Army Regulation 25–2

Information Management: Army Cybersecurity

Army Cybersecurity

Headquarters
Department of the Army
Washington, DC
4 April 2019

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–2
Army Cybersecurity

This administrative revision, dated 30 May 2019—

- Corrects the e-mail address (title page).

- This major revision, dated 4 April 2019—

- Changes the title of the regulation from Information Assurance to Army Cybersecurity (cover).

- Prescribes the use of DA Form 7789 (Privileged Access Agreement and Acknowledgement of Responsibilities) (paras 2–1*c*(3) and 2–38*a*(3)).

- Assigns responsibilities and prescribes policies for the Army Cybersecurity Program in accordance with DODI 8500.01, DODI 8510.01, and related issuances listed in appendix A (throughout).

- Implements functional elements of AR 525–2 as they relate to cyber risk management (throughout).

- Supersedes Army Directive 2013–22, Implementation and Enforcement of the Army Information Assurance Program (hereby superseded) (throughout).

- Fully integrates cybersecurity into system life cycles and makes cybersecurity a visible element of information technology portfolios (throughout).

- Implements a standard, integrated, change management process for Army information technology across all mission and business areas to ensure efficient and secure handling of all changes to the Army's information technology infrastructure, applications, systems, architecture, software, and hardware (throughout).

- Ensures that information technology and resources (personnel, equipment, and training) support operational and enterprise objectives, and are consistent with applicable laws, regulations, and standards (throughout).

- Ensures that mission-essential tasks for cybersecurity readiness are set, and assessment data are collected, processed (in an automated fashion, where possible), analyzed, reported, and continually monitored to ensure that corrective actions are taken to address readiness issues (throughout).

Headquarters
Department of the Army
Washington, DC
4 April 2019

*Army Regulation 25–2

Effective 4 May 2019

Information Management : Army Cybersecurity

Army Cybersecurity

By Order of the Secretary of the Army:

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

Official:

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

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This regulation establishes the Army Cybersecurity Program and sets forth the mission, responsibilities, and policies to ensure uniform implementation of public law and Office of Management and Budget, Committee on National Security Systems, and Department of Defense issuances for protecting and safeguarding Army information technology, to include the Army-managed portion of the Department of Defense Information Network, (hereafter referred to as information technology) and information in electronic format (hereafter referred to as information). Information technology includes infrastructure, services, and applications used directly by the Army or for the Army by legal agreements or other binding contracts.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, to include all Headquarters, Department of the Army staff, Army commands, Army Service component commands, direct reporting units, all other Army agencies, and all personnel, authorized users and privileged users, unless otherwise stated. It applies to all Army information technology and information in electronic format at all classification levels; and Special Access Program and Sensitive Activity information systems except when handling sensitive compartmented information. Nothing in this regulation alters or supersedes the existing authorities and policies of the Department of Defense or the Director of National Intelligence regarding the protection of sensitive compartmented information as directed by Executive Order 12333. The Director of National Intelligence has delegated authority for all Army Sensitive Compartmented Information systems to the Deputy Chief of Staff, G–2.

Proponent and exception authority. The proponent of this regulation is the Army Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this regulation 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, at the rank of O–6 or GS–15. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and risk. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through its higher headquarters to the policy proponent. The request must include formal review by the activity's senior legal officer and endorsement by the authorizing official. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions, in accordance with AR 11–2, and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Army Chief Information Officer/G–6 (SAIS–CB), 107 Army Pentagon, Washington, DC 20310–0107 (army.ciog6.policy-inbox@mail.mil).

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to the Publications and Blank Forms) directly to Army Chief Information Officer/G–6 (SAIS–CB), 107 Army Pentagon, Washington, DC 20310–0107 (usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil).

Committee management. AR 15–39 requires the proponent to justify establishing or continuing committee(s), to coordinate draft publications, and to coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527. Further, if it is determined that an established "group" identified within this regulation later takes on the characteristics of a committee, as found in AR 15–39, then the proponent will follow all AR 15–39 requirements for establishing and continuing the group as a committee.

Distribution. This publication 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)

*This regulation supersedes AR 25-2, dated 24 October 2007 and AD 2013-22, dated 28 October 2013.

UNCLASSIFIED

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
This regulation establishes policies and assigns responsibilities for the Army Cybersecurity Program to ensure adherence to Department of Defense (DOD) cybersecurity policies, processes, and standards. It integrates and coordinates with the functional elements of AR 525–2 to safeguard Army assets. The cybersecurity program sets the conditions necessary for the Army to protect and safeguard information technology (IT) capabilities; support mission readiness and resilience; and ensure the confidentiality, integrity, and availability of information in electronic format (hereafter referred to as information). It fully integrates risk management into every aspect of the Army.

1–2. References
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Responsibilities
See chapter 2 for responsibilities.

1–5. Records management requirements
The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule-Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Overview
Cybersecurity is a holistic program to manage IT-related security risk. To be effective, it must be integrated fully into every aspect of the Army. It requires the implementation and enforcement of proper management and operational procedures by the entire organization, from commanders and senior leaders of agencies and activities providing the strategic vision and goals for the organization, to strategic planners and project and program managers (PMs), down to each individual who helps develop, implement, and operate the IT that supports the Army's mission and business processes. Furthermore, each individual, at every level, is responsible for procedural compliance with the proper practices and procedures for safeguarding information and IT. The responsibility for ensuring that personnel abide by these practices and procedures is inherent to commanders and senior leaders of agencies and activities.

1–7. Statutory authority
Statutory authority is derived from Section 2223, Title 10, United States Code (10 USC 2223); 40 USC 11315; 44 USC, Chapter 35; and applicable Office of Management and Budget (OMB) memoranda, to include reporting requirements established via the Federal Information Security Modernization Act (FISMA) of 2014, Defense authorization and appropriations acts, and DOD issuances.

1–8. Precedence
This regulation is the proponent policy document for the Army Cybersecurity Program, which implements the DOD Cybersecurity Program. The Army will follow Director of National Intelligence (DNI), DOD, and Chairman of the Joint Chiefs of Staff (CJCS) issuances, to include directives, instructions, security technical implementation guides (STIGs), security requirements guides (SRGs), orders, and alerts. Supporting Department of the Army (DA) pamphlets will be published to provide uniform procedures for implementing and enforcing the policies in this regulation. Compliance with this regulation and the supporting DA pamphlets is mandatory. When needed, the Army Chief Information Officer/G–6 (CIO/G–6) will issue policy memoranda to amplify guidance for the policies in this document. This document does not alter or supersede existing DOD or DNI authorities and policies regarding the protection of sensitive compartmented information (SCI) and Special Access Programs (SAP) for intelligence, as directed by EO 12333, and national security

information systems, as directed by EO 13231, nor other applicable laws and regulations. The DNI has delegated authority for all Army SCI systems to the Deputy Chief of Staff (DCS), G–2. If at any time there is a conflict in this regulation with any related DNI, DOD, or Joint issuances, the higher-level policy will take precedence. Report identified conflicts or the need for amplifying guidance on DA Form 2028 (Recommended Changes to Publications and Blank Forms).

Chapter 2
Responsibilities

Commanders and senior leaders of agencies and activities at all levels and those they appoint, to include PMs, information system owners (ISOs), application owners, IT service owners, information owners, portfolio managers, resource managers, and acquisition senior and functional services managers, are accountable for the implementation and enforcement of this regulation and will ensure individual and organization accountability within organizations and activities under their purview.

2–1. Principal Officials, Headquarters, Department of the Army; Commanders of Army commands, Army service component commands, and direct reporting units; and senior leaders of agencies and activities

HQDA Principal Officials; Commanders of ACOMs, ASCCs, and DRUs; and senior leaders of agencies and activities will—

a. Implement the Army Cybersecurity Program to ensure that the personnel, processes, and IT for which they have development, procurement, integration, modification, operation and maintenance, and/or final disposition responsibility comply with this regulation and the amplifying policy guidance developed by the Army CIO/G–6. This includes, but is not limited to—

(1) Develop, maintain, and modify IT as required to ensure uniform application of cybersecurity policies, procedures, and standards, and risk management security controls, in accordance with OMB, National Institute of Standards and Technology (NIST), Committee on National Security Systems (CNSS), DOD, Joint, and Army issuances.

(2) Develop, implement, and maintain the security plan for assigned IT, as described in DODI 8510.01.

(3) Ensure that IT has been granted authorization to operate (ATO) by the assigned authorizing official (AO). Comply with all authorization decisions, including denial of authorization to operate. Enforce authorization termination dates.

(4) Transition from legacy or end-of-life cross-domain solutions (CDS) to those on the CDS baseline list managed by the Unified Cross-Domain Management Office (UCDMO).

(5) When a cross-domain service is required, leverage those provided by the Defense Information Systems Agency (DISA) to the fullest extent possible.

(6) Provide appropriate notice of privacy rights and explain monitoring policies to all users.

(7) Require user authentication to DOD information systems and networks in accordance with DODI 8520.03.

(8) Ensure an effective vulnerability management process is in place, which includes—

(a) Ensuring that baseline configurations contain all required patches and follow applicable STIGs and SRGs at the time the baseline is established, and are updated upon the release of new or revised information assurance vulnerability alerts, STIGs, and SRGs.

(b) Ensure that security patches are made available for new vulnerabilities and are applied in accordance with the suspense dates or sooner if possible, per operational directives.

(c) Employ an automated patching process, when practical, in order to minimize manpower requirements and system downtime.

(d) Provide authorized personnel the access necessary to conduct required technical compliance assessments, to include vulnerability scans.

(9) Provide for vulnerability mitigation and incident response and reporting capabilities in order to—

(a) Comply in a timely and efficient manner with DOD and Army cybersecurity directives, guidance, and alerts for implementing mitigations and taking corrective action in defense of the DOD information network (DODIN).

(b) Limit damage and restore effective service following an incident.

(c) Collect and retain audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under their purview, and provide these data to appropriate law enforcement or other investigating agencies.

(10) Implement security-informed configuration management (CM) and change management processes in accordance with NIST guidance and as described in DODI 8440.01.

(11) Implement insider threat policy, guidance, and monitoring activities as part of a comprehensive cybersecurity program directed by national, DOD, and office of the DNI leadership.

b. Assign the appropriate responsibility and authority to individuals within the organization as necessary to implement, manage, and enforce this regulation, and for all applicable roles in accordance with DODI 8510.01, DODD 8140.01, and related DOD, CNSS, and Army issuances.

(1) Appoint and oversee privileged users as required to carry out appointed functions. Ensure that privileged users meet the requirements for authorized and privileged users in accordance with this regulation. Monitor privileged users to ensure that they continue to meet the requirements.

(2) Ensure that all cybersecurity personnel under their purview are appointed in writing. Manage their training and certification through the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil.

c. Ensure that all personnel—

(1) Are appropriately cleared, trained, qualified, and authorized in accordance with applicable CNSS, DOD, and Army information security, communications security (COMSEC) and cybersecurity issuances before accessing IT, and continue as such while authorized access.

(2) Sign a user agreement of acknowledgement (paper or electronic) prior to account activation and annually thereafter that states they—

(a) Have read, understood, and agreed to abide by, notably the rules that describe user responsibilities and expected behavior for IT usage in accordance with this regulation.

(b) Have read, understood and agreed to the notice of privacy rights, and consented to monitoring and searches in accordance with this regulation.

(3) Create and maintain a profile in the ATCTS. Ensure that users' profiles are current and correct with all applicable documentation, to include completed DD Form 2875 (System Authorization Access Request (SAAR)), annually signed user agreement, applicable training certificates, and, as applicable , DA Form 7789 (Privileged Access Agreement and Acknowledgement of Responsibilities), appointment memoranda, and records of professional certifications.

d. Military and civilian personnel may be subject to appropriate action if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policies and procedures. Violations are identified in the Army IT user agreement.

(1) These provisions may be punished as violations as follows:

(a) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to IS or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may be awarded only by civilian managers or military officials who have authority to impose the specific sanction(s) proposed.

(b) Sanctions for military personnel may include, but are not limited to, some of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss or suspension of access to IS or networks and classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by service directives and any administrative measures or non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ).

(c) Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations and must maintain employee discipline. The contracting officer, or de-signee, is the liaison with the defense contractor for directing or controlling contractor performance. Outside the assertion of criminal jurisdiction for misconduct, the contractor is responsible for disciplining contractor personnel. Only the Department of Justice may prosecute misconduct under applicable Federal laws, absent a formal declaration of war by Congress (which would subject civilians accompanying the force to UCMJ jurisdiction). For additional information on contractor personnel authorized to accompany U.S. Armed Forces, see DODI 3020.41.

e. Build capabilities to support cybersecurity objectives that are shared with mission partners, and ensure that they are consistent with guidance contained in DOD 8000.01 and governed through the integrated decision structures and processes described in DODI 8500.01.

f. Identify the resources required to implement DODI 8510.01 for inclusion in the Defense planning, programming, budgeting, and execution process.

g. Incorporate cybersecurity risk assessments and decisions, in accordance with DODI 8510.01, into Army mission and business risk management processes.

h. Ensure consistent development and incorporation of cybersecurity requirements into plans and procedures across their areas of responsibility.

i. Maintain ongoing awareness of cybersecurity threats and vulnerabilities to support risk management decisions. Ensure that real-world threat data and analysis inform risk decisions. Consider shared risks. Take no unnecessary risk, but do not be risk-averse.

j. Integrate security early and throughout the IT development life cycle, capital planning, investment control, portfolio management, and enterprise architecture processes in accordance with the DOD Cybersecurity Architecture and other applicable DOD and Army issuances.

k. Integrate security standards into acquisition planning and contract administration. Ensure that contracts and other agreements include specific requirements to provide cybersecurity for information and the IT used to process that information in accordance with DODI 8500.01 and DODI 8510.01. Document baseline cybersecurity requirements as a condition of contract award for acquisitions utilizing IT.

l. Ensure that incident response and reporting programs are followed, and personnel are aware of, and held accountable for, daily practices that protect against suspected intrusions, unauthorized activity, suspected attacks, and other anomalous activity. Report suspected or confirmed incidents in accordance with Army regulations relevant to the specific incident, Army Cyber Command (ARCYBER) or supporting cybersecurity service provider's published procedures, and formal internal policies and procedures.

m. Ensure that maintenance and disposal of information on IT comply with the provisions of DODI 5015.02 and AR 25–400–2.

n. Comply with the specific policies developed by the CIO/G–6 for the Army Cybersecurity Program, in accordance with the statutory requirements outlined in FISMA.

o. For all assigned IT, comply with AO decisions.

p. Comply in a timely and efficient manner with DOD and Army cybersecurity issuances for mitigating and taking corrective action in defense of the DODIN.

q. Conduct DODIN operations and defensive cyberspace operations - internal defense measures (DCO–IDM) when directed by ARCYBER.

2–2. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

In addition to the responsibilities in paragraph 2–1, the ASA (ALT) will–

a. Ensure that DODI 8510.01 processes are appropriately integrated into the Defense Acquisition System processes for IT procurement.

b. Verify that adequate support for cybersecurity requirements is planned, resourced, and documented, and can be executed in a timely manner in accordance with DODI 8510.01 and other applicable NIST, CNSS, DOD, and Army issuances.

c. Ensure that solutions meet DODI 8510.01, system survivability key performance parameters, and requirements for cyber resiliency.

d. Issue policy and guidance to ensure that systems security engineering (SSE) and the trusted systems and networks processes, tools, and techniques described in DODI 5200.44 are incorporated into the acquisition of all applicable IT.

e. Implement DOD-wide cybersecurity solutions when possible.

f. Ensure that contracts and other agreements include specific requirements to provide cybersecurity for information and IT, including platform IT and control systems, in accordance with DOD policies, procedures, standards, and other guidance.

g. Issue policy and guidance to ensure that cybersecurity testing and evaluation (T&E) are conducted throughout the acquisition life cycle and are integrated with interoperability and other functional testing.

h. Ensure that a cybersecurity representative participates in planning, execution, and reporting of integrated T&E activities in accordance with DODI 5000.02.

i. Verify that adequate T&E support for cybersecurity requirements is planned, resourced, and documented, and can be executed in a timely manner in accordance with DODI 5134.17 and applicable Director, Operational Test and Evaluation memoranda.

j. Ensure that policy and procedures for developing program protection plans, as required by DODI 5000.02, include cybersecurity strategy requirements in accordance with DODI 8500.01 and other applicable DOD and Army issuances.

k. Ensure that program protection plan cybersecurity strategy annexes for systems are developed, implemented, and maintained consistent with DODI 5000.01, DODI 8510.01, NIST and DOD standards, and DOD architectures for all IT; that the annexes have been validated by the Army CIO/G–6; and that they enable receiving units to comply with DOD- and Army-approved processes into the sustainment phase.

l. Ensure that acquisition community personnel with IT development responsibilities meet the standard qualification criteria in accordance with DOD 8570.01–M.

m. Issue policy and guidance to ensure the mitigation of vulnerabilities that are successfully exploited during the Army Interoperability Certification System-of-Systems Network Vulnerability Assessment.

n. Review system sustainment plans for both new and existing systems, in coordination with the U.S. Army Materiel Command (AMC), to ensure cybersecurity sustainment for the system after fielding and continued compliance with DODI 8510.01.

o. Provide a capability to inventory IT assets that automatically generates a complete view of vulnerabilities and intrusion detection activities.

p. Provide an automated patch management capability as part of life-cycle management in order to minimize system downtime and to prevent adding personnel requirements to organizations using the systems.

q. Provide IT threat data support to AOs for development and execution of plan of action and milestones (POA&Ms) to address known vulnerabilities in IT, in coordination with the Army Research Laboratory System Lethality Analysis Directorate and ARCYBER.

r. Ensure that technical and equipment publications for IT-enabled end items include any cybersecurity-related requirements in accordance with the AO's ATO, for example, software patching requirements as part of preventative maintenance checks and services.

s. Support the Army CIO/G–6 and Army stakeholders during the development, implementation, and maintenance of an effective cybersecurity strategy, for both new and existing systems. This strategy will be consistent with DOD policies, standards, and architectures for all IT and will enable receiving units to comply with DOD- and Army-approved processes into the sustainment phase.

t. Oversee the transition of legacy or end-of-life CDS to CDS on the CDS baseline list managed by the UCDMO.

