORK EXTERNAL to CS
Connection Components (Firewalls, DMZ, Proxies, Servers ect)
Level 5 External Connection and CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers ect)
Control System (CS) PIT Authorization Boundary
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
4N - IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
Switch, “Proxy Device”, or Firewall
Level 2 Field Control System (IP)
2B Switches
2A - IP - Based Controllers
2D - Field Control System Computers
2C - Control Protocol HW
E
Level 1 Field Control System (non-IP)
1N -Non-IP Network
1N -Non-IP Network
1N - Non-IP Network
1N - Non-IP Network
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
1A - Non-IP Controllers
E
Level 0 Sensors & Actuators
0A - Sensors and Actuators
0B - Non-Networked Controllers
0A - Sensors and Actuators

Figure 5–1. Five-level control systems reference architecture

5–4. Information systems that impact financial reporting

a. The National Defense Authorization Act for Fiscal Year 2010 requires DOD to validate that its financial statements are audit-ready not later than 30 September 2017. The OSD determined that focused attention needs to be placed on additional practices and security controls over ISs that impact financial reporting.

b. The Financial Improvement and Audit Readiness (FIAR) requirements were separately managed with a separate process for authorization. Subsequent to the publication of DODI 8510.01 it was determined that there was duplication between the FIAR requirements and the RMF requirements.

c. To allow for concurrent A&A to meet the duplicative requirements, the DOD CIO and the OSD Comptroller issued OSD Memorandum dated 21 April 2016 (available at http://ciog6.army.mil/policylegislation/tabid/64/default.aspx) that integrates the requirements to the greatest extent possible.

d. The memorandum provides instructions to assist those completing the system A&A process (for systems that impact internal controls over financial reporting) to concurrently address controls that impact the financial statement audit readiness of these systems.

e. The framework includes the following:

(1) Summary of FIAR guidance requirements relating to the system and associated infrastructure components to be included in the scope of the assessment, defining control objectives, documentation of controls, testing of controls, and evaluation of results.

(2) A detailed mapping of Federal Information System Controls Audit Manual control techniques to NIST Special Publication 800–53.

(3) A list of the applicable NIST Special Publication 800–53 security controls to assist in the identification of common audit readiness and A&A requirements.

5–5. Special access program/sensitive activity

Army special access program/sensitive activity (SAP/SA) specific security authorization guidance is found in the Army SAP/SA Special Programs Office (SPO) Risk Management Framework Transition Guide issued by the SAP/SA senior AO. Guidance on the determination of cybersecurity requirements/controls required for security authorization of SAP/SA IS is based on the CIA impact levels and the security control requirements as defined in the Joint Security Assessment Plan Implementation Guide, as well as the Army specific requirements addressed in this pamphlet.

a. The SCA function is performed upon SAP/SA senior AO tasking by PEO Enterprise Information Systems (EIS) Defense Communications Army Transmissions Systems (DCATS), Technology Applications Office (TAO). The PEO EIS DCATS TAO maintains a staff of SCAs to support the assessor functions and report the results of assessment testing in a SAR to the Army SAP/SA senior AO together with the recommendation in support of an ATO decision.

b. The senior AO for Army SAP/SA resides in the CIO/G–6 SAP/SA SPO.

5–6. Sensitive compartmented information

RMF A&A guidance is found in DCS, G–2 sensitive compartmented information (SCI) policies. Requirements are defined in the ICD 503 and the DOD Joint Special Access Program (SAP) Implementation Guide (JSIG) (available at http://www.dss.mil/rmf.)

a. Authority for SCI certification is vested in the DCS, G–2 Information Assurance Division Chief, who is the single final authority for all SCA recommendations regarding Army SCI programs.

b. The DCS, G–2 appoints the AO for SCI ISs. The authority for granting operating approval may be delegated by the AO as necessary to the designated approving authorities within the DCS, G–2 Cybersecurity Division.

c. In those cases where there are differences between the requirements of this DA Pam and the ICD 503 manual due to the specific restrictions of the Army SCI environment, the cybersecurity requirements and controls of the ICD 503 take precedence.

