Department of the Army
Pamphlet 25–2–12

Information Management: Army Cybersecurity

Authorizing Official

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–12
Authorizing Official

This new publication, dated 8 April 2019—

- Establishes roles and duties of Army authorizing officials and outlines duties associated with risk decisions and management under the Risk Management Framework (para 2–3).

- Provides the nomination and appointment process and instructions for Army authorizing officials under the Risk Management Framework construct (paras 3–1 and 3–3 through 3–6).

- Issues position requirements as well as training and certification requirements for nomination as an Army authorizing official (para 3–2).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–12

Information Management : Army Cybersecurity

Authorizing Official

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 a new Department of the Army pamphlet.

Summary. This pamphlet provides requirements and guidelines for authorizing official nomination, appointment process, roles and duties, and the training and certification requirements for authorizing officials within the Department of Army. This pamphlet implements AR 25–2.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Authorizing official appointment for systems that process sensitive compartmented information or signals intelligence are outside of the scope of this pamphlet.

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

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

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

Contents (Listed by paragraph and page number)

Contents—Continued

Chapter 1
Introduction

1–1. Purpose
DODI 8500.01 requires appointment of an authorizing official (AO) for DOD information systems (ISs) and platform information technology (PIT) systems to ensure all DOD IS and PIT systems under their purview are authorized in accordance with DODI 8510.01. AR 25–2 authorizes the Army Chief Information Officer (CIO) to appoint AOs on behalf of the Secretary of the Army. This pamphlet defines the nomination and appointment process, including the training and certification requirements that an AO must meet prior to nomination, and the AO duties once appointed. AO appointment for systems that process sensitive compartmented information or signals intelligence are outside of the scope of this pamphlet.

1–2. References and forms
See appendix A.

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

Chapter 2
Roles and Duties

2–1. Army Chief Information Officer
In addition to the responsibilities listed in AR 25–2, the Army CIO delegates the authority for AO appointment to the Army Deputy CIO/G–6. The Army Deputy CIO will remain cognizant of and accountable for any and all actions taken pursuant to this delegation and will comply with DOD and Federal Information Security Modernization Act (FISMA) of 2014 requirements in appointing AOs for systems under their purview.

2–2. Army Senior Information Security Officer
The Army SISO, with regard to AOs—

a. Implements the Risk Management Framework (RMF) policy on behalf of the CIO/G–6.

b. Receives and processes Army AO nominations.

c. Updates the authorizing official-repository (AO–R) within 5 working days after receipt of all required information supporting a nomination, when appropriate.

d. Recommends appointment of Army AOs to the Army DCIOwhen required. When the information system owner (ISO) employs another government organization to develop their capability, the ISO's AO remains the AO for the IS or PIT system under development. The contractual requirements should include a statement that requires the delivered system to meet the RMF requirements.

2–3. Authorizing official duties
AOs are accountable to the DOD, the Army, and the public for operating secure ISs. Each AO must weigh the operational need for IS or PIT system capability against the need to protect the information and the information environment. Protecting the information environment includes the other mission and business functions reliant on the shared information environment.

a. For ISs or PIT systems under their purview, the AO, when appropriate—

(1) Identifies and includes cybersecurity requirements throughout the lifecycle of systems, to include acquisition, design, development, developmental testing, operational testing, integration, implementation, operation, upgrade, or replacement.

(2) Appoints qualified individuals to cybersecurity positions, to include the program information systems security manager (P–ISSM).

(3) Ensures oversight of cybersecurity related functions.

(4) Evaluates mission, business case, and budgetary needs with consideration of the security and operational risks.

(5) Reviews and approves the system security plan submitted by the ISO. By approving the security plan, the AO agrees to the system categorization (confidentiality, integrity, and availability levels), the set of security controls proposed to meet the security requirements for the system, and the adequacy of the system-level continuous monitoring strategy.

(6) Reviews and approves the cybersecurity strategy for program of record systems under their purview.

(7) Renders authorization decisions based on consideration of the security control assessor-Army (SCA–A) recommendation and risk assessment which includes a determination of the IS's vulnerabilities, the likelihood of the vulnerabilities being exploited, and the impact to the Army mission if exploited.