2–3. Assistant Secretary of the Army (Financial Management and Comptroller)

In addition to the responsibilities in paragraph 2–1, the ASA (FM&C) will—

a. In coordination with DCS, G–8 and ASA (ALT) verify that programmed and budgeted resources are incorporated into budget justification material for IT investments in order to ensure understanding of approved requirements that support DODI 8510.01.

b. Develop, implement, and maintain an IT security plan, as defined by DODI 8510.01, for each ASA (FM&C) IT system, to include a list and the implementation status of all required controls.

2–4. Assistant Secretary of the Army (Installations, Energy and Environment)

In addition to the responsibilities in paragraph 2–1, the ASA (IE&E) will ensure that cybersecurity requirements and operational concerns are considered and integrated into Army efforts related to installations, Army real estate, energy security and sustainability, and the environment during all phases of planning and development.

2–5. Assistant Secretary of the Army (Manpower and Reserve Affairs)

In addition to the responsibilities in paragraph 2–1, the ASA (M&RA) will—

a. Ensure that personnel policies implement applicable cybersecurity controls required across the Army, per DODI 8510.01.

b. Ensure that modified table of equipment, table of organization and equipment, military occupational specialties, and civilian occupational series are updated in order to meet requirements for cyber-related functional areas, military and civilian work roles, credentials, and security clearances. Use existing personal assignment processes and guidelines to support ongoing changes. Integrate approved cybersecurity tools, doctrine, procedures, including the risk management framework (RMF), and legal requirements into applicable programs of instruction for U.S. Army Training and Doctrine Command (TRADOC) schools.

c. Ensure that SSE functions are integrated into the systems engineering workforce and curriculum, in accordance with DODI 5134.16.

d. Coordinate with the Army CIO/G–6 regarding implementation of cybersecurity requirements for effective manning, management, and readiness assessments of the cybersecurity workforce.

2–6. Administrative Assistant to the Secretary of the Army

In addition to the responsibilities in paragraph 2–1, the Administrative Assistant to the Secretary of the Army will ensure development of procedures for managing and reporting loss or unauthorized disclosure of personally identifiable information (PII), or other Privacy Act information, including information in electronic format.

2–7. Army Chief Information Officer/G–6

In addition to the responsibilities in paragraph 2–1, as the Army CIO, the CIO/G–6 will—

a. In accordance with DODI 8500.01, on behalf of the Secretary of the Army, establish policy, resourcing, and oversight of the Army Cybersecurity Program that is consistent with DOD Senior Information Security Officer strategy and the Defense Cybersecurity Program, and complies with DODI 8500.01.

b. Issue policies and guidance for Army cybersecurity activities to support DODIN operations as described in DODI 8530.01.

c. Set the strategic direction and policy, and verify that enterprise resources are used effectively for Armywide activities, to design, build, configure, secure, operate, maintain, modernize, and sustain the Army-managed portion of the DODIN; and to protect and defend IT by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

d. Promulgate policies and guidance to ensure that all IT complies with applicable law and national, Federal, and DOD issuances, to include National Security Agency (NSA) issuances, NIST standards, DOD STIGs, and DOD SRGs, with exceptions documented and approved by the responsible AO.

e. Ensure that support for the DOD cybersecurity architecture, which is used to manage the Enterprise Information Environment Mission Area (EIEMA) portfolio, is provided as described in DODD 8115.01.

f. Validate that IT investments comply with DODI 8500.01, to include leveraging DOD-wide cybersecurity solutions to the extent practical, and DODI 8530.01; and are consistent with DOD and Army cybersecurity architecture.

g. As the Army EIEMA lead, manage the portfolio of cybersecurity capabilities in accordance with DODD 8115.01 and DODI 8115.02 to ensure that investments support DOD requirements, as described in DODI 8530.01.

h. In conjunction with DOD, ensure that in-depth cybersecurity orientation, training, certification, and awareness programs are developed and made available to all Army personnel.

i. Serve as the principal Army member of the CNSS.

j. Serve as the approval authority for Army Interoperability Certification.

k. Serve as the Army registration authority for the public key infrastructure (PKI) of the Army-managed portion of the DODIN in accordance with DODI 8520.02.

l. Serve as the Service component lead for DOD PKI. The CIO/G–6 holds responsibility, authority, and oversight, and develops policy, for cybersecurity activities, including PKI and public-key enabling technologies. The CIO/G–6 also ensures compliance with DOD, NSA, DISA, and Army policy.

m. Issue policy and guidance to ensure that Armywide activities implement CNSS and DOD COMSEC-related issuances.

n. Oversee implementation of the Army COMSEC Program, including enforcement of all applicable DOD and Army COMSEC policies, directives, criteria, standards, and doctrine, to include—

(1) Develop policy and procedures for the COMSEC material control system key management infrastructure (KMI).

(2) Oversee modernization of the Army-managed portion of the KMI.

(3) Develop policy and procedures for COMSEC account establishment.

(4) Oversee distribution of cryptographic hardware.

(5) Review proposed COMSEC programs and the associated resource requirements, and recommend resource allocations.

(6) Establish procedures ensuring that KMI operating account managers and alternate KMI operating account managers are properly appointed and trained.

(7) Review and validate all Army requirements for COMSEC products and services, and forward to the DCS, G–3/5/7 for prioritization of support to execute Army General Order (AGO) 2017–01 responsibilities and request NSA technical services.

(8) Forward validated and prioritized Army requirements for COMSEC products and services to the Director, NSA to support procurement activities.

(9) Oversee COMSEC operations, policy, procedures, and training.

(10) Provide management oversight of the Army Key Management Enterprise Infrastructure, including implementation of the KMI, the Electronic Key Management System, and the Army Key Management System.

(11) Appoint an Army voting member to the Key Management Executive Committee and Joint KMI working group.

(12) Appoint the chairperson and alternate chairperson for the Tier 1 System Management Board, which has operations management responsibilities for the Electronic Key Management System Common Tier 1 System.

o. Appoint AOs when deemed necessary.

p. Issue policy and guidance to appointed Army AOs, in accordance with DODI 8510.01, to ensure that AO decisions are integrated and synchronized with the conduct of DODIN operations.

q. Ensure that appropriate authorizations are obtained and maintained throughout the system life cycle.

r. Coordinate with ARCYBER regarding any system that introduces a "very high" or "high" risk level to determine under what conditions such a system may operate due to mission criticality.

s. Represent the Army at DOD, Federal, Joint and Army-level AO forums.

t. Appoint the Army senior information security officer (SISO).

u. Appoint the Army code signing AO.

v. Advise the ASA (ALT) to ensure that all IT is acquired in accordance with DOD and Army cybersecurity issuances.

w. Advise Army mission area leads to ensure that cybersecurity requirements are addressed for all IT.

x. Oversee transition of legacy or end-of-life CDS to CDS on the CDS baseline list managed by UCDMO.

y. When a CDS is required, promote use of DISA-provided cross-domain services to the extent possible.

z. Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing Army-owned or controlled IT.

aa. Issue policy and guidance to ensure that cybersecurity solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities, or access to or use of information and data by individuals with disabilities, in accordance with law and DOD issuances.

bb. Ensure that cybersecurity requirements are addressed and visible in all capability portfolios, and are properly addressed during IT development in the non-kinetic (cyber) piece of the systems survivability key performance parameters, technical architectures, IT life-cycle management processes, and investment programs that incorporate IT.

cc. As the functional proponent and Army staff integrator for Information Technology and Information Management, coordinate and advocate for resources for Armywide cybersecurity solutions with appropriate Program Evaluation Groups (PEGs), to include overseeing appropriations allocated to the Army Cybersecurity Program.

dd. Ensure that system-of-systems network vulnerability assessments are integrated into the Army Interoperability Certification program.

ee. Coordinate with the Inspector General (DAIG) and the Army Auditor General to identify root causes and solutions for systemic and critical cybersecurity issues reported to the Army Risk Management Council (ARMC).

ff. Issue and annually review the requirements governing the appropriate use of Army IT, which will be included in all Army IT user agreements.

gg. Validate whether program protection plan cybersecurity strategy annexes comply with DODI 8510.01 and DODI 5000.02.

hh. Sustain an Armywide PKI for the Army-managed portion of the DODIN, in accordance with DODI 8520.02.

ii. Oversee the Army registration authority for the issuance of PKI credentials.

jj. Provide guidance and oversight of Army IT implementation to ensure that ports, protocols, and services follow the requirements outlined in DODI 8551.01. Designate, in writing, a primary and one or more alternate voting representatives to the DOD Ports, Protocols, Services Management Configuration Control Board and ensure representation at all Ports, Protocols, Services Management Configuration Control Board meetings. Representatives will be designated in accordance with the requirements identified in DODI 8551.01.

kk. Provide regulatory and policy direction and oversight for the ATO and authority to connect processes.

ll. Coordinate with the DCS, G/3/5/7 regarding the issuance of appropriate implementation instructions to ensure that all Army organizations are responsive to ARCYBER DODIN operations and DCO–IDM directives.

mm. Develop and publish common cybersecurity assessment benchmarks based on the DOD RMF and in accordance with NIST guidance.

nn. In addition to the responsibilities in paragraph 2–1, as the Army Staff G–6, the CIO/G–6 will—

oo. Promote and facilitate the Army Cybersecurity Program and related activities to support DODIN Operations and DCO, as described in DODI 8530.01.

pp. Oversee management of cybersecurity activities to support DODIN operations and DCO–IDM, as described in DODI 8530.01.

qq. Maintain an Army cross-domain support element to coordinate cross-domain activities with the Unified Cross-Domain Services Management Office, in accordance with DOD CIO guidance. Ensure use of DISA-provided cross-domain services as the preferred method of addressing cross-domain requirements for secret networks. Cross-domain systems for domains above secret will adhere to cross-domain intelligence community standards and requirements.

rr. Manage resources for Army cybersecurity programs, to include Army Joint Worldwide Intelligence Communications System (JWICS), in accordance with ASA (FM&C) directives and guidance published in the Army Planning Priorities Guidance and the Army Programming Guidance Memorandum.

ss. Ensure that cybersecurity inspections and compliance oversight activities are accomplished in coordination with AR 525–2, and that the cybersecurity trend information is shared with key stakeholders.

tt. Integrate Federal-, DOD-, and Joint-directed cybersecurity requirements into the Army technical architecture and capability sets.

2–8. The Inspector General

In addition to the responsibilities in paragraph 2–1, the DAIG will—

a. Conduct an annual independent evaluation to determine the effectiveness of the Army Cybersecurity Program and cybersecurity practices, as required by 44 USC 3555.

b. As part of the evaluation of the Army Cybersecurity Program and cybersecurity practices, leverage FISMA Inspector General metrics to assess the maturity of the Army's implementation of framework functions to address risks.

c. Leverage the cybersecurity mission-essential task list to identify systemic readiness issues and report the root causes of such at least annually.

d. Coordinate with the Army CIO/G–6 and the Army Auditor General to identify root causes and support identification of solutions for systemic and critical cybersecurity issues reported to the ARMC.

2–9. Army Auditor General

In addition to the responsibilities in paragraph 2–1, the Auditor General will—

a. Help resolve cybersecurity issues by identifying solutions for issues that cause unacceptable Army-wide risk or inefficient use of resources.

b. Coordinate with the Army CIO/G–6 and the DAIG to identify solutions for root causes of systemic and critical cybersecurity issues reported to the ARMC.

2–10. Deputy Chief of Staff, G–1

In addition to the responsibilities in paragraph 2–1, the DCS, G–1 will—

a. Assign a position designation (PD) for personnel occupying cybersecurity positions using the criteria found in DODM 5200.02 and DODI 1400.25, Vol. 731; and document the PD in the Defense Civilian Personnel Data System.

b. Ensure that the PD includes the associated suitability and fitness requirements in accordance with DOD policies, procedures, standards, and other guidance, as described in DODI 1400.25, Vol 731.

c. The ASA (M&RA), in delegating operational responsibilities for the human resources management domain, directs the DCS, G–1 to provide oversight of all IT business systems in the human resource management domain within the business mission area.

2–11. Deputy Chief of Staff, G–2

In accordance with IC directives, the DCS, G–2 is the Army's senior intelligence officer and serves as the Army intelligence element lead. In this capacity, the DCS, G–2 has delegated authority from the DNI over IC operating environments, to include the Top Secret DOD Intelligence Information System's JWICS and standalone SCI systems. On the DCS, G-2's behalf, the Director, Intelligence Community Information Management (DAMI–IM) serves as the Army's Intelligence CIO, AO, and security control assessor (SCA). The DAMI–IM promulgates policies and guidance that govern operations and ensure the Army's adherence to IC directives and IC standards. Nothing in this regulation alters or supersedes the existing authorities and policies of the DOD or the DNI regarding the protection of SCI, as directed by EO 12333. The DNI has delegated authority for all Army SCI systems to the DCS, G–2. In addition to the responsibilities in paragraph 2–1, the DCS, G–2 will—

a. Serve as the Army senior intelligence officer and Army Intelligence lead with purview over IT that processes SCI.

(1) Oversee Armywide activities to manage the Army portion of the JWICS and SCI systems, in accordance with DNI issuances.

(2) Issue policy and guidance to manage the Army portion of the JWICS and SCI systems, in accordance with DNI issuances.

b. Include the DOD cybersecurity architecture in their management of the Army portion of the Defense Intelligence mission area portfolio as described in DODD 8115.01.

c. Ensure that IT investments in the Defense Intelligence mission area portfolio comply with DODI 8500.01.

d. Issue procedures for promptly managing and reporting actual or potential compromise of classified information and unauthorized disclosure of controlled unclassified information (CUI) in an electronic format, to include such losses on cleared contractor systems.

e. Develop a policy for and ensure the collection, analysis, and dissemination of national, DOD, theater, and Army-level cyber threat data, in accordance with applicable national, DOD and Army issuances.

f. Prescribe the activities, policies, processes, procedures, and protocols for reportable intelligence and information related to cyberspace.

g. Review programs to evaluate physical security compliance with COMSEC policies and procedures issued by CNSS, NIST, DOD, the Joint Staff, and the Army.

h. Develop policy and procedures for safeguarding and controlling COMSEC, controlled cryptographic items (CCIs) and cryptographic high-value product (CHVP) material.

i. Develop policy and procedures for COMSEC monitoring.

j. Make final adjudication decisions to determine when reported COMSEC incidents result in COMSEC insecurities.

k. Manage the DA Cryptographic Access Program.

l. Coordinate with the Army CIO/G–6 and the NSA, as appropriate, regarding the release of Army COMSEC material or foreign COMSEC material in the Army's custody to nonmilitary agencies, the general public, foreign nationals, or foreign governments.

m. Accept the cryptographic access granted by other DOD components.

n. Ensure that CNSS requirements, as they apply to DCS, G–2 responsibilities, are met.

o. The Director, Intelligence Community Information Management serves as the Army's intelligence chief information officer for IT that processes SCI.

(1) Serve as the approval authority for external information systems' penetration and exploitation testing of JWICS and SCI intelligence networks.

(2) Oversee security control assessors for the Army-managed portion of the JWICS and SCI systems.

p. Oversee the hardware programming life cycle of Army JWICS IT.

q. Oversee vulnerability and risk assessment of JWICS IT infrastructure, as dictated by DNI directives.

r. Establish guidance to control RMF compliance for JWICS IT through regular formal security assessments.