Chapter 6
Assess Only

This chapter describes the assess only construct with an overview of RMF policy, unique terms, roles and duties, and documentation requirements to assist the Army workforce that has anything to do with IT. With mission assurance utmost in mind, this chapter is intended to provide an AO and staff with an approach to remediate or mitigate risks that may impact organizational operations, assets, individuals, other organizations, or the Nation as posed by Army IT vulnerabilities. Risks associated with vulnerabilities inherent in IT, global sourcing and distribution, and adversary threats to Army use of cyberspace must be considered in Army employment of capabilities to achieve objectives in military, intelligence, and business operations.

6–1. Implementation requirements

a. RMF introduced the concept that all IT do not rise to the level of an IS or PIT system, but receive, process, store, display, or transmit DOD information. DODI 8510.01 identifies these types of IT as IT below the system level and require the IT to be securely configured and reviewed by the cognizant ISSM and SCA prior to being accepted and connected into an authorized computing environment (in other words, an IS or PIT system operating under an ATO). The cybersecurity requirements for Army IT will be managed through RMF in accordance with the principals established in DODI 8510.01.

b. IT products, services, and PIT do not require authorization for operation through the process required for A&A. These types of IT must be securely configured in accordance with applicable DOD policies and will be configured in accordance with applicable STIGs. When a STIG is not available, an applicable security requirements guide may be used (available at https://iase.disa.mil/stigs/agct/pages/index.aspx). All IT products, services, and PIT do not have named STIGs; therefore, implement assess only. Some IT will need a customized assessment based on their functional capabilities, their operational environment, data flows, and developmental environment. The ISO/PM ensures qualified individuals are identified who have the knowledge, skills, and abilities necessary to evaluate the IT.

Note. A third-party validation is not required.

6–2. Terms

In order to distinguish between the concepts of “assess and authorize” and “assess only,” and to highlight the uniqueness between the two models, the following terms are used:

a. Assessment. The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an IS. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Assessment is synonymous with risk analysis. Source NIST Special Publication 800–39.

b. Information technology product. IT products (including applications) will be configured in accordance with applicable STIGs. This review ensures products will not introduce vulnerabilities into the hosting IS and PIT system. See the RMF Knowledge Service for additional guidance on the review of products. Unified capability products will receive unified capability certification for cybersecurity in accordance with DODI 8100.04.

c. Information technology service. An IT service consists of IT capabilities outside the service user organization’s authorization boundary, and the service user’s organization has no direct control over the application or assessment of required security controls. Army organizations that use IT services are typically not responsible for authorizing them (in other words, not responsible to issue an authorization decision). IT services are provided according to a formal agreement between Army entities or between Army and an entity external to Army. Capabilities may include, for example, information processing, storage, or transmission.

(1) *External.* Army organizations that use external IT services provided by a non-DOD Federal Government entity must ensure the security protections provided by the external service is sufficient for the Army organization’s operational mission, and the service is operating under a current endorsement, approval, or authorization from the providing agency. Army organizations that use external IT services provided by a commercial or other non-Federal Government entity must ensure the security protections provided by the external service are sufficient for the Army organization’s operational mission. Interagency agreements or government statements of work for these external services must contain requirements for SLAs that include the application of appropriate security protection requirements. Army organizations contracting for external IT services in the form of commercial cloud computing services must comply with Army cloud computing policy and procedural guidance as published.

(2) *Internal.* Internal IT services are delivered by Army IT. Army organizations that use internal IT services must ensure the security protections provided by the internal service are sufficient for the Army organization’s operational mission, and written agreements describing at a minimum the roles and responsibilities of both the providing and the receiving organization are in place.

d. Platform information technology. PIT has a single purpose, that is, to support the operations of the platform on which it resides. If removed from the platform, it has no function or purpose. When PIT is part of a program of record, the RMF requirements are applicable to the PIT included on the platform. Examples of platforms that may include PIT are weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health ITs, vehicles and alternative fueled vehicles (for example, electric, bio-fuel, liquid natural gas) that contain car computers, buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, and so forth), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices, and advanced metering or sub-metering and their associated data transport mechanisms (for example, data links and dedicated networks).