(8) Reviews the authorization to operate (ATO) with conditions and updates plans of action and milestones (POA&Ms) for ISs or PIT systems with a risk level of very high or high within 6 months of the authorization date and ensures implementation.

(9) Remains accountable for continued operations of ISs under their purview at an acceptable level of risk.

(10) Approves the system continuous monitoring strategy and ensures an acceptable level of residual risk is maintained through the use of the system-level continuous monitoring strategy.

(11) Manages the timely update and execution of system-level POA&Ms.

(12) Ensures IS or PIT system authorization statuses are current in the Army Portfolio Management Solution (APMS).

(13) Ensures that the Army instances of the Enterprise Mission Assurance Support Service (eMASS) are used to implement the RMF process for all ISs or PIT systems under their purview.

(14) Reviews the results of the annual assessment, documented in the security assessment report (SAR), which will recommend no change to the authorization status, downgrade to a denial of authorization to operate (DATO), or continue operations.

(15) Revisits and revises the authorization decision or authorizes continued operations based in part on the annual assessment recommendation in the SAR.

(16) Ensures POA&Ms are updated based on the results of the annual assessment and as the cybersecurity posture changes.

(17) Provides a course of action to the Army SISO on how noncompliant ISs or PIT systems under their purview will satisfy the FISMA reporting requirements.

b. The decision to operate an IS or PIT system at an acceptable level of residual risk is determined and documented by the AO in the authorization approval. Authorization decisions rely, in part, on the SCA–A risk assessment and recommendation provided in the SAR. The SAR captures the SCA–A determination of the operational risk introduced through deployment of the IS or PIT system.

c. Accreditation under the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is not provided for new capabilities or those with expired DIACAP accreditations. All existing DIACAP authorizations will expire no later than the end of fiscal year (FY) 2018. Beyond FY 2018, all authorizations will be under the RMF.

d. Once the IS or PIT system is authorized, the AO records the authorization decision in the authorization decision document, which becomes part of the security authorization package that is maintained in eMASS.

e. The AO may authorize or deny operations in the form of an ATO, interim authorization to test (IATT) or a DATO.

(1) Grant an ATO if overall risk is determined to be acceptable and there are no noncompliant controls with a level of risk of very high or high. The ATO must specify an authorization termination date that does not exceed three years from the authorization date.

(2) A one-year ATO with conditions may be granted under limited circumstances, when noncompliant controls with a risk level of very high or high exist that cannot be immediately corrected or mitigated, but overall system risk is determined to be acceptable due to mission criticality. An ATO with conditions for ISs or PIT systems with a risk level of high or very high can be issued only with concurrence of the Army CIO that the security risk of continued system operation is acceptable due to mission criticality. The Army CIO will coordinate with U.S. Army Cyber Command (ARCYBER) concerning any system that introduces a very high or high risk level to determine under what conditions such an IS or PIT system may operate if it is determined that the system must be allowed to operate due to mission criticality. AOs will review the ATO with conditions and updated POA&M within 6 months of the authorization date. AOs must ensure implementation of the updated POA&M. Continued operation after one year with a level of risk of very high or high requires a new decision from the Army CIO. The ATO with conditions must specify an AO review period that is within 6 months of the authorization date.

(3) Grant an IATT only when an operational environment or live data is required to complete specific test objectives (for example, when replicating certain operating conditions in the test environment is impractical) and expiring at the completion of testing (normally for a period of less than 90 days). Operation of an IS under an IATT in an operational environment is for testing purposes only.

(4) An ATO (rather than an IATT) is required if operational testing and evaluation is being conducted in the operational environment or on deployed capabilities.

(5) Issue a DATO when the operational risk is determined to be unacceptable. If the system is operational when the AO issues a DATO, stop operations and terminate network connections immediately. When decommissioning a system, issue a DATO and update APMS and eMASS as appropriate.