2–12. Deputy Chief of Staff, G–3/5/7

In addition to the responsibilities in paragraph 2–1, the DCS, G–3/5/7 will—

a. Ensure utilization of the DOD cybersecurity architecture.

b. Ensure that IT investments comply with DODI 8500.01.

c. Validate that the cybersecurity and cyber resilience of capabilities are addressed consistent with NIST, CNSS, DOD, and Army issuances.

d. Ensure that vulnerability mitigation, incident response, and reporting capabilities are integrated with IT-enabled Army capabilities across mission and functional areas, as described in DODI 8500.01 and DODI 8530.01.

e. Ensure that cybersecurity training is integrated and conducted throughout the Army.

f. Report systemic or critical cybersecurity-related issues identified during Army protection program assessments, critical infrastructure risk management assessments, and insider threat monitoring to applicable governing bodies. Cybersecurity will be included as part of Army protection program assessments and protection-related actions, in accordance with AR 525–2.

g. Track operational compliance with directed vulnerability mitigation and incident response actions related to cyberspace operations.

h. Establish and maintain a multi-disciplinary threat management capability, called an Army Insider Threat Hub, to conduct and integrate the monitoring, analysis, reporting, and response to insider threats.

i. Ensure that cybersecurity is included as a specific readiness status reporting requirement for Army units, organizations and installations, as applicable, in accordance with the DOD Cybersecurity Discipline Implementation Plan (CSDIP) dated August 2015.

j. Serve as the Army lead to synchronize and integrate cybersecurity with other industrial control system priorities.

k. Prioritize the Army requirements, validated by the Army CIO/G–6, for COMSEC products and services, and provide to the Army CIO/G–6, who will forward to the Director, NSA to support procurement activities.

l. Coordinate and synchronize cybersecurity resiliency reviews of Army warfighting platforms.

m. Validate the cybersecurity mission-essential task list for readiness status reporting.

n. Ensure consideration of the AO's risk decision when conducting operational risk assessments.

o. In coordination with the Army CIO/G–6, issue appropriate implementing instructions to ensure that all Army organizations are responsive to ARCYBER DODIN Operations and DCO–IDM directives.

p. Coordinate and synchronize all Army-led cybersecurity and protection inspections of ACOMs, ASCCs, and DRUs, including service providers for installations.

2–13. Deputy Chief of Staff, G–4

In addition to the responsibilities in paragraph 2–1, the DCS, G–4 will—

a. Ensure that logistics policies implement applicable cybersecurity controls required across the Army, per DODI 8510.01, to include but not limited to: asset management, sustainment, and maintenance.

b. Integrate IT asset management into existing asset management and inventory procedures.

c. Provide policy and procedures to ensure accountability and visibility of CCI in accordance with the related CNSS, DOD, and Army issuances.

d. Maintain centralized records of COMSEC material and CHVP at the Army level, in accordance with applicable DOD and Army issuances.

e. Provide life-cycle support planning for COMSEC that includes the resources for sustainment in accordance with applicable CNSS, DOD, and Army issuances.

2–14. Deputy Chief of Staff, G–8

In addition to the responsibilities in paragraph 2–1, the DCS, G–8 will independently assess the development, integration, and defense of programming to support Army cyber investments in the program objective memorandum and the Planning, Programming, Budgeting and Execution System.

2–15. Assistant Chief of Staff for Installation Management

In addition to the responsibilities in paragraph 2–1, ACSIM will–

a. Ensure that cybersecurity requirements are integrated into Army facilities, energy, and environmental systems life-cycle planning.

b. Ensure that contracts and other agreements include specific requirements to provide cybersecurity for systems supporting Army facilities and energy and environmental missions.

c. Implement cybersecurity controls for control systems, as appropriate, to mitigate unacceptable cyber risks to Army missions.

d. Implement specific cybersecurity requirements for managing facilities' control systems.

e. Under the supervision of the ASA (IE&E), develop and execute Army strategy, policy, plans, and programs; ensure the execution of other DA organizations' policies, plans, and programs, consistent with law, regulation, and policy; and review and assess the execution of Army policies, plans, and programs related to Army installation management, military facilities investment requirements and strategy, housing, installation environmental management and stewardship, privatization and energy security, and sustainability issues.

f. Under the supervision of ASA (M&RA), develop infrastructure and monitor the execution of programs for installation services and management that support readiness and enhance the well-being of Soldiers and Families.

2–16. Provost Marshal General

In addition to the responsibilities in paragraph 2–1, the Provost Marshal General will ensure that the physical security program includes the measures required to safeguard IT and COMSEC equipment appropriately.

2–17. Commanders of Army commands, Army service component commands, and direct reporting units, and senior leaders of agencies and activities

In addition to the responsibilities in paragraph 2–1, Commanders of ACOMs, ASCCs, and DRUs, and senior leaders of agencies and activities will—

a. Incorporate cybersecurity into Organizational Inspection Programs and Staff Assistance Visits, in accordance with AR 1–201.

b. Include assessments of the current cyber risk to designated capabilities and assigned missions when determining and reporting unit readiness status.

c. Conduct DODIN operations and DCO–IDM in accordance with directives issued by ARCYBER.

2–18. Commanding General, U.S. Army Training and Doctrine Command

In addition to the responsibilities in paragraphs 2–1 and 2–17, the Commanding General (CG), TRADOC will—

a. Assess and enable management of cyber risk to capabilities by ensuring that cybersecurity requirements are addressed consistent with national and DOD directives, to include presidential policy directives and executive orders, applicable OMB memoranda, DODI 8510.10, and the Manual for the Operation of the Joint Capabilities Integration Development System (JCIDS), Appendix C to Enclosure D, Content Guide for System Survivability Key Performance Parameters.

b. Develop, integrate, and synchronize cybersecurity training, education, and leader development that prepares leaders and units to support cyber operations.

c. Develop and maintain a cybersecurity mission-essential task list for readiness status reporting.

d. Identify, collect, analyze, and disseminate doctrine, organization, training, materiel, leadership and education, personnel, and facilities cybersecurity solutions based on operations, tactics, techniques, procedures and lessons learned, and integrate them into best practices and doctrine.

e. Ensure that the NSA/Joint Service-developed program of instruction for the KMI/management client, and the respective course administrative data and program of instructions for the COMSEC Account Manager Course and Local

COMSEC Management Software, are strictly followed in institutional COMSEC classrooms at the Cyber Center of Excellence and applicable satellite COMSEC training facilities.

f. Develop, test, and recommend operational and organizational concepts and doctrine to achieve cybersecurity goals and ensure that standardized management and operational cybersecurity controls are implemented, as described in DODI 8510.01.

g. Develop and provide cybersecurity requirements to materiel developers and ensure compliance with DODI 8510.01 and Joint and Army issuances.

2–19. Commanding General, U.S. Army Materiel Command

In addition to the responsibilities in paragraphs 2–1 and 2–17, the CG, AMC will—

a. Provide Armywide materiel developer cybersecurity support for research, development, production, and sustainment.

b. Serve as the lead for research and development of cybersecurity identify, protect, detect, respond, and recover technologies; and analysis of products that align IT with the overall needs of the warfighter, as well as the intelligence and business activities that support the warfighter.

c. Manage test and evaluation activities of the Communications - Electronics Research, Development and Engineering Center Commercial COMSEC Evaluation Program in support of the Army CIO/G–6. Ensure that tests and evaluations are supported in accordance with AR 700–142. As part of the issue resolution process, collaborate with the NSA prior to introduction to the Army inventory.

d. Manage Communications - Electronics Research, Development and Engineering Center cryptographic and key management technology exploration and validation activities in support of the Army CIO/G–6.

e. Assist IT functional proponents in identifying cybersecurity requirements for proposed and existing sustaining base, tactical, and weapon systems under AMC purview.

f. Provide IT threat data support to AOs for development and execution of POA&Ms to address known vulnerabilities in IT, in coordination with the Program Executive Office (PEO) Simulation, Training, and Instrumentation Threat System Management Office and the Army Research Laboratory System Lethality Analysis Directorate.

g. Integrate approved cybersecurity tools, doctrine, procedures, legal requirements, and techniques into applicable sustainment training programs of instruction provided by Life Cycle Management Command.

h. On a reimbursable basis, provide any required cybersecurity services to the Army-managed portion of the Defense Research and Engineering Network (DREN), as described in DODI 8530.01.

i. Review system sustainment plans, in coordination with ASA (ALT), to ensure cybersecurity sustainment for the system after fielding and continued compliance with DODI 8510.01.

j. Provide life-cycle management guidance for COMSEC capabilities, in accordance with applicable NIST, CNSS, DOD, and Army issuances.

k. The Communications Security Logistics Activity will ensure a continual ATO for, and host and operate, the Army Information System Security Program Application on behalf of the Army CIO/G–6 in order to meet the CNSS and DOD requirements to control COMSEC.

l. Program, budget, and procure COMSEC equipment, test measurement and diagnostic equipment, keying material, and other materiel necessary to support AMC-conducted resident and exportable training and new equipment training.

2–20. Commanding General, U.S. Army Cyber Command

The CG, ARCYBER will—

a. Serve as the single point of contact for reporting and assessing Army cyberspace incidents, events, and operations on the Army's portion of the DODIN.

(1) Establish and maintain a single source to report Army organizations' cyberspace incidents to U.S. Cyber Command.

(2) Develop and publish cyberspace incident response guidelines, checklists, and procedures in coordination with law enforcement and counterintelligence agencies.

(3) Assess incident reports to identify systemic or critical cybersecurity-related issues and report them to the ARMC.

b. Synchronize and integrate Army assessments of and responses to cyberspace events and incidents.

c. Execute the Army's insider threat initiatives in accordance with Army Insider Threat Program direction.

d. Plan and direct cybersecurity protective measures on the Army's portion of the DODIN at the strategic and operational levels.

e. Direct actions on the Army's portion of the DODIN in response to emerging threats and vulnerabilities.

f. Support the development of cybersecurity policy, standards, processes, and operational procedures, and coordinate Army cybersecurity programs and funding.

g. Advise the Army CIO/G–6 of trends that present unacceptable cyber risk or inefficient or ineffective use of resources. Leverage data from Government accountability office reports; DOD, Joint and Army cybersecurity inspection and assessment programs, to include Army protection program assessments and Army Inspector General and Army Audit Agency reports; incident and problem reports within Army-managed IT services; and automated data collection methods, to the greatest extent practical for optimal use of resources.

h. Operate and maintain the Army cyberspace incident database for trend analysis. Leverage data from existing DOD, Joint, and Army cybersecurity inspection and assessment programs to identify compliance trends that present unacceptable risk, and share the results with the Army CIO/G–6 and Army stakeholders.

i. Prescribe the activities, policies, processes, procedures, and protocols for reportable cyberspace intelligence and information, as well as incident management, event management, problem management, operational security, and database and internet/web management.

j. Establish, maintain, and direct standardized tactics, techniques, and procedures through which commanders and Army organizations ensure network availability and the security and defense of mission-critical and mission-essential systems; and that integrate approved response options to protect warfighter, business, and intelligence functions in cyberspace.

k. In coordination with the U.S. Cyber Command and through HQDA, ensure Army compliance with the Cyber Threat Sharing Act of 2015.

l. Conduct information operations missions, in accordance with AR 525–20, in support of the Army Cybersecurity Program.

m. Serve as the Army cybersecurity service provider for general services (that is, secure internet protocol router network (SIPRNet) and non-classified internet protocol router network (NIPRNet)); and, as such, obtain and maintain U.S. Strategic Command accreditation.

n. Conduct vulnerability assessments, blue team vulnerability evaluations and intrusion assessments, cybersecurity inspections, and red team operations (using internal or external capabilities) to provide a systemic view of Army enclave and information system cybersecurity posture.

o. Manage Army vulnerability mitigation and incident response and reporting processes in order to—

(1) Comply with mitigations directed by Commander, U.S. Strategic Command orders or other directives, such as alerts and bulletins, and provide support to cyberspace defense.

(2) Limit damage and restore effective service following an incident.

(3) Collect and keep audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under ARCYBER's purview, and provide this data to appropriate law enforcement or other investigating agencies.

(4) Establish procedures to ensure prompt management action and reporting in accordance with DODM 5200.01, Volume 3, for an actual or potential compromise of classified information; DODM 5200.01, Volume 4, for an actual or potential unauthorized disclosure of CUI (for example, proprietary information, law enforcement information); DOD 5220.22–M, when such losses occur on cleared contractor systems; and DOD 5400.11–R for a loss or unauthorized disclosure of PII or other Privacy Act information.

(5) Comply with CNSSI 1010.

p. Develop and publish Army-wide orders and procedures for privileged/elevated access in accordance with Army, DOD, and national policies; update these documents as needed; and publish these documents on both the NIPRNet and SIPRNet.

q. Execute the Army's registration authority responsibilities related to issuance of PKI credentials.

r. Execute the SCA function in accordance with guidance provided by the Army CIO/G–6.

s. Issue directives for the conduct of DODIN operations and DCO–IDM to all ACOM, ASCC, Army National Guard, Army Reserve Command, DRU, Army staff and Secretariat, and other Army organizations. Commander, ARCYBER will notify the CIO/G6 upon issuing any DODIN Operations or DCO–IDM directives.

t. In coordination with the Army CIO/G–6, make quarantine or disconnect decisions.

2–21. Commanding General, U.S. Army Intelligence and Security Command

The CG, U.S. Army Intelligence and Security Command (INSCOM) will execute AO responsibility for JWICS within INSCOM and for those JWICS systems/enclaves receiving SCI services from INSCOM's Ground Intelligence Support Activity. This authority does not extend to Army Programs of Record, cross-domain solutions, non-INSCOM Quick Reaction Capabilities, or Joint SCI/SAP systems that require the Intelligence Overlay Tier C overlay and Intelligence Community enterprise systems (defined as those systems that require authorization with/through the Intelligence Community Chief Information Officer). CG, INSCOM also will execute the AO function for Army-managed, non-Program of Record SCI systems, in accordance with DNI issuances. In addition to the responsibilities in paragraphs 2–1 and 2–17, the CG, INSCOM will—

a. Participate with the Army CIO/G–6, DCS, G–2, ARCYBER, and Criminal Investigation Command in analyses and studies concerning foreign intelligence threats, criminal intelligence, and operational vulnerabilities against which cybersecurity countermeasures will be directed.

b. Serve as the AO for Army cryptologic capabilities.

c. Serve as the Army Service Cryptologic Component and point of contact for IT under the purview of the NSA that has application solely for U.S. Signals Intelligence.

2–22. Commanding General, U.S. Army Test and Evaluation Command

In addition to the responsibilities in paragraphs 2–1 and 2–17, the CG, U.S. Army Test and Evaluation Command (ATEC) will—

a. Ensure that cybersecurity responsibilities are integrated into operational and developmental testing and evaluation (T&E) for Army acquisition programs.

b. Report systemic or critical cybersecurity-related issues found during T&E activities to the ARMC.

c. Support execution of Army Interoperability Certification and System-of-Systems Network Vulnerability Assessments.

d. Provide accredited developmental and operational test data for enterprise systems and IT under consideration for Army acquisition.

2–23. Commanding General, U.S. Army Criminal Investigation Command

In addition to the responsibilities in paragraphs 2–1 and 2–17, the CG, U.S. Army Criminal Investigation Command (USACIDC) will—

a. Conduct criminal investigations of intrusions and malicious activities involving U.S. Army IT and information, to include national security offenses, data exfiltration, denial of service attacks, social engineering attacks, malicious logic, web page defacements, insider criminal activity.

b. Provide criminal and technical intelligence analyses of vulnerabilities, methodologies, tools, techniques, and practices obtained from computer crime investigations and computer forensic examinations to support cybersecurity defense activities, assessment and authorization, and program developers and managers.

c. Serve as: chief enforcer of Federal laws governing the investigation of criminal offenses; the sole entity for law enforcement investigation determinations; and the sole Army interface with Federal and civilian law enforcement agencies.

d. Provide investigative information to the Defense Cyber Crime Center or National Cyber Investigative Joint Task Force to enable proper synchronization, coordination, and technical deconfliction of investigations and operations.

e. Participate with the Army CIO/G–6, the DCS, G–2, INSCOM, ARCYBER, and 1st Information Operations Command (LAND) in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which cybersecurity countermeasures will be directed.

f. Conduct cyber-crime prevention surveys, training and unit site visits to identify cybersecurity vulnerabilities and related crime-conducive conditions.

g. Report systemic or critical cybersecurity-related issues identified during investigations or found during crime prevention surveys to the ARMC.

2–24. Army senior information security officer

Appointed by the Army CIO, the Army SISO will direct and coordinate the Army Cybersecurity Program, to include but not limited to–

a. Oversee development and dissemination of the overall cybersecurity policy for the Army.

b. Oversee the Army SCA function to include assessment of the quality, capacity, visibility, and effectiveness of cybersecurity assessments, and direct modifications as necessary.

c. Serve as the Army voting member in the DOD RMF Technical Advisory Group (TAG) and the manager for the Army section of the online Knowledge Service.

d. Develop policy to ensure that the Army cybersecurity assessment process remains consistent with DOD policy and guidance.

e. Adjudicate and resolve DODI 8510.01 process issues and concerns that cannot be resolved at the SCA level.

f. Establish priorities for assessment and authorization package processing associated with FISMA, Network Integration Evaluation and critical warfighter activities.

g. Develop qualification standards for the cybersecurity professionals responsible for conducting security assessments.

h. Oversee implementation and enforcement of DODI 8510.01 within the Army.

i. Establish and oversee the workforce of cybersecurity professionals responsible for conducting security assessments.

j. Serve as the single cybersecurity coordination point for Joint and Army-wide programs that are deploying information technologies to Army enclaves.

k. Coordinate with ASA (ALT) to integrate cybersecurity concepts into the DOD acquisition process.

l. Recommend updates and additions for NIST security controls.

m. Recommend updates and additions to the security control baselines and overlays that are published in CNSSI 1253 to the DOD RMF TAG.