6–3. Platform information technology

Owners of special purpose systems (in other words, platforms) who, in consultation with an AO, determine that a collection of PIT rises to the level of a PIT system is required to perform a full RMF A&A. PIT systems must be designated as such by responsible Army component heads or their delegates (ISO, PEO/PM, O–ISSM, P–ISSM, and AODR) and authorized by an AO specifically appointed to authorize PIT systems.

6–4. Assess only construct

a. The SCA–Army develops and documents the guidance for determination if the capability is DOD IT. If determined DOD IT, the IT type determination wizard is located on the RMF Knowledge Service to help determine if the capability qualifies for assess only. The responsibility for determining eligibility and ensuring all products, services, and PIT have completed the appropriate evaluation and configuration processes prior to acceptance and connection into an authorized computing environment or connection to an IS or PIT system lies with the ISO, ISSO, O–ISSM, and P–ISSM with the review and approval of the responsible AO.

b. The assess only construct was developed to characterize the different types of capabilities and their requirements as shown in figure 6–1. The construct comprises two scenarios:

(1) Scenario I: Assessed—not included in an existing boundary.

(2) Scenario II: Assessed—included in an existing boundary.

c. Within each scenario the process of evaluation may differ. The construct will be used by Army organizations as the framework for the assess only requirement of the RMF.