(6) An AO may downgrade or revoke an authorization decision at any time if risk conditions or concerns so warrant.

f. When there is a transfer of AO responsibilities and duties, for whatever reason, the incoming AO should review all risk decisions from the previous AO. The incoming AO will assume the risk previously accepted by the prior AO.

Chapter 3
Nomination Requirements

3–1. Minimum nomination requirements

The CIO/G–6 will appoint an AO for each IS operating within or on behalf of the Department of the Army when appropriate.

a. To be nominated as an AO, the individual must—

(1) Be a U.S. citizen.

(2) Be a DOD official.

(3) Be a general officer (GO), senior (Federal) official, senior executive service (SES), or equivalent.

(4) Be in a position to assume formal responsibilities for operating Army ISs or PIT systems at an acceptable level of risk to organizational operations (to include mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

(5) Have a level of authority commensurate with accepting, in writing or through DOD public key infrastructure-certified digital signature, the risk of operating the IS.

(6) Hold a U.S. Government security clearance and formal access approvals commensurate with the level of information processed by the system under their jurisdiction, or a secret clearance, whichever is higher.

(7) Be trained and certified as required in this pamphlet (see para 3–2).

b. Once appointed by the Army CIO, the AO authority will not be further appointed or delegated, except as provided in this pamphlet.

c. Submit requests to waive the requirements in this DA Pam with justification to the Army SISO through the Headquarters, Department of the Army (HQDA) CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil.

3–2. Training and certification requirements

a. Prior to nomination, the nominee must complete the DOD-required AO computer based training (CBT) accessible on the Information Assurance Virtual Training Center located at https://iatraining.us.army.mil. Ensure the certificates of completion are available on the AO's profile in the Army Training and Certification Tracking System (ATCTS) at https://atc.us.army.mil.

b. The Army AO CBT meets the DOD AO certification requirement. AOs must retake the DOD AO CBT every 3 years and the upload the latest certificate of completion to the AO's profile in ATCTS at https://atc.us.army.mil.

c. AOs are required to take the DOD eMASS AO CBT located at https://disa.deps.mil/ext/cop/mae/netops/emass/sitepages/home.aspx. Ensure the certificate of completion and DD Form 2875 (System Authorization Access Request (SAAR)) are available in ATCTS and submit a request for an account to the Army eMASS manager, at usarmy.huachuca.netcom.mbx.emass-helpdesk@mail.mil.

d. AOs must register in the Army instances of eMASS on both the Nonclassified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET), if applicable, prior to commencement of any AO RMF activities. The Army NIPRNET eMASS instance is located at https://emass-army.csd.disa.mil. The Army SIPRNET eMASS instance is located at https://emass-army.csd.disa.smil.mil.

3–3. Nomination and appointment process

Prior to consideration for AO appointment, the P–ISSM (formerly known as the information assurance program manager) will submit a nomination request via digitally signed email to the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil.

a. Appointment requests must include the following information:

(1) Name and title of the person submitting the nomination.

(2) The nominee's full name, rank/grade, title within the organization, and email address (NIPRNET and SIPRNET).

(3) Relationship of the nominee to the ISs or PIT systems. For example, "The listed ISs are under the purview of (add nominee's name) as part of their responsibilities as (add position)."

(4) Statement of compliance with AO requirements as documented in paragraphs 3–1 and 3–2.

(5) Clearance level.

(6) Highest system classification level.

(7) List of the ISs or PIT systems names, acronyms, and associated APMS numbers for which appointment is being requested. Ensure the acronyms and names are consistent with APMS.

(8) Statement validating the AO's training and certificate of completion are current and uploaded to ATCTS at https://atc.us.army.mil.

b. Upon receipt of the nomination, the Army SISO team will process the request as follows:

(1) A "reply all" to the email nomination with an acknowledgment email accepting the action.

(2) Verify certifications have been completed and are available in ATCTS.

(3) Update the AO–R. The AO–R is the official resource for Army AOs and is available on the DOD RMF Knowledge Service, in the Army Workspace on the Army policy page at https://rmfks.osd.mil/rmf/collaboration/component%20workspaces/usarmyce/pages/default.aspx.

c. The Army SISO will send an AO appointment via digitally signed email that includes acknowledgment of the AO–R update.

d. The AO will upload the Army appointment email message to ATCTS.