2–25. Authorizing official

a. The CIO is responsible for the appointment of trained and qualified AOs for all Army information systems and platform IT (PIT) systems within their component. AOs should be selected from senior leadership positions within business owner and mission owner organizations to promote accountability in authorization decisions that balance mission and business needs with security concerns. 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 Army information systems and PIT systems under their purview in accordance with DODI 8510.01. The AO is responsible for authorizing or denying the operation (or the testing) of the assigned Army information system by issuing an authorization decision (that is, ATO, interim authority to test, and denial of ATO). The AO cannot delegate authorization decisions. (Other AO responsibilities and tasks may be delegated to formally appointed and qualified AO designated representatives.)

b. An AO reviews the security authorization package, including supporting material, and the recommendation of the security control assessor and the Army as the basis for determining risk to reach an authorization decision. An authorization decision with conditions for systems that present a risk level of high or very high can only be issued with the concurrence of the Army CIO/G–6. The AO shall provide the Army SISO a course of action for how non-compliant information systems will satisfy FISMA reporting requirements. An AO may downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2 –12.

2–26. Authorizing official designated representative

a. The authorizing official designated representative (AODR) is an organizational official who acts on behalf of an AO to coordinate and conduct the required day-to-day activities associated with the security authorization process. AOs may appoint multiple AODRs to perform different AO activities on their behalf. In accordance with DODI 8510.01, the only activity that cannot be delegated to the AODR is the authorization decision and signing of the associated authorization decision document. AODRs must complete training consistent with AO training and certification requirements. When the AO is replaced for any reason, their AODR appointments become invalid.

b. The AODR—

(1) Can be empowered by AOs to make certain decisions related to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring of POA&M implementation, and the assessment and/or determination of risk.

(2) May also be called upon to prepare the final authorization package, obtain the AO's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials.

(3) May not make the authorization decision or sign the associated authorization decision document (that is, the acceptance of risk to organizational operations and assets, individuals, other organizations, and the nation). These functions rest solely with the AO and may not be delegated.

c. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2 –14.

2–27. Security control assessor

a. The SCA holds the authority and responsibility for the assessment of all information systems and PIT systems governed by the Army Cybersecurity Program. Within the Army, the SCA function is divided into four distinct roles: SCA-Army, SCA-validator, SCA-representative, and SCA-organization. The Army SISO either performs the SCA functions or formally delegates SCA-Army activities to ARCYBER to execute for all governed information systems and PIT systems.

b. The SCA evaluates the cybersecurity capabilities and services of an Army information system or PIT system and recommends acceptance of risk or denial of ATO to the AO. This recommendation accompanies the RMF security authorization package and serves as the primary basis for the AO's authorization decision. The SCA also continuously assesses and guides the quality and completeness of RMF activities and tasks, and the resulting artifacts.

c. For a comprehensive list of duties and responsibilities, please refer to DA Pam 25–2 –14.

2–28. Information system owner

a. All Army information systems and PIT systems have an appointed ISO who holds primary responsibility for managing system procurement, development, integration, modification, operation and maintenance, life-cycle management, and disposal at the program level. The ISO is responsible for ensuring that the appropriate operational security posture is maintained. The ISO will work with AOs, information system security managers (ISSMs), information system security officers (ISSOs), and PMs to ensure compliance with DODI 8510.01 for the systems they own. The ISO will ensure the appointment of an ISSM, ISSO, and a user representative for each IT system in order to implement and maintain cybersecurity and satisfy the RMF program's requirements.

b. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2–14.

2–29. Program and system managers

a. A PM or system manager (SM) is responsible for development, production, and sustainment of a capability that meets user operational needs. Additionally, the PM/SM serves as the focal point for the integration of cybersecurity into and throughout the system life cycle.

b. For each assigned information system or PIT system, the PM/SM will appoint an ISSM with the support, authority, and resources to satisfy the responsibilities established in DODI 8510.01. The PM/SM will ensure that each program acquiring an information system or PIT system has an assigned information system security engineer who is fully integrated into the systems engineering process. The PM/SM also will ensure that the planning and execution of all RMF activities are aligned, integrated with, and supportive of the system acquisition process.

c. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2–14.

2–30. Information system security officer

a. Appointed by the PEO, PM, or commander, the ISSO is responsible for ensuring that the appropriate operational security posture is maintained for the Army information system or PIT system. The ISSO implements and enforces all DOD information system and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documents. The ISSO also ensures that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for the information systems and PIT systems under their purview, before they are granted access to those systems. This includes activities related to maintaining situational awareness and initiating actions to improve or restore a sound cybersecurity posture. The ISSO will assist the ISSM in meeting their duties and responsibilities, as well.

b. When circumstances warrant, a single individual may fulfill both the ISSM and the ISSO roles.

c. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2–14.

2–31. Information system security manager

a. ISSM roles within the Army are divided into two distinct categories: program ISSMs, who operate at the command level, where the AO resides; and organization ISSMs, who operate at the organization level, where the AO does not reside. Organization ISSMs perform similar duties to the program ISSMs at all appropriate levels of the command, including subordinate commands, posts, installations, and tactical units.

b. The ISSM acts as a technical advisor to the AO. He or she holds primary responsibility for maintaining the overall security posture of the systems within his or her organization, and is accountable for the implementation of DOD 8510.01. ISSMs develop the organization's cybersecurity program, which must address cybersecurity architecture, requirements, objectives and policies; cybersecurity personnel; and cybersecurity processes and procedures. ISSMs are also in charge of the continuous monitoring of systems within their purview to ensure compliance with cybersecurity policies. ISSMs ensure the secure configuration and approval of IT below the system level (that is, products and IT services), in accordance with applicable guidance, prior to acceptance into or connection to a DOD information system or PIT system.

c. ISSMs ensure that ISSOs are appointed in writing. They provide ISSOs direction, in accordance with DODI 8500.01, and ensure that ISSOs are following established cybersecurity policies and procedures.

d. For a comprehensive list of duties and responsibilities, please refer to the DA Pam 25–2–14.

2–32. Information system security engineer

The information system security engineer is an individual or group of people responsible for conducting information system security engineering activities, including system architecture, design, development, and configuration, that technically define a system's overall security posture. The information system owner/PM/SM will ensure that each program acquiring an information system or PIT system has an assigned information system security engineer who is fully integrated into the systems engineering process.

2–33. User representative

The Army information system user representative is the individual or organization that represents operational and functional requirements of the user community for a particular system during the RMF process. The user representative supports security controls assignment, implementation, and assessment to ensure that user community needs are met. While this role is not mandatory, it is highly recommended that it be fulfilled. The individuals within this role understand the operating environment and the system's mission criticality, reliability and survivability requirements, and so forth. As the cyber environment and its threats are constantly evolving, it is vital that the ISO and user provide input to and inform the authorization process.

2–34. All personnel

Every individual at each level is responsible for compliance with the proper practices and procedures for safeguarding information and IT. Military and civilian personnel will be considered for appropriate action if they knowingly, willfully, or negligently violate the acceptable use policy or otherwise compromise, damage, or place at risk DOD or Army information or IT by not following this regulation and the applicable DOD and Army issuances. Contractor personnel must be informed that there may be consequences if they violate Army and DOD cybersecurity policy.

2–35. Army-appointed authorizing officials

AOs are accountable for the security risks associated with the operation of IT. AOs will ensure that all activities and functions associated with security authorizations are carried out, to include but not limited to—

a. Render authorization decisions for IT under their purview, in accordance with DODI 8510.01 and Army CIO guidance.

b. Implement cybersecurity reciprocity procedures, as described in DODI 8510.01. AOs should implement reciprocal acceptance of DOD and other Federal agency and department IT ATOs to the maximum extent possible.

c. Assess and approve development and execution of POA&M to address known vulnerabilities in IT, with the support of IT threat data from PEO Simulation, Training, and Instrumentation's Threat System Management Office and the Army Research Laboratory System Lethality Analysis Directorate.

2–36. Army code signing attribute authority

The Army code signing attribute authority will issue code-signing identifiers designating organizations and individuals who are authorized to receive code-signing certificates, and ensure that such designations are kept to a minimum, consistent with operational requirements. Refer to DA Pam 25–2–13 for additional guidance regarding code-signing certificates.

2–37. Authorized users

Authorized users will—

a. Meet DOD cybersecurity awareness requirements, in accordance with DOD 8570.01–M; establish an ATCTS account prior to gaining network access; and complete and record awareness training annually.

b. Use IT only for official or authorized purposes.

c. Ensure that classified and unclassified sensitive information/CUI is only accessed, stored, and processed on IT that is formally and explicitly authorized for the classification level, caveats, and sensitivity of the information, in accordance with DODM 5200.01 and DODD 5230.11.

d. Immediately report all cybersecurity-related events (for example, unauthorized disclosure) and potential threats and vulnerabilities (for example, insider threats) to the appropriate ISSO, ISSM, and/or security manager.

e. Appropriately safeguard authenticators for accessing IT and information, such as passwords, personal identification numbers, common access cards (CACs), and other smartcards, to prevent their loss or compromise. Report the loss of CACs to the appropriate CAC issuance office in accordance with AR 600–8–14.

f. Protect terminals, workstations, other input or output devices, and resident data from unauthorized access.

g. Inform the responsible ISSO or ISSM when access to specific IT is no longer required (for example, completion of project, transfer, retirement, resignation).

h. Adhere to policies and procedures governing the secure operation and authorized use of IT, including operations security.

i. Meet the security clearance requirements in AR 380–67 for the classification level of the information processed by the IT system they are accessing.

j. Foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations may be authorized access to IT and information in accordance with DA Pam 25–2–18, Foreign Personnel Access to Information Systems and national, DOD, and Army issuances and IT security authorizations.

2–38. Privileged users and accounts

Privileged users are individuals who are authorized to perform security-relevant functions that ordinary users are not authorized to perform. Only those users who require privileged/elevated access to carry out their assigned functions are eligible to be a privileged user. The Regular Army, the Army National Guard/Army National Guard of the United States and the U.S. Army Reserve will follow all policies and responsibilities regarding privileged users. Refer to DA Pam 25–2–7 for amplifying procedures and guidance.

a. In addition to the requirements in paragraph 2–26, privileged users will—

(1) Obtain within 6 months of being appointed as a privileged user and maintain thereafter the appropriate DODD 8140.01 and DOD 8570.01–M certifications.

(2) Hold an active security clearance commensurate with the classification level of the information processed by the IT they are accessing.

(3) Review, complete, and sign (physically or digitally) a DA Form 7789 and update ATCTS accordingly prior to using privileged access. (Go to https://atc.us.army.mil.)

(4) Configure and operate IT within the authorities vested in them, in accordance with the applicable DOD and Army issuances.

(5) Use PKI credentials issued through the Army PKI registration authority for all privileged user access to NIPRNet, SIPRNet, DREN, and secure DREN systems. Alternative multifactor authentication technology may be used only when authorized by the Army CIO/G–6.

(6) Conduct DODIN operations and DCO–IDM in accordance with ARCYBER directives.

b. ISSOs or ISSMs appointed to oversee command/organization user accounts for cybersecurity programs will authorize or deny each request, then forward to the service provider for consideration.

c. For enterprise-managed system accounts, service providers will—

(1) Authorize or deny the granting of privileged/elevated access.

(2) Enforce all privileged user policies.

(3) Revoke privileged/elevated access when—

(a) User account documentation is not fully compliant.

(b) Positions and/or functions no longer require such access.

(c) Notified by the command or Army activity that such access is no longer required.

d. Command and service providers will—

(1) Monitor all personnel with privileged access to Army IT and information.

(2) Require use of PKI or other multifactor authentication to implement applicable cybersecurity controls, per DODI 8510.01.

Chapter 3
The Army Cybersecurity Program

3–1. Cybersecurity Program functions

The Army Cybersecurity Program synchronizes and standardizes cybersecurity requirements for safeguarding IT and information to support the execution of critical Army missions and essential functions. The Army must–

a. Incorporate cyber risk management principles and best practices into organization-wide strategic planning considerations, core missions, and business processes, and supporting organizational IT.

b. Integrate cybersecurity requirements into system development life-cycle processes.

c. Establish practical and meaningful boundaries for organizational information systems in order to identify what the organization is responsible for protecting. Also identify what needs to be protected under its direct control and management or within its scope of responsibilities, including people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes.

d. Correctly categorize IT in accordance with CNSSI 1253, implement the corresponding set of security controls from NIST SP 800–53 Rev. 4, and use assessment procedures from DOD Control Correlation Identifiers (CCI) and other DOD and Army guidance found on the DOD RMF Knowledge Service at https://rmfks.osd.mil.

e. Plan for the following when managing cyber risks in order to minimize the impact on DOD and Army missions and business operations.

(1) *Operational resilience.*

(a) Ensure that information resources are trustworthy by meeting trusted systems and networks requirements and best practices, in accordance with DODI 5200.44.

(b) Ensure that units are prepared for information resource degradation or loss during missions by performing developmental T&E of cybersecurity.

(c) Ensure that network operations have the means to prevail in the face of adverse events by establishing proactive protective internal defensive measures.

(2) *Interoperability.* Ensure the ability of IT to interoperate with other Army, DOD, and mission partner IT, as required.

(3) *Cyberspace.* Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DOD information networks. Cyberspace defense information will be shared with all appropriately cleared and authorized personnel in support of DOD enterprise-wide situational awareness.

(4) *Performance.* Manage mission outcomes based on strategic goals and objectives.

(5) *DOD and Army information.* Implement policies and procedures required by DOD and the Army in operational environments to minimize risk.

(6) *Identity assurance.* Verify credentials to ensure that users are authorized and in compliance with DOD standards.

(7) *Workforce.* Follow DOD guidelines to manage the workforce in accordance with cybersecurity objectives.

(8) *Cybersecurity.* Safeguard information using required protection processes to support cybersecurity objectives in line with Defense support to civilian agencies and partner-assisted missions.

(9) *Culture of accountability.* Work to execute and enforce Armywide responsibilities by aligning mission goals and standards, in accordance with cybersecurity guidelines.

(10) *Shared risk responsibility.* Manage responsibilities in a cohesive operational environment to mitigate disruptive events.

(11) *Adherence to Department of Defense and Army architectures.* Follow DOD and Army guidelines and procedures, and adhere to DODI 8510.01.

(12) *Continuous monitoring.* Maintain ongoing awareness of information and IT in order to support risk-related decisions at all tiers (the Army as an organization, mission/business processes and the IT itself). Utilize information readily available through implemented security controls.

(13) *Reciprocity.* The Army will use the DOD repository, the Enterprise Mission Assurance Support Service (eMASS) or its successor, to share security authorization packages and risk assessment data with AOs from other organizations in order to reduce redundant testing, assessment, and documentation, and the associated costs in time and resources; and to support making credible, risk-based decisions regarding the acceptance and use of systems and the information that they process, store, or transmit.

3–2. Cybersecurity governance activities

Governance provides strategic guidance, ensures that cybersecurity objectives are achieved, evaluates whether risk is managed appropriately, and verifies that enterprise resources are used effectively. Governance activities will ensure—

a. Alignment of cybersecurity objectives with mission and business strategies.

b. Understanding of the regulatory, legal, risk, environmental, and operational requirements; and that these requirements inform the management of cyber risk, policy development, and resource allocation.

c. Integration of cybersecurity considerations and requirements into processes involving strategy development, enterprise architecture, capital planning and IT portfolio management, budget oversight, workforce planning, training and education, service level agreements, supply chain risk management, mission partner relationships, traditional security and risk management programs, and inspections, audits, and investigations.

d. Army risk management and compliance processes provide for the effective management of cyber risk at the strategic, mission and business process, and IT levels, in accordance with DODI 8500.01, DODI 8510.01, and related CNSS, NIST, and DOD issuances. Baseline security controls will be developed in accordance with AR 25–30 and DA Pam 25–40. Published guidance will be posted on the Army workspace within the DOD RMF Knowledge Service (https://rmfks.osd.mil).

e. Army cybersecurity roles and responsibilities are coordinated and aligned within the Army and with mission partners.