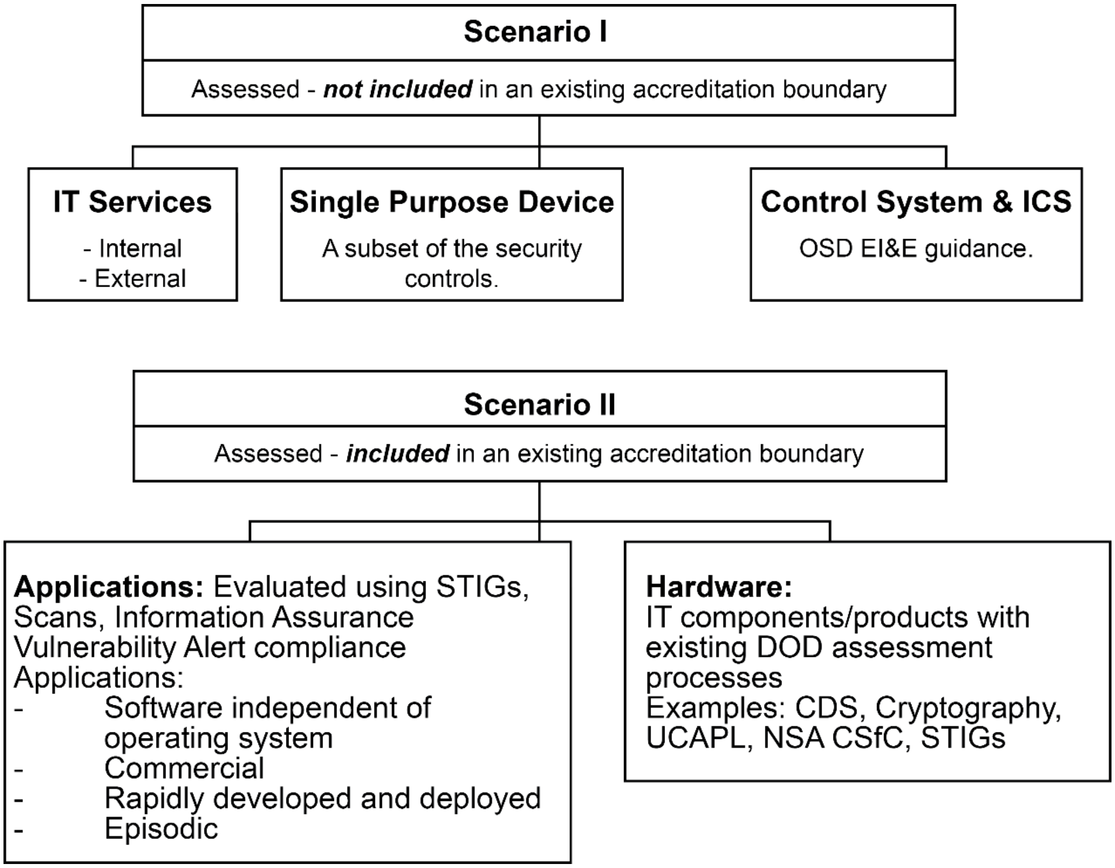

Scenario I
Assessed - not included in an existing accreditation boundary
IT Services
- Internal
- External
Single Purpose Device
A subset of the security controls.
Control System & ICS
OSD EI&E guidance.
Scenario II
Assessed - included in an existing accreditation boundary
Applications: Evaluated using STIGs, Scans, Information Assurance Vulnerability Alert compliance
Applications:
- Software independent of operating system
- Commercial
- Rapidly developed and deployed
- Episodic
Hardware:
IT components/products with existing DOD assessment processes
Examples: CDS, Cryptography, UCAPL, NSA CSfC, STIGs

Figure 6–1. Assess only construct

6–5. Scenario I: Assessed—not included in an existing accredited boundary

Scenario I is applicable to IT that is not or will not be included or incorporated or integrated into an existing authorization boundary. The P–ISSM and/or the SCA–organization evaluate and endorse the IT prior to its use. Scenario I applies to the following IT:

a. Single purpose devices. Examples of single purpose devices include PIT or products with embedded IT that perform a singular function and require minimal or no configuration. The P–ISSM and/or the SCA–organization evaluate this type of IT for use in a specific operational environment, but can be used across a range of similar operational environments based on the initial evaluation (for example, training simulators, diagnostic test and maintenance equipment, medical devices, and so forth).

b. Information technology services. Refer to paragraph 6–2*c* for a discussion of IT services.

6–6. Scenario I: Requirements

The SCA–Army develops and documents the procedures in a TTP and posts them on the RMF Knowledge Service. The P–ISSM and/or SCA–organization are responsible for performing a risk assessment of the IT and determine the risk level (likelihood of exploit and impact). If the risk is low or very low, the P–ISSM is authorized to approve its use. The IT owner provides the compelling artifacts and the approval is available in eMASS for reuse by others. If the risk is moderate, high, or very high, the P–ISSM submits the risk assessment results and a risk acceptance recommendation to the IT AO for a determination on additional actions or approvals. The IT AO makes a risk acceptance determination and coordinates with the CIO/G–6 prior to finalization of the risk acceptance decision. If the risk is not acceptable, the AO documents the decision and rejects the new IT in the current authorization boundary. The decision is documented in eMASS.

6–7. Scenario II: Assessed—included in an existing accredited boundary

Scenario II is applicable to IT that will be assessed and connected into an existing authorization boundary. Scenario II applies to the following IT situations:

a. IT that has been through a specific policy process, evaluation, and/or assessment and become part of an existing authorization boundary baseline.

b. IT that has been through a specific policy process, evaluation, and/or assessment and connected in an existing authorization boundary but maintains IT independence and does not become part of an existing authorization baseline. IT is identified as:

(1) Applications. Software independent of an operating system, integrated into a currently authorized IS. Applications can be commercial off-the-shelf, government off-the-shelf, mobile applications, or open source software. Examples include IT associated with rapid response initiatives that do not rise to the level of an IS and IT used in an episodic nature that do not raise to the level of an IS.