3–4. System additions/deletions for currently appointed authorizing officials

a. The P–ISSM will send a system add and/or delete request via digitally signed email to the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil that includes the following information:

(1) Name and title of person submitting the request.

(2) Name, title, and certification status of the current CIO/G–6 appointed AO.

(3) Relationship of the AO to the added and/or deleted systems. For example, "The listed ISs are under/no longer under the purview of (add AO's name) as part of their responsibilities as (add position)."

(4) The system name, acronym, and APMS number of the systems to be added or deleted. Multiple systems can be included in one request.

(5) The status of the system in APMS. (For example, "This system has been added/removed/decommissioned in APMS and the effective date of the change.")

b. The cognizant AO will be copied on the request.

c. The HQDA CIO/G–6 RMF team will send an acknowledgment email accepting the action.

(1) The certification status will be validated.

(2) The AO–R will be updated.

(3) "Reply all" to the request will be sent via email acknowledging the AO–R has been updated to include the requested additions/deletions.

3–5. Transfer of authorizing official duties

Transfer of AO duties can occur when an AO rotates out of the position, responsibilities are realigned, or when ISs or PIT systems are transferred from one AO to another under life cycle functions. The transfer requirements are the same for each transfer scenario and include the following:

a. Immediately upon notification of the change, the P–ISSM will send a digitally signed email to the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil that includes the following information:

(1) Name and title of person submitting the request.

(2) Name and title of the current AO.

(3) Name, title, and email address (NIPRNET and SIPRNET) of the receiving AO.

(4) Relationship of the incoming/receiving AO to the systems.

(5) Reason for the transfer.

(6) System name, acronym, and APMS number of IS or PIT systems being transferred.

(7) Statement validating the receiving AOs certifications are current and uploaded to ATCTS, located at https://atc.us.army.mil.

(8) The status of the system in APMS when appropriate. For example, "This system has been transferred from (add organization name) to (add organization name) in APMS on (add date)."

b. Both AOs will be copied on the transfer email submitted by the transferring organization.

c. The SISO team will send an acknowledgment email with acceptance of the action.

(1) The AO certification status will be validated.

(2) The AO–R will be updated.

(3) A "reply all" to the request will be sent via email acknowledging the AO–R had been updated to reflect the transfer.

3–6. Decommission

The AO's responsibilities and duties end when the IS or PIT system is decommissioned or removed from service.

a. Immediately upon notification of the change, the P–ISSM will send a digitally signed email to the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil that includes the following information:

(1) Name and title of person submitting the request.

(2) Name and title of the current AO.

(3) System name, acronym, and APMS number of system to be decommissioned.

(4) The status of the system in APMS. For example, "This system has been decommissioned in APMS."

b. The SISO team will send an acknowledgment email with acceptance of the action.

(1) The AO–R will be updated.

(2) A "reply all" to the request will be sent via email acknowledging the AO–R has been updated to remove the decommissioned system.

(3) The AO appointment for the decommissioned IS is considered rescinded when the AO–R is updated.

c. The system decommissioning strategy and the updated security plan is uploaded to eMASS.

Chapter 4
Supporting Roles

4–1. Authorizing official designated representative

AOs may appoint members of their staff, in writing or by digitally signed email, as authorizing official designated representatives (AODRs) to perform day-to-day AO activities if they so desire.

a. AOs may appoint multiple AODRs to perform different AO activities on their behalf. When the appointed AO is replaced for any reason, the AODR appointment(s) becomes invalid.

b. AOs will define the specific day-to-day activities being authorized in the AODR appointment. AODRs are not authorized to make the ATO, IATT, or DATO risk decisions on behalf of the AO.

c. Prior to appointment, AODRs must complete AO CBT, and maintain certification in accordance with this pamphlet, consistent with the AO training and certification requirements in paragraph 3–2. Ensure certificates of completion are uploaded to ATCTS in the AODR's profile.