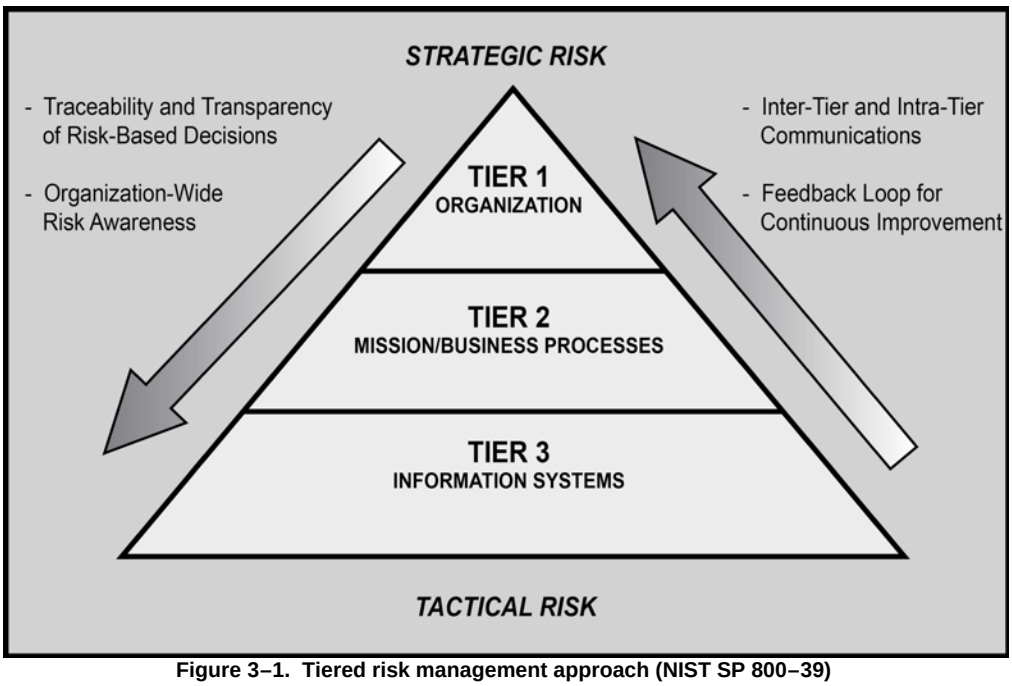

Figure 3–1. Tiered risk management approach (NIST SP 800–39)

3–3. Governance structure

The Army Cybersecurity Program leverages the multi-tiered organization-wide risk management approach defined in NIST SP 800–39 (see fig 3–1).

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 at the mission owner 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 systems, and is guided by the risk context, risk decisions, and risk activities at Tiers 1 and 2.

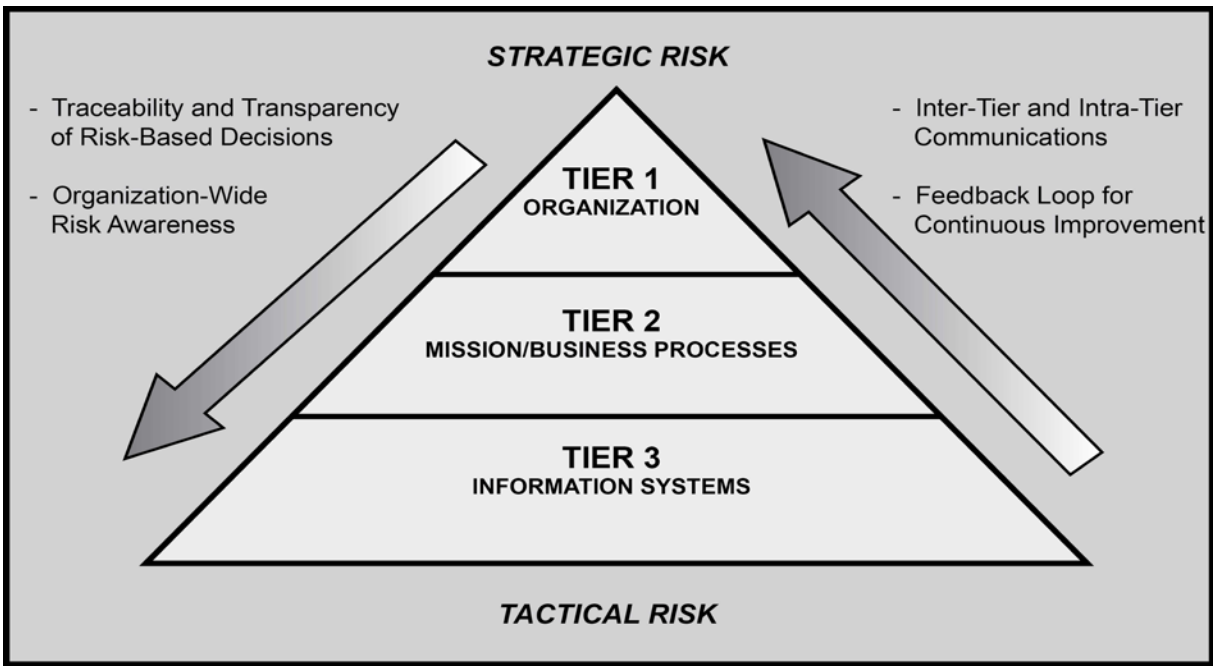

Figure 3–2. Army cybersecurity governance

3–4. Army Cybersecurity governance

The Army cybersecurity governance structure (fig 3–2) establishes the framework for how the Army will manage cybersecurity risk with respect to existing Army and DOD corporate boards and processes. The intention is to ensure that 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 or the risk management process on a regular basis. The new forums discussed below (ARMC, AO Forum, and Army Risk Management Advisory Group (ARMAG) will ensure that these topics are raised to the appropriate level, and informed decisions can be made, while engaging the cybersecurity community of interest at all levels.

a. The Army leverages existing Army and DOD governance bodies (shaded areas of fig 3–2: Army Enterprise Network Council, CIO Executive Board, Army Cyberspace Council, Army Protection Program Board of Directors, Defense Security Accreditation Working Group, RMF TAG, and so forth) to discuss cybersecurity risk topics and make organizational and mission/business area risk decisions. These governing bodies are already established and their roles and responsibilities are defined in their corresponding charters. This regulation focuses on establishing the cybersecurity bodies at Tiers 1 to 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 regulation and will be incorporated into the next version of this regulation. Army cybersecurity funding requirements and prioritization will be coordinated among the Risk Executive Function, the CIO/G–6, and the senior-level governing bodies. Army cybersecurity governance also will establish mission area principal AOs.

(1) *Information Technology Oversight Council.* The Information Technology Oversight Council is a senior review group established by HQDA and co-chaired by the Under Secretary of the Army and the Vice Chief of Staff of the Army. The Information Technology Oversight Council 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 ARMC will identify risk tolerance, accept risk that impacts the Army's mission, and recommend funding prioritization to minimize risk to the Army's mission. It will be co-chaired by CIO/G–6 and ARCYBER, and will advise the CIO/G–6. Members include representatives from Deputy Under Secretary of the Army, mission area principal AOs, the Army SISO, the Intelligence Community (represented by the DCS, G–2), the DCS, G–8, and the DCS, G–3/5/7.

(3) *Authorizing Official Forum.* The AO Forum will provide Army-appointed AOs strategic guidance and direction related to their authorities and responsibilities under the RMF, per the direction of the Army CIO/G–6 and within the terms

of the risk management strategy developed by the risk executive function and DODI 8510.01. The AO Forum will be chaired by the Army SISO; its members are the Army AOs.

(4) *Army Risk Management Advisory Group.* The ARMAG will clarify policy to support RMF implementation within the Army and issue new Army-specific cybersecurity policies to further this process. The ARMAG will coordinate issue resolution with the community of interest and elevate issues as necessary to the AO Forum. It also will produce additional policies associated with security control baselines and overlays, advise established Army forums to address RMF priorities and cross-cutting issues, and develop policy and guidance for facilitating reciprocity within the Army. The chair, who is appointed by the SISO, is an O–6/GS–15 in the CIO/G–6; this person also serves as the Army's representative to the DOD RMF TAG. Members of the ARMAG are the appointed program ISSMs and AODRs.

Chapter 4
Cybersecurity Risk Management Program

4–1. Army Risk Management Program

The Army Risk Management Program and supporting processes manage information security risk to Army operations, missions, functions, organizational assets, individuals, other organizations, mission partners, and the nation. It includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

a. The Army Risk Management Program analyzes the mission and business environment, along with IT and cybersecurity considerations, in accordance with AR 525–2. It includes—

(1) Mission analysis that identifies and prioritizes critical mission-essential functions, other operational requirements, and critical assets in order to focus Army Protection Plan priorities and resources.

(2) Risk assessments to inform risk decisions.

b. Cybersecurity issues are addressed in the development, documentation, and updating of protection plans for critical infrastructure and key resources.

c. Analysis of all IT assets is conducted to determine criticality to the organization and to prioritize mission-critical functions and dependencies.

4–2. Cyber risk management

Cyber risk is one component of the overall risk environment, and will inform organizations' risk management strategies and activities. Mission processes are defined with consideration of cybersecurity and the resulting cyber risk to organizational operations, IT assets, and users. The Army's program for managing cyber risk uses a formal risk management approach that assigns properly trained personnel to execute the Army's information risk management enterprise.

a. Cyber risk must be included in risk assessments and addressed appropriately in decision-making processes, to include strategic and operational planning, policy development, requirements development and validation, development of solutions, and resource allocation and execution.

b. Required risk management activities include—

(1) Identification and evaluation of risks associated with (i) operational, managerial, and technical IT-related vulnerabilities, (ii) threats, and (iii) the assessed potential impact of vulnerability exploitation. The threat environment to be considered will include naturally occurring threats, threats associated with global sourcing and distribution, threats from both malicious and non-malicious internal sources, and external adversarial threats to the Army's use of cyberspace in the employment of warfighting, intelligence, business, and enterprise information environment capabilities.

(2) Risk mitigation controls and countermeasures that are commensurate with the potential impact of loss of confidentiality, integrity, or availability of the potentially affected information, IT, or other assets, based on the missions they support.

(3) Determination and reporting of information systems' cyber risk posture status and compliance with applicable law, orders, policies, principles, standards, procedures, and methodologies.

4–3. Risk Management Framework

All Army IT that receives, processes, stores, displays, or transmits Army information is subject to the Army implementation of the DOD RMF assess and authorize or assess only processes, in accordance with DODI 8510.01 and the DA Pam 25–2–14 policy and procedures for assessing and managing risk per CNSS and NIST issuances. Army IT is broadly grouped as information systems, PIT, IT services, and IT products. It includes IT in tactical environments, IT that supports research, development, test, and evaluation, and Army-controlled IT operated by a contractor or other entity on behalf of the Army.

a. IT will be registered in accordance with DODI 8510.01 in the DOD-provided registry, the eMASS, or its successors. Refer to the RMF Knowledge Service at https://rmfks.osd.mil, and the Army workspace on the DOD RMF Knowledge Service for Army-specific implementation guidance.

b. All Army system and data owners must be identified in accordance with AR 25–1 and the Army Data Board. Information system and PIT authorization boundaries will be defined and recorded, in accordance with DODI 8510.01.

c. All Army IT will be categorized for impact level, and an individually tailored baseline suite of control requirements will be established, in accordance with DODI 8510.01 and CNSSI 1253. Control scoping and tailoring decisions will be made in accordance with CNSSI 1253 overlays and published guidance. Control overlay appendices to CNSSI 1253 will be applied in accordance with guidance provided by the DOD RMF Knowledge Service and the Army workspace at https://rmfks.osd.mil.

d. No Army IT will be operated in a production environment or will process real-world data without going through an assess and authorize or assess only process and obtain an authorization from the AO or other authorized official, as required by DOD policy. AOs will make risk management decisions, to include decisions to avoid, accept, or mitigate risk, and will ensure that those decisions are implemented in accordance with DA Pam 25–2–12.

e. The progression of Army IT risk management processes, including the recording of system and PIT control baseline requirements, controls designed and in place to meet those requirements (including documentation artifacts), and results of independent testing of the design and operation of controls, will be recorded in eMASS or its successor.

f. Corrective actions to address gaps within the accepted level of risk associated with IT assets will be closed in accordance with POA&M approved by the responsible AO within directed timelines.

4–4. Continuity of operations

a. The Army Continuity of Operations Program (COOP) enables the sustainment of the Army's mission-essential functions within 12 hours of, and for up to 30 days after, a disaster event before returning to normal operations, in accordance with AR 500–3. COOP is business/mission process-centric, and Army IT plays a part. Minor threats or disruptions to Army organizations and facilities that do not require relocation to an alternate site are typically not addressed by COOP planning.

b. In accordance with DODI 8510.01, CNSSI 1253, and NIST SP 800–34 Rev. 1, every Army PIT and information system will have a unique contingency plan that provides procedures to respond to system capability disruptions, from something as minor as running out of printer paper, to an event as significant as destruction of a data center.

(1) Each Army IT contingency plan will be based on a business impact analysis that catalogs and characterizes the system's components, supported mission/business processes, and interdependencies. The business impact analysis's purpose is to correlate the system with the critical mission/business processes and services provided; based on that information, characterize the consequences of a disruption; and enable prioritization and sequencing of restoration activities.

(2) The plan will address eventual, full IT restoration without deterioration of the security safeguards originally planned and implemented, and must be reviewed and approved by the appropriate personnel and roles, in accordance with DODI 8510.01.

(3) Cybersecurity personnel will—

(a) Coordinate recovery planning activities with incident handling activities.

(b) Regularly review the IT recovery plan.

(c) Update the contingency plan to address changes to the organization, IT, or environment of operation, and problems encountered during contingency plan implementation, execution, or testing. Communicate contingency plan changes to the appropriate key contingency personnel.

(d) Protect the recovery plan from unauthorized disclosure and modification.

(e) Execute disaster recovery exercises periodically and implement corrective actions based on exercise results.

(f) Coordinate disaster recovery exercises with key recovery personnel. Refer to DA Pam 25–1–2 for additional guidance on planning and conducting exercises.

(g) Report all IT incidents and implementations of the contingency plan in accordance with DA Pam 25–2–17.

4–5. Physical security

Access to and physical protection of computing facilities. Employ physical security measures (for example, access control, visitor control, physical control, testing) for network and computing facilities that process publicly releasable, sensitive, or classified information in order to restrict access to only authorized personnel with appropriate clearances and a need to know, according to AR 190–13 and AR 190–16.

4–6. Information security

All personnel will—

a. Comply with the policies of AR 380–5 for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information that requires protection in the interest of national security.

b. Protect classified IT systems and information from insider threats with the required comprehensive managerial, operational, and technical security controls.

c. Address insider threats in accordance with policy and procedures in DODD 5205.16.

d. Obtain the appropriate clearance and designation of need to know for the system or network prior to gaining access approval.

4–7. Communications security

a. The program management office and/or the system owner will implement COMSEC requirements for IT, including those integral to weapons systems and weapons support systems, throughout the IT life cycle (that is, concept definition, design and development, test and evaluation, procurement, installation, operation, maintenance, and disposal).

b. All COMSEC maintenance training must be done in accordance with applicable national, DOD, and HQDA instructions, and AR 25–12.

c. DA Pam 25–2–16 implements DODI 8523.01 DODI 8500.01, and DODI 8510.01 as they relate to communications security. It provides Army communications security guidance for all IT capabilities used in and by the Army; as well as for National Security Systems that utilize commercial products and/or architectures to protect information designated as data-at-rest and/or data-in-transit. The pamphlet also provides procedural guidance related to the policies established in this AR. It contains instructions, processes, formats, reporting requirements, and guidelines necessary to register and track all Army deployments and use of commercial solutions and equipment. All Army organizations must comply with DA Pam 25–2–16 and DODI 8523.01.

4–8. Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions

Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions (TEMPEST) denies interception and exploitation of classified, and in some instances unclassified, information by containing compromising emanations within the facility where information is being processed. PMs, or ISOs when there is no identified PM, must ensure that IT components, associated data communications, and networks are protected in accordance with national emissions standards, TEMPEST, AR 380–27, and procedures based on the security category or classification of the information.

4–9. Operations security

Operations security (OPSEC) protects critical information from adversary observation and collection in ways traditional security programs cannot. The ISSM, in coordination with the OPSEC officer, will develop and implement an OPSEC review plan as part of inspection programs, as required by AR 530–1.

4–10. Protection of information technology and information

a. Data security. On behalf of the AO, AODRs, and ISSMs will—

(1) Properly and adequately safeguard Army and DOD-originated information residing on mission partner IT, with documented agreements indicating required levels of protection.

(2) Ensure that maintenance and disposal of information on IT comply with the provisions of DODI 5015.02 and NIST SP 800–88.

(3) Ensure that qualified cybersecurity personnel are integrated into all phases of the system development life cycle.

(4) Regularly conduct, maintain, and test information backups.

(5) Protect the integrity and availability of publicly available applications and information.

(6) Ensure that information protection needs arising from mission requirements are assessed and IT processes are applied to support them.

(7) Safeguard information and records (data) in accordance with applicable NIST, DOD, and Army issuances. Required activities include--

(a) Assign all DOD and Army information in electronic format appropriate levels of confidentiality, integrity, and availability that reflect the importance of both information sharing and protection, in accordance with DODI 8510.01.

(b) Manage information and data to protect their confidentiality and integrity.

(c) Leverage processes and tools to prevent data exfiltration, mitigate the effects of data exfiltration, and maintain confidentiality and integrity of sensitive information.