(2) Hardware that has been through an existing DOD assessment policy process, for example, cross domain solutions (CDS), cryptography, capabilities evaluated prior to being added to the Unified Capabilities Approved Product List (UCAPL) or the National Security Agency Commercial Solutions for Classified (NSA CSfC) Program. Evaluated IT can be incorporated into a current authorization per the conditions of the assessment.

c. No additional evaluation/authorization is required.

6–8. Scenario II: Requirements

The SCA–Army develops and documents the procedures in a TTP and posts them on the RMF Knowledge Service. The P–ISSM and/or SCA–organization are responsible for performing a risk assessment of the IT and determine the risk level (likelihood of exploit and impact). If the risk is low or very low, the P–ISSM, with agreement from the AO, approves the connection. The IT owner provides the compelling artifacts and the connection decision is made available in eMASS for reuse by others. If the risk is moderate, high, or very high, the P–ISSM submits the risk assessment results and a risk acceptance recommendation to the IT AO for a determination on additional actions or approvals. The IT AO makes a risk acceptance determination and coordinates with the CIO/G–6 prior to finalization of the risk acceptance decision. If the risk is not acceptable, the AO documents the decision and rejects the new IT in the current authorization boundary. The decision is documented in eMASS.

Appendix A

References

Section I

Required Publications

AR 25–2
Army Cybersecurity (Cited on title page.)

DODI 8500.01
Cybersecurity (Cited on title page.) (Available at http://www.esd.whs.mil/dd.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited on title page.) (Available at http://www.esd.whs.mil/dd.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (https://armypubs.army.mil). DOD publications are available at http://www.esd.whs.mil/dd.

AR 25–1
Army Information Technology

AR 25–30
Army Publishing Program

AR 380–381
Special Access Programs (SAPS) and Sensitive Activities

AR 381–11
Intelligence Support to Capability Development

Army CIO/G–6 Memorandum dated 26 January 2016
Update to the Department of the Army Strategy for the Implementation of the Risk Management Framework (RMF) for Department of Defense Information Technology (IT) (Available at http://ciog6.army.mil/policylegislation/tabid/64/default.aspx.)

CNSSI 1253
Security Categorization and Control Selection for National Security Systems (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSI 4009
Committee on National Security Systems (CNSS) Glossary (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

DA Pam 25–2–6
Cybersecurity Training and Certification Program

DA Pam 25–2–12
Authorizing Official

DOD Cybersecurity Policy Chart
(Available at http://iac.dtic.mil/csiac/ia_policychart.html.)

DOD Program Manager's Guidebook for Integrating Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle
(Available at https://www.dau.mil/tools/t/dod-program-manager-guidebook-for-integrating-the-cybersecurity-risk-management-framework-(RMF)-into-the-System-Acquisition-Lifecycle.)

DOD Special Access Program (SAP) Program Manager's (PM) Handbook to the Joint Special Access Program (SAP) Implementation Guide (JSIG) and the Risk Management Framework (RMF)
(Available at https://www.dss.mil/documents/isp/dod_sap_pm_handbook_jsig_rmf_2015aug11.pdf.)

DOD 8570.01–M
Information Assurance Workforce Improvement Program

DODD 5144.02
DOD Chief Information Officer (DOD CIO)

DODD 8115.01
Information Technology Portfolio Management

DODD 8140.01
Cyberspace Workforce Management

DODI 5000.02
Operation of the Defense Acquisition System

DODI 5000.75
Business Systems Requirements and Acquisition

DODI 5025.01
DOD Issuances Program

DODI 5200.02
DOD Personnel Security Program (PSP)

DODI 5400.16
DOD Privacy Impact Assessment (PIA) Guidance

DODI 8100.04
DOD Unified Capabilities (UC)

DODI 8320.02
Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations

DODI 8582.01
Security of Unclassified DOD Information on Non-DOD Information Systems

DODM 5200.02
Procedures for the DOD Personnel Security Program (PSP)

Executive Order 13636
Improving Critical Infrastructure Cybersecurity (Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.)