(d) Leverage protective processes and tools to secure data at conception, in transit, at rest, and throughout the entire life cycle.

(e) Protect transmission of information through appropriate COMSEC measures and procedures set forth in DODI 8523.01 and applicable NIST, CNSS, DOD, and Army issuances.

1. For IT that processes classified information, use only COMSEC, CHVP, or Commercial Solutions for Classified products and services approved by the National Security Agency/Central Security Service (NSA/CSS).

2. For IT that processes sensitive information or information not approved for public release, use only COMSEC, CHVP, or Commercial Solutions for Classified products and services approved by the NSA/CSS or the National Information Assurance Partnership. This guidance recognizes that the protection of "For Official Use Only" information is necessary; however, the level of encryption does not have to meet that of classified information.

3. Protect CUI and PII using cryptographic and key management systems that comply with CNSSP No. 11.

4. Protect CUI and PII in transit and at rest, in accordance with DODI 8500.1.

5. If no listed COMSEC product meets the organization's requirement, coordinate with the Army CIO/G–6 to sponsor a product for testing that does meet the requirement. The sponsoring organization will reimburse the respective labs for costs associated with testing and evaluation.

6. Submit requests through the Army CIO/G–6 for NSA services.

7. Implement key and certificate management planning on COMSEC products and services in the Army infrastructure. This includes the handling of cryptographic keys and other related security parameters (for example, IDs and passwords) during the entire life cycle of the keys: generation, distribution, storage, accounting, establishment, and destruction.

(f) Leverage integrity-checking mechanisms in order to verify the integrity of IT and data.

(g) Separate—physically or logically—development, test, user acceptance, and production environments in accordance with DISA guidance.

(h) Deny unauthorized persons information derived from telecommunications, and ensure the authenticity of telecommunication systems.

(i) Apply security measures to communications and IT that generate, handle, store, process, or use classified or sensitive information—the loss of which would adversely affect the national security interest.

(j) Ensure that IT components, associated data communications, and networks are protected in accordance with national emissions standards, TEMPEST, AR 380–27, and procedures based on the security category or classification of the information.

b. Protective technology. On behalf of the AO, AODRs and ISSMs will manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Required activities include–

(1) Use protective technologies and perform protective activities consistent with the Army's and the organization's risk strategy to ensure the security and resilience of systems and assets.

(2) Collect and keep audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under his or her purview, and provide these data to appropriate law enforcement or other investigating agencies.

(3) Limit audit access to databases containing PII in order to ensure confidentiality while effectively implementing cybersecurity principles.

(4) Implement technology components (for example, hardware and software) that have the ability to predict, prevent, reconfigure, optimize, self-defend, and recover with little or no human intervention. Attempts made to reconfigure, self-defend, and recover may produce an incident audit trail.

(5) Use, mark, and protect authorized removable media in accordance with AR 380–5 and relevant DOD and Army guidance.

(6) Use the principle of least functionality, while enabling mission outcomes, in order to control access to systems and assets.

4–11. Access control

ISSMs will limit access to assets, systems, information, services, and associated facilities to authorized users, processes, and devices, and to authorized activities and transactions. Required activities include–

a. Actively manage the creation, deletion, use, dormancy, and deletion of system and application accounts.

b. Utilize standardized enterprise architecture and IT service management processes, with technical enforcement, in order to secure and control access to IT assets, to include information, systems, and other resources.

c. Allow only authorized access, employing the principles of least privilege and separation of duties, to users who are necessary to accomplish assigned tasks, in accordance with organizational missions and business functions.

d. Approve access permissions and monitor users to ensure that they continue to meet the requirements for their access type.

e. Track, control, and enforce the use, assignment, and configuration of administrative privileges on computers, networks, and applications through automated, technical controls to the greatest extent possible in order to prevent unauthorized use.

4–12. System and services acquisition

PMs, or ISOs when there is no identified PM, will perform, or are responsible for, the following:

a. General.

(1) Risk will be addressed as early as possible and in an integrated manner across the IT life cycle and in a visible element of IT portfolios.

(2) Require newly acquired IT products to be free of known security vulnerabilities or obtain an AO acceptance of risk or establish an AO-approved risk mitigation strategy to manage the risk to an acceptable level.

(3) Program for technology upgrades and continued support from a qualified DOD software maintainer or vendor, as necessary, to ensure continued compliance with applicable laws, NIST standards, and DOD strategic and operational risk decisions.

(4) In the case of open source or custom software, a qualified DOD software sustainment organization, such as the software centers under AMC, or vetted government contractor vendor must be engaged to properly maintain the open source components.

(5) Use of open source software must be approved by the AO with purview over the system or product, when the risk is above low. Refer to the "Assess Only" page on the DOD RMF Knowledge Service at https://rmfks.osd.mil.

(6) Use of shareware and freeware often involves significant risks and serious legal issues and is not permitted unless a documented exception is granted by the Army SISO.

(7) Ensure that all installed IT products are supported by the vendor for security patches to address publicly known security vulnerabilities.

b. Acquisition/procurement of information technology solutions.

(1) PMs, or ISOs when there is no identified PM, must develop, implement, and maintain an effective cybersecurity strategy that is consistent with DOD policies, procedures, and standards, and DA Pam 25–2–11.

(2) PMs, or ISOs when there is no identified PM, will integrate DODI 8510.01 activities with acquisition processes for all IT-enabled systems to ensure that overall system risk is determined to be acceptable according to DOD risk acceptance guidance, JCIDS key performance parameters, and NIST standards.

(3) PMs, or ISOs when there is no identified PM, must develop, implement, and maintain countermeasures that address the risks to their systems, products, and applications so as to achieve mission assurance with the lowest level of risk feasible. Countermeasures will address anti-tamper, cybersecurity, operations security, information security, personnel security, physical security, secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations, in accordance with DODI 5200.39, DODI 5200.44, and DODI 8500.01, as appropriate. The objective is to achieve an acceptable level of risk, as described in DODI 8510.01, such that the need to accept high risk is eliminated.

(4) All IT must be acquired in accordance with public law and have been evaluated and validated in accordance with appropriate NIST, DOD, and Army issuances before purchase.

(5) IT capabilities that are acquired or provided as a service must align to DOD's Information Enterprise and the Joint Information Environment, in accordance with DODI 5000.74.

c. Information technology products.

(1) *Network technologies.* The DOD Unified Capabilities (UC) Approved Products List (APL) is the authoritative list of products that have completed interoperability and cybersecurity certification. It is available at https://aplits.disa.mil. The cybersecurity tools approval process is outlined in DA Pam 25–2–2.

(a) For IT products that support UC on the Army-managed portion of the DODIN, excluding cryptologic SCI IT and classified cryptologic products, only those listed on the DOD UC APL are approved for purchase.

(b) IT products approved for purchase, that is, those listed on the DOD UC APL, must be procured through the Project Director, Computer Hardware and Enterprise Software Solutions (CHESS) contract vehicles. See the Project Director CHESS website for further information (https://chess.army.mil).

(c) Requests for exemptions to purchase IT products not on the DOD UC APL will be made in accordance with DODI 8100.04.

(d) Only the Army CIO/G–6 is authorized to approve requests for exemptions to the requirement to purchase IT products through Project Director CHESS.

(2) *Communications security products.* In addition to NIST and DOD issuances, national security systems must comply with CNSS issuances related to COMSEC.

(a) For IT that processes classified information, acquire/procure only COMSEC products and services approved by NSA/CSS.

(b) For IT that processes sensitive information or information not approved for public release, acquire/procure only security-enabled products and services approved by the NSA/CSS or those for which National Information Assurance Partnership has issued a validation certificate that meets the requirements for EAL 3 and the common criteria controlled access protection profile per CNSSP 11.

(3) If no listed product meets the organization's requirement, coordinate with the Army CIO/G–6 to sponsor a product for testing that does meet the requirement and coordinate with the National Information Assurance Partnership program office. The sponsoring organization will reimburse the respective labs for costs associated with testing and evaluation.

d. Information technical services.

(1) *Leverage existing services.* To the maximum extent practical, the PM, or ISO when there is no identified PM, should leverage existing IT services that may be shared within and among DOD components and among Federal government agencies.

(2) *Authorized cloud service providers.* Use of commercial cloud-based solutions and services that reduce the cost of IT ownership is encouraged. However, only commercial cloud service providers who obtain and maintain a DOD provisional authority for their cloud service offerings are authorized for use.

4–13. Software assurance

a. Software assurance is both the level of confidence in, and processes in place to provide assurance that, software used by the Army functions as intended and is free of intentional and unintentional vulnerabilities.

b. Army program/project/product managers (or system owners when there is no identified program, project, or product manager) will ensure, as part of supply chain risk management and through implementation of the Army's trusted systems and networks strategy (in accordance with DODI 5200.44 and the system acquisition requirements of DODI 5000.02) that risks associated with software acquired for use in Army IT are identified, evaluated, and managed prior to use and throughout the software life cycle.

4–14. Cross-domain solutions

a. A cross-domain solution is a form of controlled interface that manually or automatically adjudicates access or transfer of information between different security domains. A security domain is a system or network operating at a particular sensitivity level that implements a security policy and is administered by a single authority.

b. The AO will ensure that services that provide cross-domain capabilities, including IT systems, automated data transfers, and manual data transfers, comply with provisions outlined in DODI 8540.01, CJCSI 6211.02d, and DA Pam 25–2–1.

4–15. Identity, credential, and access management

a. Requirements for the identification, authentication, and access control of entities performing actions on Army PIT and information systems are applicable to people, non-person entities, and processes operating on their behalf. These requirements are found primarily in DODI 8510.01, CNSSI 1253, DODI 8520.02, DODI 8520.03, DoD Interim Digital Authentication Guidelines, DoD CIO IEA IdAM Portfolio Description 2.0, and the DOD CSDIP. They will be implemented in accordance with DA Pam 25–2 –13.

b. It is Army policy that all privileged users of Army PIT and information systems will use multifactor authentication to provide a heightened level of identity assurance (this includes authentication to network accounts and network infrastructure devices (routers/switches)). The Army standard and preferred solution for multifactor user authentication is hardware PKI tokens issued by the DOD PKI.

4–16. Mobility

a. A multifunction mobile device is an advanced, yet highly portable, computing platform that supports one or more compact input interfaces (for example, touch screens, stylus, and miniature keyboard) to facilitate user interaction. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. A multifunction mobile device can assume any number of form factors including, but not limited to, a smartphone, personal digital assistant, or small form factor wireless tablet.

b. The DOD CIO memo, "DOD Commercial Mobile Device (CMD) Implementation Plan," establishes policy and assigns responsibilities for the acquisition, implementation, and operation of CMD technologies for DOD operations. Additionally, the DOD CIO memo states that DOD shall institute policies and standards to ensure the secure adoption and proper use of mobile devices and related support infrastructure; and that the policies and standards shall support the fluid and dynamic nature of mobile technology, enable timely deployment, and provide a means for robust management and

control. DOD mobility governance was developed to address the roles and responsibilities assigned to the DOD components.

c. In addition, Army program/project/product managers and multifunction mobile device users will comply with specific mobility control requirements found in the CNSSI 1253 implementation of NIST SP 800–53 Rev. 4.

4–17. Monitoring

a. Continuous monitoring maintains ongoing awareness of information and IT in order to support risk-related decisions at all tiers (Army as an organization, mission/business processes, and the IT itself).

(1) ISSMs will utilize information readily available through the implemented security controls.

(2) ISSMs will monitor IT at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. All required activities must comply with NIST SP 800–137.

b. User activity monitoring supports DODIN operations and DCO–IDM. More information can be found in DODI 8530.01.

4–18. Configuration management

a. CM is a collection of activities focused on establishing and maintaining the integrity of Army IT products, PIT, and information systems through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout their life cycles. Legacy DOD policy toward CM has focused almost exclusively on change control and the operation of change control boards at the program management level. However, with DOD's adoption of the RMF and the NIST control framework, a broader view of CM has been accepted by DOD and the Army.

b. The 2008 DOD NetOps Strategic Vision cites DOD enterprise-level CM as an objective of institutionalizing network operations. The 2014 U.S. Army Network Operations Reference Architecture Version 1.0 (aligned to the DOD enterprise) describes an Army Network Operations Configuration Record Service as "the CM service that provides output information to computing and data storage services (within the common operating environment) on configuration records and the CM database."

(1) The DOD and Army envisioned CM services as going a long way toward enabling Army compliance with many of the organization-level NIST SP 800–53 Rev. 4 family of operational, managerial, and technical CM controls required by DODI 8510.01 and CNSSI 1253, as well as many other organization and system-level requirements that individual Army program/project/product managers and system owners must implement. These same requirements are reflected in eMASS, where accountability also is managed.

(2) In addition to the requirements of CNSSI 1253, DODI 8551.01 standardizes procedures to catalog, regulate, and control the use and management of protocols in the Internet protocol suite, and associated ports. The ports, protocols, and services management requirements of DODI 8551.01 are not found in eMASS, but PMs and system owners are still accountable for their implementation.

4–19. Incident response and reporting

a. An IT incident is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b. Army cyber incident reporting and handling are subject to the requirements of CJCSM 6510.01, CJCSI 6510.01, and DODI 8530.01. In addition, DOD implementation of the RMF, through the CNSSI 1253 application of the NIST SP 800–53 Rev. 4 control framework, includes an entire family of incident response requirements at the system and organization level, which are reflected, and for which accountability is managed, in eMASS.

c. CNSSI 1253 requires every PIT and information system in the Army portfolio to have a uniquely developed incident response plan tailored to the PIT or system to which it applies, and a uniquely developed contingency plan based on a business impact analysis conducted for the system. In addition, CNSSI 1253 includes specific requirements associated with incidents involving transfer of classified information onto an information system not authorized to store or process that information (spillage).

d. Program/project/product managers and system owners implement incident response and reporting requirements in accordance with DA Pam 25–2–17.

4–20. Media security

a. Media sanitization.

(1) Media sanitization is the action taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. It is the process of removing information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

(2) The policy requirement for media sanitization is found in the DODI 8510.01 requirement for the application of CNSSI 1253 to all DOD PIT and information systems. CNSSI 1253 applies NIST SP 800–53 Rev. 4 control MP–6, Media Sanitization, to all PIT and information systems in the Army IT portfolio. In addition, DODM 5200.01, Volume 3 contains specific DOD requirements for reuse and disposal of media.

(3) Program/project/product managers and system owners will implement DA Pam 25–2–8 procedures prior to media disposal, release out of organizational control, or release for reuse.

b. Reuse of computer hard drives.

(1) Media, as defined by FIPS 200, include hard drives. The policy cited above also applies to hard drive reuse.

(2) Program/project/product managers and system owners will implement DA Pam 25–2–3 guidance and procedures prior to releasing hard drives for reuse.

c. Removable media. Removable media are any type of storage media designed to be removed from a computer. This includes external hard drives, optical media (for example, CDs, DVDs), and flash media (for example, memory cards, USB flash drives, and solid-state drives). Refer to AR 380–40 to be in accordance with authorizations for removable media use and protection. Relevant DOD and Army guidance, such as ARCYBER OPORD 2017–009, Removable Media Use Within Army Networks, dated 16 October 2016, will provide further guidance.

4–21. Internet and commercial cloud service providers

a. Leverage existing services. To the maximum extent practical, the PM, or ISO when there is no identified PM, should leverage existing IT services that may be shared within and among DOD components and among Federal government agencies. See AR 25–13 for internet service provider requirements.

b. Use only authorized cloud service providers. Use of commercial cloud-based solutions and services that reduce the cost of IT ownership is encouraged. However, only commercial cloud service providers who obtain and maintain a DOD Provisional Authority for their cloud service offerings are authorized for use.

4–22. Wireless services

Wireless local area network and wireless-enabled portable electronic device technologies (for example, smartphones, tablets) must adhere to the policy requirements in DODD 8100.02 and the procedural instructions of DA Pam 25–2–9. This pamphlet provides guidance for the vetting, approval, acquisition, and use of wireless technology and wireless-enabled tools within the Army. Please refer to Army Regulations, DODI 8420.01, and DISA Wireless STIG - Version 6, Release 9.

4–23. Peripheral devices

Peripheral devices, such as printers, scanners, facsimile, and multifunction devices, are generally included within the ATO system boundary of the local area network to which they are connected. In such cases, the peripheral device is treated like any component of the hosting information system, and is subject to the same CNSSI 1253 requirements as the system that hosts the peripheral device. In cases where peripheral devices are not within the accreditation boundary of a local area network or larger system, they must either be treated as independent information systems and be granted individual ATOs prior to processing Army information, or be bundled into "type" authorizations in accordance with DODI 8510.01.

4–24. Teleworking security

a. In accordance with DODI 1035.01 the Army actively promotes and implements teleworking in support of its commitment to workforce efficiency, emergency preparedness, and quality of life. Telework facilitates the accomplishment of work; can serve as an effective recruitment and retention strategy; enhances efforts to employ and accommodate people with disabilities; and creates cost savings by decreasing the need for office space and parking facilities, and by reducing transportation costs, including costs associated with payment of transit subsidies.

b. In accordance with DODI 8500.01, telework solutions involving the use of DOD-owned, government-furnished equipment for remote access to unclassified DOD networks will comply with the requirements of applicable security controls defined in NIST SP 800–53 Rev. 4, as implemented for DOD by CNSSI 1253. Telework solutions involving the use of non-government-furnished equipment for remote access to unclassified DOD networks will be developed by Army activities that desire the capability based on the guidance provided in NIST SP 800–114, then evaluated and approved by the DOD CIO on a case-by-case basis.

4–25. Privately owned information technology

a. The use of privately owned IT (that is, Employee Owned Information Systems (EOIS)) is authorized within the Army under the following conditions-

(1) To access your own Sensitivity Level 1 PII, and Protected Health Information using a DoD Self-service Logon (DS Logon) Username and Password (UN/PW) credential from a Self-Service web portal.

(2) To access non-Self Service web-based training with a non-DS Logon UN/PW credential to access Sensitivity Level 1 data.

(3) To access Sensitivity Level 2 and 3 web-based data with Credential Strength D; credential D can use either multi-factor one-time password or PKI certificate technology solution.

b. EOIS used to access or process unclassified FOUO information (that is, official data) is restricted and only permitted with AO approval.

(1) If approved by the AO, EOIS and contractor-owned and -operated information systems, will meet all security requirements for government-owned hardware and software when managing, storing, or processing Army or DOD unclassified FOUO information, or conducting official communications or business.

(2) Cybersecurity requirements and authorized software availability for the use and safeguarding of privately owned IT will be included in security training.

c. Remote privileged access to DOD systems using privately owned IT is prohibited.

4–26. Workforce management, training, education, and certification

Provide Army personnel and partners cybersecurity awareness education and training to perform their cybersecurity-related duties and responsibilities consistent with related DOD and Army issuances. Requirements include–

a. Manage the cybersecurity workforce, as defined in DODD 8140.01. The DODD 8140.01 definition of cyberspace workforce will replace the current definition of information assurance workforce. Comply with DA Pam 25–2–6.

b. Army Civilian, military, and contracted support personnel assigned to perform cyberspace work roles will meet qualification standards established in DOD 8570.01–M, and supporting issuances, in addition to other existing workforce qualification and training requirements assigned to their billets and positions.

c. Army contracting officials will apply the Defense Federal Acquisition Regulation to contracted support designated to perform cyberspace workforce roles.

d. All authorized users of IT systems will complete initial cybersecurity awareness training as a condition of access, and thereafter must complete annual cybersecurity awareness refresher training. All users must obtain the appropriate clearance and need to know for the system or network prior to gaining access.

e. Privileged users will obtain the appropriate certification for their work role in accordance with DOD 8570.01–M and its issuances.

f. In addition to DOD-mandated cybersecurity awareness training, organizations will provide Army-specific, mission-specific, and system-specific orientation, training, awareness, and reinforcement programs to authorized users of IT, as required to comply with this regulation.

g. All Army personnel must document, monitor, update, and retain their training and certification status on ATCTS (https://atc.us.army.mil).

h. All COMSEC maintenance training must be done in accordance with applicable national, DOD, and HQDA instructions, and AR 25–12.

Chapter 5
Acceptable Use

5–1. User agreement

Authorized users will sign a user agreement (paper or electronic) prior to account activation, annually thereafter, and whenever the baseline or applicable supplemental user agreement is revised.

a. Users will sign the agreement acknowledging that they–

(1) Have read, understood, and agreed to abide by their responsibilities and the rules of behavior for IT usage and information handling, in accordance with this regulation and associated DA Pams.

(2) Have read, understood, and agreed to the notice of privacy rights, and consented to authorized monitoring and searches, in accordance with this regulation.

(3) Have read, understood, and accepted that violations of their responsibilities, unacceptable use of IT, and/or mishandling of information may be punishable by administrative and/or judicial sanctions, may result in revocation or suspension

of authorized access, may require remedial training in order to regain access, and/or may negatively influence adjudication decisions of security clearances.

b. The Army CIO/G–6 will publish the baseline user agreement and annually review and update the baseline user agreement, as required. The baseline user agreement will provide the minimum requirements that govern the appropriate use of IT and will be included in all IT user agreements.

c. Organizations may develop supplemental rules to address mission and function-specific requirements. A copy of the supplemental rules will be provided to the Army CIO/G–6. The language in the baseline user agreement will not be removed or made less stringent.

d. Organizations will track the issuance, signing, and periodic reviews of user agreements for all users under their management control. A copy of the signed acknowledgement will be added to the user's ATCTS profile.

5–2. User responsibilities and rules of behavior

All personnel, to include authorized and privileged users, will comply with their responsibilities and this regulation. These responsibilities and rules of behavior are in place to help protect the confidentiality, integrity, and availability of IT and information. Noncompliance with laws and DOD and Army regulations pertaining to the use of IT and the handling of information may raise security concerns about an individual's reliability and trustworthiness for access to IT and information.

a. Access to DOD and Army IT and information is for official use and authorized purposes only as set forth in DOD 5500.7–R or as further limited by this policy. Official use is defined as use necessary to further an Army interest or otherwise directly related to the conduct of the Army business, or having an indirect impact on the ability to conduct Army business, and includes emergency communications and communications necessary to carry out the business of the Federal government. Authorized use must not adversely affect the performance of official duties or degrade IT performance, must be of reasonable duration and frequency as determined by commanding officers and supervisors, and does not violate user responsibilities or the rules of behavior.

b. Military, civilian, and contractor personnel may be subject to administrative and/or judicial sanctions if they knowingly, willingly, or negligently compromise, damage, or place IT or information at risk by violating the user agreement. Individuals involved with the misuse of IT or prohibited activities may be subject to suspension of computer account access for a defined period of time and/or required to complete the appropriate remedial training.

5–3. Notice of privacy rights and authorized monitoring and searches

Consistent with the DOD banner and user agreement, any use of Army IT is made with the understanding that users will have no expectations as to the privacy or confidentiality of any electronic communication, including minor incidental personal uses. The Army reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on Army IT, including minor incidental personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.

Chapter 6
Compliance

6–1. Oversight and inspections

a. The Army will implement an enterprise-level approach to achieve alignment and integration of requirements for inspection and oversight of component and command traditional security (information, personnel, physical, and industrial) and cybersecurity programs in order to identify compliance trends that present unacceptable cybersecurity risk or result in inefficient use of resources. This will be accomplished by–

(1) Collecting data through automated processes whenever possible in order to limit disruption to the activities of the organization from which the information is required and support continuous monitoring objectives.

(2) Conducting vulnerability assessments, intrusion assessments, penetration testing, and other applicable activities (using internal or external capabilities) to provide a systemic view of the current IT risk posture.

(3) Leveraging data collected by existing DOD, Joint, and Army inspections, audits, investigations, and program assessments, whenever practical, to inform compliance and risk assessments.

(4) Army activities will share applicable assessment results with the ARMC, which will coordinate with Army stakeholders who have the authority to take appropriate action to resolve systemic issues and mitigate unacceptable risk. The purpose of sharing these results is not to support punitive or other negative action, but to identify and resolve systemic issues and mitigate unacceptable risk to missions and business functions. When requested, anonymity of the reporting organization will be preserved as much as possible in order to encourage reporting.

b. All IT will be assessed for interoperability and cybersecurity compliance and sustainment as part of the acquisition process. Interoperability and cybersecurity sustainment include continued alignment with current industry best practices, in particular the ability to operate with vendor-supported applications and operating systems.

6–2. Compliance reporting requirements

ACOMs will report the status of cybersecurity metrics, when directed, to ensure that leadership has useful, up-to-date information regarding the level of performance and existing gaps in the cybersecurity posture.

a. Statutory requirements for reporting information required by the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires all Federal agencies, departments, and their contractors to adequately safeguard their IT and assets. DOD must meet or exceed the standards required by OMB and the Secretary of Commerce, pursuant to FISMA and 40 USC 11331. Commanders and senior leaders of agencies and activities who have the responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of IT will ensure that IT under their purview complies with DODI 8510.01.

b. Privacy impact assessments.

(1) A privacy impact assessment will be conducted for data collection instruments that collect, maintain, use, and/or disseminate PII in an electronic form about members of the public, DOD personnel (government civilians, members of the military, and non-appropriated fund employees), contractors, or foreign nationals employed at U.S. military facilities in order to assess whether the PII is collected, stored, or disseminated in a manner that protects the privacy of individuals and their information.

(2) Privacy impact assessments will be completed in accordance with DODI 5400.16, AR 25–1, and DA Pam 25–1–1, and documented on DD Form 2930 (Privacy Impact Assessment (PIA)).

c. Cybersecurity readiness. Commanders will emphasize the importance of cybersecurity discipline within their organizations, and ensure that their organizational inspection program assesses cybersecurity readiness and compliance against higher-level risk management policy and guidance. Cybersecurity readiness assessments will be included in unit status reports.

d. Systemic or critical cybersecurity issues. Systemic or critical cybersecurity-related issues will be reported via memorandum to the Office of the Chief Information Officer/G–6 (SAIS–ZA), 107 Army Pentagon, Washington, DC 20310–0107.

e. Cyber events. Report suspected or confirmed incidents in accordance with Army regulations relevant to the specific incident, ARCYBER published procedures, applicable COOP plans (per AR 500–3), IT contingency plans (per DA Pam 25–1–2), incident response plans, and organizational policies and procedures.

Appendix A

References

Section I

Required Publications

AGO 2017–01
Assignment of Functions and Responsibilities within Headquarters, Department of the Army (Cited in para 2–7*n*(7).)

AR 25–1
Army Information Technology (Cited in para 4–3*b*.)

AR 25–13
Army Telecommunications and Unified Capabilities (Cited in para 4–21*a*.)

AR 25–30
Army Publishing Program (Cited in the title page.)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in para 2–1*m*.)

AR 190–13
The Army Physical Security Program (Cited in para 4–5.)

AR 190–16
Physical Security (Cited in para 4–5.)

AR 380–40
Safeguarding and Controlling Communications Security Material (U) (Cited in para 4–20*c*.)

AR 380–67
Personnel Security Program (Cited in para 2–1*d*(2)(*b*).)

AR 500–3
U.S. Army Continuity of Operations Program Policy and Planning (Cited in para 4–4*a*.)

AR 525–20
Information Operations (Cited in para 2–20*l*.)

AR 600–8–14
Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel (Cited in para 2–37*e*.)

ARCYBER OPORD 2012–347
Army Use of Removable Media (Cited in para 4–20*c*.) (Available at http://www.arcyber.army.mil/.)

CNSSI 1010
Cyber Incident Response (Cited in para 2–20*o*(5).) (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSP No. 11
National Policy Governing the Acquisition of Information Assurance (IA) And IA-Enabled Information Technology Products (Cited in para 4–12*a*(7)(*e*)3.) (Available at https://www.cnss.gov/.)

Cyber Threat Sharing Act of 2015
(Cited in para 2–20*k*.) (Available at https://www.congress.gov/bill/113th-congress/house-bill/624.)

DA Pam 25–1–1
Army Information Technology Implementation Instructions (Cited in para 6–2*b*(2).)

DA Pam 25–1–2
Information Technology Contingency Planning (Cited in para 4–4*b*(3)(*f*).)

DA Pam 25–2–1
Army Cross Domain Solution and Data Transfer Management (Cited in para 4–14*b*.)

DA Pam 25–2–2
Cybersecurity Tools Unified Capabilities Approved Products List Process (Cited in para 4–12*c*(1).)

DA Pam 25–2–3
Reuse of Army Computer Hard Drives (Cited in para 4–20*b*(2).)

DA Pam 25–2–6
Cybersecurity Training and Certification Program (Cited in para 4–26*a*.)

DA Pam 25–2–7
Army Information System Privileged Access (Cited in para 2–38*b*(7).)

DA Pam 25–2–8
Sanitization of Media (Cited in4-20*a*(3).)

DA Pam 25–2–9
Wireless Security Standards (Cited in para 4–22.)

DA Pam 25–2–11
Cybersecurity Strategies for Programs of Record (Cited in para 4–12*b*(1).)

DA Pam 25–2–12
Authorizing Official (Cited in para 2–25*b*.)

DA Pam 25–2–13
Identity, credential, and access management and Public Key Infrastructure Implementing Instructions (Cited in para 2–36.)

DA Pam 25–2–14
Risk Management Framework (Cited in para 2–26*b*.)

DA Pam 25–2–16
Communication Security (Cited in para 4–7*c*.)

DA Pam 25–2–17
Incident Reporting (Cited in para 4–4*b*(3)(*g*).)

DA Pam 25–2–18
Foreign Personnel Access to Information Systems (Cited in para 2–37*j*.)

DA Pam 25–40
Army Publishing Program Procedures (Cited in para 3–2*d*.)

Defense Federal Acquisition Regulation
(Cited in para 4–26*c*.) (Available at http://www.dcaa.mil/far.html.)

DISA Wireless STIG – Version 6, Release 9
(Cited in para 4–22.) (Available at http://iase.disa.mil/stigs/net_perimeter/wireless/pages/index.aspx.)

DOD CIO Memo
DOD Commercial Mobile Device (CMD) Implementation Plan (Cited in para 4–16*b*.) (Available at http://ciog6.army.mil/portals/1/policylegislation/armyitpolicydocuments/2013/army%20mobility%20strategy_26nov2013.pdf.)

DoD CIO Memo
DoD Interim Digital Authentication Guidelines (Cited in para 4–15*a*) (Available at https://www.milsuite.mil/book/docs/doc-522019.)

DOD Cybersecurity Discipline Implementation Plan (CSDIP)
(Cited in para 2–12*i*.) (Available at http://dodcio.defense.gov/portals/0/documents/cyber/cyberdis-impplan.pdf.)

DoD Information Enterprise Architecture Identity and Access Management (IdAM) Portfolio Description 2.0
(Cited in para 4–15*a*.) (Available at https://dodcio.defense.gov/portals/0/documents/diea/dod%20iea%20v2%200_volume%20ii_description%20document_final_20120806.pdf.)

DOD NetOps Strategic Vision
(Cited in para 4–18*b*.) (Available at http://dodcio.defense.gov/portals/0/documents/diea/dod_netops_strategic_vision.pdf.)

DODD 1404.10
DoD Civilian Expeditionary Workforce (Cited in para 2–1*d*(4).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5205.16
The DOD Insider Threat Program (Cited in para 4–6*c*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8100.02
Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG) (Cited in para 4–22.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8115.01
Information Technology Portfolio Management (Cited in para 2–7*e*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8140.01
Cyberspace Workforce Management (Cited in para 2–1*b*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 1035.01
Telework Policy (Cited in para 4–24*a*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5000.01
The Defense Acquisition System (Cited in para 2–2*k*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5000.74
Defense Acquisition of Services (Cited in para 4–12*b*(5).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5200.39
Critical Program Information (CPI) Identification and Protection Within Research Development, Test, and Evaluation (RDT&E) (Cited in para 4–12*b*(3).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8420.01
Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies (Cited in para 4–22.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8500.01
Cybersecurity (Cited in para 2–1*e*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Cited in para 2–1*a*(2).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling (Cited in para 2–7*k*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8520.03
Identity Authentication for Information Systems (Cited in para 2–1*a*(7).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8523.01
Communications Security (COMSEC) (Cited in para 4–7*c*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations (Cited in para 2–7*b*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8540.01
Cross Domain (CD) Policy (Cited in para 4–14*b*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8551.01
Ports, Protocols, and Services Management (PPSM) (Cited in para 2–7*jj*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODM 5200.01, Volume 4
DOD Information Security Program: Controlled Unclassified Information (CUI) (Cited in para 2–20*o*(4).) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODM 5200.02
Procedures for the DOD Personnel Security Program (PSP) (Cited in para 2–10*a*.) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

EO 13231
Critical Infrastructure Protection in the Information Age (Cited in para 1–8.) (Available at https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001–10–16-initial.pdf.)

Federal Information Security Modernization Act (FISMA) of 2014
(Cited in para 1–7.) (Available at https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.)

FIPS 200
Minimum Security Requirements for Federal Information and Information Systems (Cited in para 4–20*b*(1).) (Available at http://csrc.nist.gov/publications/pubsfips.html.)

Manual for the Operation of the Joint Capabilities Integration Development System (JCIDS)
(Cited in para 2–18*a*.) (Available at https://dap.dau.mil/policy/documents/2015/jcids_manual_with_errata_through_20151218.pdf.)

NIST SP 800–34 Rev. 1
Contingency Planning Guide for Federal Information Systems (Cited in para 4–4*b*.) (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–39
Managing Information Security Risk: Organization, Mission, and Information System View (Cited in para 3–3.) (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–53 Rev. 4
Security and Privacy Controls in Federal Information Systems and Organizations (Cited in para 3–1*d*.) (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–53A Rev. 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations (Cited in para 3–1*d*.) (Available at http://csrc.nist.gov/publications/pubssps.html.)