Financial Improvement and Audit Readiness (FIAR) Guidance
(Available at http://comptroller.defense.gov/portals/45/documents/fiar/fiar_guidance.pdf.)

FIPS PUB 199
Standards for Security Categorization of Federal Information and Information Systems (Available at http://csrc.nist.gov/publications/fips/fips199/fips-pub-199-final.pdf.)

FIPS PUB 200
Minimum Security Requirements for Federal Information and Information Systems (Available at http://csrc.nist.gov/publications/fips/fips200/fips-200-final-march.pdf.)

FISMA of 2014
(Available at https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.)

Health Insurance Portability and Accountability Act of 1996
(Available at https://www.gpo.gov/fdsys/pkg/plaw-104publ191/content-detail.html.)

ICD 503
Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation (Available at https://www.dni.gov/files/documents/icd/icd503.pdf.)

Joint Security Assessment Plan Implementation Guide
(Available at http://www.dss.mil/documents/isp/jsig_2016april11_final_(53Rev4).pdf.)

National Defense Authorization Act for Fiscal Year 2010
(Available at https://www.gpo.gov/fdsys/pkg/plaw-111publ84/pdf/plaw-111publ84.pdf.)

NIST Special Publication 800–30, Revision 1
Guide for Conducting Risk Assessments (Available at http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.)

NIST Special Publication 800–34, Revision 1
Contingency Planning Guide for Federal Information Systems (Available at http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf.)

NIST Special Publication 800–37, Revision 1
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Available at http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf.)

NIST Special Publication 800–39
Managing Information Security Risk: Organization, Mission, and Information System View (Available at http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf.)

NIST Special Publication 800–53, Revision 4
Security and Privacy Controls for Federal Information Systems and Organizations (Available at http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.)

NIST Special Publication 800–53A, Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (Available at http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53ar4.pdf.)

NIST Special Publication 800–60, Volume 1, Revision 1
Guide for Mapping Types of Information and Information Systems to Security Categories (Available at http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v1r1.pdf.)

NIST Special Publication 800–60, Volume 2, Revision 1
Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices (Available at http://csrc.nist.gov/publications/nistpubs/800–60-rev1/sp800-60_vol2-rev1.pdf.)

NIST Special Publication 800–82, Revision 2
Guide to Industrial Control Systems (ICS) Security (Available at http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf.)

NIST Special Publication 800–137
Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Available at http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.)

OMB Circular A–130
Managing Information as a Strategic Resource (Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/a130/a130revised.pdf.)

OSD Memorandum dated 21 April 2016
Enhanced Integration of Financial Management Requirements with the Risk Management Framework (Available at http://comptroller.defense.gov/portals/45/documents/fiar/workproducts/integration_of_fm_reqs_with_risk_mgmt.pdf.)

Stand–Alone Information System and Closed Restricted Network Assessment and Authorization Operational, Tactics, Techniques, and Procedures (TTP), Version 1.0
(Available at https://rmfks.osd.mil.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate website (https://armypubs.army.mil); DD Forms are available on the Office of the Secretary of Defense website (http://www.esd.whs.mil/directives/forms).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2930
Privacy Impact Assessment (PIA)

Glossary

Section I

Abbreviations

A&A
assessment and authorization

ACYC
Army Cyberspace Council

AENC
Army Enterprise Network Council

AO
authorizing official

AODR
authorizing official designated representative

APMS
Army Portfolio Management Solution

APP
Army Protection Program

AR
Army regulation

ARCYBER
U.S. Army Cyber Command

ATCTS
Army Training and Certification Tracking System

ATD
authorization termination date

ATO
authorization to operate

CAC
common access card

CCB
configuration control board

CCI
control correlation identifier

CCP
common control provider

CDS
cross domain solutions

CEH
Certified Ethical Hacker

CIA
confidentiality, integrity, and availability

CIO
chief information officer

CISA
Certified Information Systems Auditor

CISSP
Certified Information Systems Security Professional

CMB
configuration management board

CND–AU
Computer Network Defense–Auditor

CNSS
Committee on National Security Systems

CNSSI
Committee on National Security Systems instruction

COI
community of interest

CRN
closed restricted network

DA
Department of the Army

DA Form
Department of the Army form

DA Pam
Department of the Army pamphlet

DCATS
Defense Communications Army Transmissions Systems

DCS
Deputy Chief of Staff

DD Form
Department of Defense form

DEERS
Defense Enrollment Eligibility Reporting System

DIACAP
Department of Defense Information Assurance Certification and Accreditation Process