U.S. Army Network Operations Reference Architecture Version 1.0
(Cited in para 4–18*b*.) (Available at
http://ciog6.army.mil/architecture/tabid/146/default.aspx.)

10 USC 2223
Information Technology: additional responsibilities of Chief Information Officers (Cited in para 1–7.) (Available at http://uscode.house.gov/.)

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.

AECA
Arms Export Control Act (Available at https://www.pmddtc.state.gov/regulations_laws/aeca.html.)

AR 1–201
Army Inspection Policy

AR 11–2
Managers' Internal Control Program

AR 15–39
Department of the Army Intergovernmental and Intragovernmental Committee Management Program

AR 20–1
Inspector General Activities and Procedures

AR 25–12
Communications Security Equipment Maintenance and Maintenance Training

AR 25–22
The Army Privacy Program

AR 70–1
Army Acquisition Policy

AR 70–77
Program Protection

AR 195–2
Criminal Investigation Activities

AR 195–5
Evidence Procedures

AR 220–1
Army Unit Status Reporting and Force Registration - Consolidated Policies

AR 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–27
Control of Compromising Emanations

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

AR 525–2
The Army Protection Program

AR 530–1
Operations Security

AR 700–142
Type Classification, Materiel Release, Fielding, and Transfer

AR 735–5
Property Accountability Policies

ATP 3–39.12
Law Enforcement Investigations

CJCSI 6211.02D
Defense Information Systems Network (DISN) Responsibilities (Available at http://www.jcs.mil/library/cjcs-instructions/.)

CJCSM 6510.01B
Cyber Incident Handling Program (Available at http://www.jcs.mil/library/cjcs-manuals/.)

CNSSD 504
Directive on Protecting National Security Systems from Insider Threat (Available at https://www.cnss.gov/cnss/issuances/directives.cfm.)

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.)

CNSSI 4031
Cryptographic High-Value Products (CHVP) (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSI 7000
TEMPEST Countermeasures for Facilities (U) (Available at https://www.iad.nsa.smil.mil/resources/library/cnss_section/index.cfm. Can only be accessed on SIPRNet.)

CNSSP 7
Policy on Use of Commercial Solutions to Protect National Security Systems (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

CNSSP 12
National Information Assurance (IA) Policy for Space Systems Used to Support National Security Missions (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

CNSSP 15
Use of Public Standards for Secure Information Sharing (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

CNSSP 21
National Cybersecurity Policy on Enterprise Architecture Frameworks for National Security Systems (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

CNSSP 300
National Policy on Control of Compromising Emanations (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

DA Pam 25–403
Guide to Recordkeeping in the Army

Defense Information Systems Network (DISN) Connection Process Guide (CPG)
(Available at https://www.disa.mil/~/media/files/disa/services/disn-connect/references/disn_cpg.pdf.)

Deputy Assistant Secretary of Defense (System Engineering) Program Protection Plan
(Available at http://www.acq.osd.mil/se/docs/ppp-outline-and-guidance-v1-july2011.pdf.)

Director, Central Intelligence Agency Directives
(Available at https://www.cia.gov/library/readingroom/document/.)

DOD 5220.22–M
National Industrial Security Program Operating Manual (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DOD 5220.22–R
Industrial Security Regulation (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DOD 5400.11–R
Department of Defense Privacy Program (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DOD 8570.01–M
Information Assurance Workforce Improvement Program (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

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

DODD 5205.07
Special Access Program (SAP) Policy (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.09
Clearance of DOD Information for Public Release (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.25
Withholding of Unclassified Technical Data from Public Disclosure (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5400.11
DOD Privacy Program (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5500.07
Standards of Conduct (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 8000.01
Management of the Department of Defense Information Enterprise (DOD IE) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 1400.25 Volume 731
DOD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5000.02
Operation of the Defense Acquisition System (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5015.02
DOD Records Management Program (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5134.16
Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5134.17
Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5200.02
DOD Personnel Security Program (PSP) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5400.16
DOD Privacy Impact Assessment (PIA) Guidance (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8100.04
Unified Capabilities (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8115.02
Information Technology Portfolio Management Implementation (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8440.01
DOD Information Technology (IT) Service Management (ITSM) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8580.02
Security of Individually Identifiable Health Information in DOD Health Care Programs (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODM 5200.01, Volume 3
DOD Information Security Program: Protection of Classified Information (Available at http://dtic.mil/whs/directives/corres/pub1.html.)

EO 12333
United States Intelligence Activities (Available at https://www.archives.gov/federal-register/codification/executive-order/12333.html.)

EO 13556
Controlled Unclassified Information (Available at https://www.federalregister.gov/executive-orders.)

FIPS 140–2
Security Requirements for Cryptographic Modules (Available at http://csrc.nist.gov/publications/pubsfips.html.)

Intelligence Community Directives (ICD)
(Available at https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.)

Joint Information Environment Security Architecture
(Available at http://www.disa.mil/~/media/files/disa/about/jie101_000.pdf.)

JP 1–02
Department of Defense Dictionary of Military and Associated Terms (Available at http://dtic.mil/doctrine/new_pubs/jointpub.htm.)

JP 3–12(R)
Cyberspace Operations (Available at http://dtic.mil/doctrine/new_pubs/jointpub.htm.)

JP 6–0
Joint Communication Systems (Available at http://dtic.mil/doctrine/new_pubs/jointpub.htm.)

NIST SP 800–14
Generally Accepted Principles and Practices for Securing Information Technology Programs (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–30 Rev. 1
Guide for Conducting Risk Assessments (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–37 Rev. 1
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–88 Rev. 1
Guidelines for Media Sanitization (Available at http://csrc.nist.gov/publications/pubssps.html.)

NIST SP 800–137
Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Available at http://csrc.nist.gov/publications/pubssps.html.)

NSA/CSS (National Security Agency/Central Security Service) Manuals
(Available at https://www.nsa.gov/news-features/declassified-documents/nsa-css-policies/.)

NSTISSP No. 101
National Policy on Securing Voice Communications (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

RMF Knowledge Service
(Available at https://rmfks.osd.mil/rmf/general/securitycontrols/pages/commoncontrols.aspx.)

10 USC 2222
Defense business systems: business process reengineering; enterprise architecture; management (Available at http://uscode.house.gov/.)

22 USC 2551
Congressional statement of purpose (Available at http://uscode.house.gov/.)

29 USC 791
Employment of individuals with disabilities (Available at http://uscode.house.gov/.)

29 USC 794
Nondiscrimination under Federal grants and programs (Available at http://uscode.house.gov/.)

29 USC 794d
Electronic and information technology (Available at http://uscode.house.gov/.)

40 USC Subtitle III, Chapter 113
Responsibilities for Acquisitions of Information Technology (Available at http://uscode.house.gov/.)

40 USC 11315
Agency Chief Information Officer (Available at http://uscode.house.gov/.)

40 USC 11331
Responsibilities for Federal information systems standards (Available at http://uscode.house.gov/.)

44 USC, Chapter 35
Coordination of Federal Information Policy (Available at http://uscode.house.gov/.)

44 USC 3555
Annual Independent Evaluation (Available at http://uscode.house.gov/.)

Section III

Prescribed Forms

DA Form 7789
Privileged Access Agreement and Acknowledgement of Responsibilities (Prescribed in para 2–1*c*(3).)

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (http://armypubs.army.mil.)

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2875
System Authorization Access Request (SAAR)

DD Form 2930
Privacy Impact Assessment (PIA) (Available at http://www.esd.whs.mil/directives/forms/.)

Appendix B

Internal Control Evaluation

B–1. Function

The function covered by this checklist is the administration of Army cybersecurity in information management and IT organizations.

B–2. Purpose

The purpose of this checklist is to assist HQDA, ACOMs, ASCCs, DRUs, PEOs, PMs, and installations in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.

B–3. Instructions

Answers must be based on the actual testing of internal controls (such as document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions

a. Have appropriate security personnel (for example, ISSMs) been appointed?

b. Have risk analyses been performed for systems that process, access, transmit, or store Army information?

c. Are the appropriate leadership and management personnel aware of the results of risk analyses and risk assessments?

d. Have security assessments been performed per standard Army methodologies, as detailed in this regulation, to ensure consistency?

e. Does the organization understand the cyber risk to organizational operations?

f. Is access to assets and associated facilities limited to authorized users?

g. Have the organization's personnel and partners been provided cybersecurity awareness training?

h. Does the organization ensure that its technical security solutions are consistent with policy and procedures?

i. Is anomalous activity detected in a timely manner and its potential impact on systems clearly understood?

j. Are response processes in place and adequately maintained to ensure timely response to detected cybersecurity events?

k. Is there a plan in place to ensure response activities will be coordinated with internal and external stakeholders, to include external support from law enforcement?

l. Are recovery planning and processes continuously evaluated for relevance and improvement?

B–5. Supersession

No supersession.

B–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to Army Chief Information Officer/G–6 (SAIS–CB), 107 Army Pentagon, Washington, DC 20310–0107 (army.ciog6.policy-inbox@mail.mil).

Glossary

Section I

Abbreviations

ACOM
Army command

ACSIM
Assistant Chief of Staff for Installation Management

AGO
Army General Order

AMC
Army Materiel Command

AO
authorizing official

AODR
authorizing official designated representative

APL
Approved Products List

AR
Army Regulation

ARCYBER
Army Cyber Command

ARIMS
Army Records Information Management System

ARMAG
Army Risk Management Advisory Group

ARMC
Army Risk Management Council

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASA (FM&C)
Assistant Secretary of the Army (Financial Management & Comptroller)

ASCC
Army service component command

ATCTS
Army Training and Certification Tracking System

ATEC
Army Test and Evaluation Command

ATO
authorization to operate

CAC
common access card

CCI
controlled cryptographic item

CDS
cross-domain solution

CG
commanding general

CHESS
Computer Hardware and Enterprise Software Solutions

CHVP
cryptographic high-value product

CIO/G–6
Chief Information Officer

CJCSI
Chairman of the Joint Chiefs of Staff

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CJCSM
Chairman of the Joint Chiefs of Staff Manual

CM
configuration management

CMD
commercial mobile device

CNSS
Committee on National Security Systems

CNSSD
Committee on National Security Systems Directive

CNSSI
Committee on National Security Systems Instruction

CNSSP
Committee on National Security Systems Policy

COMSEC
communications security

COOP
Continuity of Operations Program

COTS
commercial off-the-shelf

CSDIP
Cybersecurity Discipline Implementation Plan

CUI
controlled unclassified information

DCO–IDM
defensive cyberspace operations - internal defense measures

DCS
Deputy Chief of Staff

DD
Department of Defense (form)

DISA
Defense Information Systems Agency

DNI
Director of National Intelligence

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODIN
DOD information network

DODM
Department of Defense manual

DREN
Defense Research and Engineering Network

DRU
direct reporting unit

DS LOGON
DOD self-service logon

EIEMA
Enterprise Information Environment Mission Area

EIOS
Employee owned information system

eMASS
Enterprise Mission Assurance Support Service

EO
executive order

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act of 2014

GS
general schedule

HQDA
Headquarters, Department of the Army

IC
intelligence community

INSCOM
Information Security Command

ISO
information system owner

ISSM
Information System Security Manager

ISSO
Information System Security Officer

IT
information technology

JCIDS
Joint Capabilities Integration Development System

JWICS
Joint Worldwide Intelligence Communications System

KMI
key management infrastructure

NIPRNet
non-classified internet protocol router network

NIST
National Institute of Standards and Technology

NIST SP
National Institute of Standards and Technology Special Publication

NSA
National Security Agency

NSA/CSS
National Security Agency/Central Security Services

NSTISSP
National Security Telecommunications and Information Systems Security Policy

OMB
Office of Management and Budget

OPSEC
Operational Security

Pam
Pamphlet

PD
position designation

PEO
Program Executive Office

PII
personally identifiable information

PIT
Platform Information Technology

PKI
Public Key Infrastructure

PM
program manager

POA&M
plan of action and milestones

RMF
risk management framework

RRS–A
Records Retention Schedule-Army

SAP
Special Access Program

SCA
Security Control Assessor

SCI
sensitive compartmented information

SIPRNet
secure internet protocol router network

SISO
senior information security officer

SM
system manager

SP
special publication

SRG
security requirements guide

SSE
systems security engineering

STIG
Security Technical Implementation Guide

T&E
test and evaluation

TAG
Technical Advisory Group

TEMPEST
Telecommunications Electronics Materiel Protected from Emanating Spurious Transmissions

TRADOC
Training and Doctrine Command

UC
Unified Capabilities

UCDMO
Unified Cross-Domain Management Office

UCMJ
Uniform Code of Military Justice

UN/PW
Username/password

USACIDC
U.S. Army Criminal Investigation Command

USC
United States Code

Section II

Terms

Acceptable Use
Outlines the acceptable use of computer equipment within a DOD/Army organization.

Authenticator
The value or data object (for example, a password, a biometric template, or a cryptographic key) used to prove the claimant possesses and controls the identity credential. Assertion-based authenticators (that is, a personal identification number, a password, or a passphrase) are data with no associated physical characteristics or device. Cryptographic-based authenticators are cryptographically generated data or keys (usually only machine-readable) carried or stored on a physical device, such as the cryptomodule on a smartcard. Defined in DODI 8520.03.

Authorized user
Any appropriately cleared individual required to access IT to carry out or assist in a lawful and authorized governmental function. Authorized users include DOD employees, contractors, and guest researchers.

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. Defined in CNSSI 4009.

Capability
Defined in DODI 8115.02.

Commercial solutions for classified
A commercial off-the-shelf (COTS) end-to-end strategy and process in which two or more COTS products can be combined into a solution to protect classified information.

Compilation
An aggregation of preexisting items of information. Pursuant to DODM 5200.01 Volume 1, compilations of information that are individually unclassified (or classified at a lower level) may be classified (or classified at a higher level) if the compiled information reveals an additional association or relationship that qualifies for classification and is not otherwise revealed by the individual elements of information.

Cryptographic High–Value Product
NSA-approved products incorporating only UNCLASSIFIED components and UNCLASSIFIED cryptographic algorithms. This includes COTS products approved by the NSA, but does not include composed commercial solutions or their components, unless an individual component has been approved as a CHVP. Un-keyed CHVPs are not classified or designated as a CCI.

Cyber Events
Any observable occurrence in a system and/or network.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communications, and electronic communications, including information contained therein, to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation. Defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

Cybersecurity Architecture
Consists of strategies, standards, and plans that have been developed for achieving an assured, integrated, and survivable information enterprise. Defined in DOD Instruction 8510.01.

Cybersecurity Service Provider
An organization that provides one or more cybersecurity services to implement and protect the DODIN. Defined in DOD Directive 8530.01.

Cybersecurity Workforce
Develops and maintains a trained and qualified cybersecurity workforce by providing a continuum of learning from basic literacy to advanced skills, recruiting and retaining highly qualified professionals, and keeping workforce capabilities current in the face of constant change.

Cyberspace
A global domain within the information environment.

Cyberspace operations
The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Defined in JP 1–02.

Defensive cyberspace operations – internal defense measures
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Defined in JP 1–02.

Department of Defense information network operations
Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks in order to create and preserve information assurance on those information networks. Defined in JP 1–02.

Electronic communication
The transfer of information (signs, writing, images, sounds, or data) transmitted by computer, phone, or other electronic device. Electronic communication includes, but is not limited to: text messages, emails, chats, instant messaging, screensavers, blogs, social media sites, electronic device applications, and web/video conferencing.

Incident response
Actions conducted to resolve information systems security incidents, restore systems to operational status, and provide technical and administrative corrections to protect systems from further attacks.

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. Defined in 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 that: 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Information technology life cycle
The IT life cycle: concept definition, design and development, test and evaluation, procurement, installation, operation, maintenance, and disposal.

Insider threat
The threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Defined in DODD 5205.16.

Intrusion
Unauthorized act of bypassing the security mechanisms of a system.

Key management
The activities involving the handling of cryptographic keys and other related security parameters (for example, passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.

Mission partners
Those with whom DOD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations and other nations, multinational organizations, non-governmental organizations, and the private sector. Defined in DODD 8000.01.

Operating environment
The environment in which users run application software.

Portfolio management
The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.

Principle of least functionality
Helps to minimize the potential for introduction of security vulnerabilities and includes, but is not limited to: disabling or uninstalling unused/unnecessary operating system functionality, protocols, ports, and services; and limiting the software that can be installed and the functionality of that software.

Principle of least privilege
Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of IT.

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. Defined in CNSSI 4009.

Risk Management Framework
The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (NIST SP 800–53 Rev. 4)

Safeguard
Protection included to counteract a known or expected condition. Incorporated countermeasure or set of countermeasures within a base release.

Service provider
An organization that provides one or more cybersecurity services to implement and protect the DODIN.

System owner
Person or organization that has responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

Systemic issue
Systemic issues normally include functional systems, such as personnel and logistics, and tend to surface through a general pattern of noncompliance throughout the various echelons of a command. The problems are often beyond the ability of local commanders to solve, so something may be wrong with the system.

User activity monitoring
The technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Defined in CNSSI 4009.