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODI
Department of Defense instruction

DODIN
Department of Defense Information Network

DREN
Defense Research and Engineering Network

DTS
Defense Travel System

EI&E
Energy, Installations, and Environment

EIS
Enterprise Information Systems

eMASS
Enterprise Mission Assurance Support System

FIAR
Financial Improvement and Audit Readiness

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

GCIH
Global Information Assurance Certification Certified Incident Handler

GS
general schedule

GSE
Government Sponsored Enterprise

GSEC
Global Information Assurance Certification Security Essentials

GSNA
Global Information Assurance Certification Systems and Network Auditor

HSPD
Homeland Security Presidential Directive

IA
information assurance

IAM
information assurance management

IAT
Information Assurance Technical

IAVM
information assurance vulnerability management

ICAN
installation campus area network

ICD
Intelligence Community Directive

ICS
industrial control system

IO
information owner

IPPS–A
Integrated Personnel and Pay System–Army

IS
information system

ISA
International Society of Automation

ISCM
information security continuous monitoring

ISO
information system owner

ISSE
Information system security engineer

ISSM
information system security manager

ISSO
information system security officer

IT
information technology

ITOC
Information Technology Oversight Council

LMP
Logistics Modernization Program

LWN
LandWarNet

MO
mission owner

MOA
memorandum of agreement

MOU
memorandum of understanding

NEC
Network Enterprise Center

NETCOM
Network Enterprise Technology Command

NIPRNET
Nonclassified Internet Protocol Router Network

NIST
National Institute of Standards and Technology

NSA CSfC
National Security Agency Commercial Solutions for Classified

NSPD
National Security Presidential Directive

NSS
National Security Systems

O–ISSM
organization information system security manager

OMB
Office of Management and Budget

OSD
Office of the Secretary of Defense

OT
operational technology

PAO
principal authorizing official

PEO
program executive officer

PII
personally identifiable information

P–ISSM
program information system security manager

PIT
platform information technology

PKI
Public Key Infrastructure

PLC
programmable logic controller

PM
program manager

POA&M
plan of action and milestones

REF
risk executive function

RMAG
Risk Management Advisory Group

RMF
Risk Management Framework

SAP/SA
Special Access Program/Sensitive Activity

SAR
security assessment report

SCA
security control assessor

SCADA
supervisory control and data acquisition

SCI
sensitive compartmented information

SCNA
Security Certified Network Architect

SCNP
Security Certified Network Professional

SIPRNET
Secret Internet Protocol Router Network

SIS
stand-alone information system

SISO
Senior Information Security Officer

SLA
service level agreement

SM
system manager

SOP
standard operating procedure

SP
security plan

SPO
Special Programs Office

SSCP
Systems Security Certified Practitioner

SSE
systems security engineering

STIG
Security Technical Implementation Guide

T&E
test and evaluation

TAO
Technology Applications Office

TEMPEST
Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions

TSP
tenant security plan

TTP
tactics, techniques, and procedures

UCAPL
Unified Capabilities Approved Product List

UR
user representative

Section II

Terms

Authorization boundary
All components of an information system to be authorized for operation by an AO and excludes separately authorized systems, to which the information system is connected (see NIST Special Publication 800–37).

Authorization to operate
The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls (see CNSSI 4009).

Authorizing official
A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (see CNSSI 4009).

Authorizing official designated representative
An organizational official acting on behalf of an AO in carrying out and coordinating the required activities associated with security authorization (see DODI 8510.01).

Availability
A loss of availability is defined as the disruption of access to or use of information or an information system (see FIPS PUB 199).

Common control provider
The ISO or CCP is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (in other words, security controls inherited by ISs).

Common security control
A security control that is inherited by one or more organization information systems (see NIST Special Publication 800–37).

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is defined as the unauthorized disclosure of information (see NIST Special Publication 800–53).

Continuous monitoring
Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions (see NIST Special Publication 800–137).

High impact
The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; in other words, causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced, results in major damage to organizational assets, results in major financial loss, or results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries (see CNSSI 4009).

Hybrid security control
A security control that is implemented in an information system in part as a common control and in part as a system-specific control (see NIST Special Publication 800–37).

Impact level
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability (see CNSSI 4009).

Industrial control system
General term that encompasses several types of control systems, including SCADA systems, distributed control systems (DCS), and other control system configurations such as PLCs often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (for example, electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (for example, manufacturing, transportation of matter or energy).

Information owner
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal.

Information Security Risk Management Committee
When the DOD Information Security Risk Management Committee accepts the risk on behalf of the DOD Information Enterprise, the receiving organization may not refuse to deploy the IS (see DODI 8510.01).

Information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see CNSSI 4009).

Information system life cycle
The phases through which an information system passes, typically characterized as initiation, development, operation, and termination (in other words, sanitization, disposal, and/or destruction) (see CNSSI 4009).

Information system owner or program manager
Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system (see NIST Special Publication 800–37).

Information system security engineer
The ISSE is an individual or group of people responsible for conducting IS security engineering activities, including system architecture, design, development, and configuration, that technically define a system’s overall security posture. The ISSE function is largely fulfilled by system administrators or security engineers.

Information system security officer
Individual assigned responsibility by the senior agency information security officer, AO, management official, or ISO for maintaining the appropriate operational security posture for an information system or program (see CNSSI 4009).

Information technology
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. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (see CNSSI 4009).

Integrity
Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. A loss of integrity is defined as the unauthorized modification or destruction of information (see CNSSI 4009).

Interim authorization to test
Temporary authorization to test an IS in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization (see CNSSI 4009).

Low impact
The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; in other words, causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced, results in minor damage to organizational assets, results in minor financial loss, or results in minor harm to individuals (see CNSSI 4009).

Moderate impact
The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; in other words, causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced, results in significant damage to organizational assets, results in significant financial loss, or results in significant harm to individuals that does not involve loss of life or serious life threatening injuries (see CNSSI 4009).

Plan of action and milestones
A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones (see CNSSI 4009).

Reciprocity
Mutual agreement among participating enterprises to accept each other’s security assessments in order to reuse information system resources and/or to accept each other’s assessed security posture in order to share information (see CNSSI 4009).

Residual risk
Portion of risk remaining after security measures have been applied (see CNSSI 4009).

Risk
Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security (see NIST Special Publication 800–37).

Risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system (see NIST Special Publication 800–37).

Risk management
The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes the conduct of a risk assessment, the implementation of a risk mitigation strategy, and employment of techniques and procedures for the continuous monitoring of the security state of the information system (see NIST Special Publication 800–37).

Risk Management Framework
A structured approach used to oversee and manage risk for an enterprise (see CNSSI 4009).

Security control assessor
The individual, group, or organization responsible for conducting security control assessment (see NIST Special Publication 800–37).

Security control inheritance
A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides (see NIST Special Publication 800–37).

System–specific security control
A security control for an information system that has not been designated as a common security control or the portion of a hybrid security control that is to be implemented within an information system (see NIST Special Publication 800–37).

Type authorization
A method of system authorization that allows a single security authorization package to be developed for an archetype (common) version of a system, and the issuance of a single authorization decision that is applicable to multiple deployed instances of the system (see DOD 8510.01).

Section III

Special Abbreviations and Terms
This section contains no entries.