d. Forward AODR appointments to the Army SISO via the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil, and to the AO supporting P–ISSM.

e. The SISO team will update the AO–R to reflect the AODR for the specific AO.

f. The P–ISSM will provide the AODR appointment to all applicable ISOs, Network Enterprise Centers, and RMF team members.

g. AOs will not designate the AO risk acceptance decision and/or authorization to anyone including the AODR. Only the appointed AO can perform this function. The AO is not authorized to further appoint or delegate this function.

h. The appointed AO remains accountable for all AO functions, even when duties have been delegated.

i. The AODR working closely with the AO supporting P–ISSM will establish and document routine processes and procedures to ensure that the appointed AO is knowledgeable of the cybersecurity posture and any issues that impact the security posture of systems under their purview.

j. Do not appoint system owners as AODRs for ISs or PIT systems under their purview.

4–2. Authorizing official-repository

The AO–R is the authoritative resource for AO identification within the Army and is available on the Army Workspace on the DOD RMF Knowledge Service on the Army policy page at https://rmfks.osd.mil/rmf/collaboration/component%20workspaces/usarmycw/pages/default.aspx. The AO–R captures the IS or PIT system name, acronym and associated APMS number, the appointed AO, and the certification date. It also captures the contact information for the P–ISSM supporting the AO and the AODR as appropriate.

4–3. Army Chief Information Officer/G–6 representative

The Army SISO is the Army CIO/G–6 representative in the AO appointment process. Send all AO nominations to the Army SISO through the HQDA CIO/G–6 RMF team at usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@mail.mil.

Appendix A

References

Section I

Required Publications

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

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

DODI 8500.01
Cybersecurity (Cited in para 1–1.) (Available at http://www.esd.whs.mil/dd.)

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

FISMA of 2014
(Cited in para 2–1.) (Available at https://www.congress.gov/bill/113th-congress/senate-bill/2521/text.)

Section II

Related Publications

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

AR 25–30
The Army Publishing Program

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

DODD 5000.01
The Defense Acquisition System

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

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

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 2875
System Authorization Access Request (SAAR)

Glossary

Section I

Abbreviations

AO
authorizing official

AODR
authorizing official designated representative

AO–R
authorizing official-repository

APMS
Army Portfolio Management Solution

AR
Army regulation

ARCYBER
U.S. Army Cyber Command

ATCTS
Army Training and Certification Tracking System

ATO
authorization to operate

CBT
computer based training

CIO
Chief Information Officer

CNSSI
Committee on National Security Systems instruction

DA Form
Department of the Army form

DA Pam
Department of the Army pamphlet

DATO
denial of authorization to operate

DD Form
Department of Defense form

DIACAP
Department of Defense Information Assurance Certification and Accreditation Process

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

eMASS
Enterprise Mission Assurance Support Service

FISMA
Federal Information Security Modernization Act

FY
fiscal year

GO
general officer

GS
general schedule

HQDA
Headquarters, Department of the Army

IATT
interim authorization to test

IS
information system

ISO
information system owner

IT
information technology

NIPRNET
Nonclassified Internet Protocol Router Network

P–ISSM
program information systems security manager

PIT
platform information technology

POA&M
plan of action & milestones

RMF
Risk Management Framework

SAR
security assessment report

SCA–A
security control assessor-Army

SES
senior executive service

SIPRNET
Secret Internet Protocol Router Network

SISO
Senior Information Security Officer

Section II

Terms

Authorization decision
A digitally signed official designation from an AO, made visible to the CIO/G–6, regarding acceptance of the risk associated with operating an IS. Expressed as ATO, IATT, or DATO.

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

Authorizing official
A GO, SES, or equivalent with the authority to assume responsibility formally for operating DOD ISs or PIT systems at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (see DODI 8500.01).

Authorizing official designated representative
Appointed by the AO to act on their behalf in carrying out and coordinating the required activities associated with security authorization (see DODI 8510.01).

Chief Information Officer
Agency official responsible for providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that ISs are acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; developing, maintaining, and facilitating the implementation of a sound and integrated IS architecture for the agency; and promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Denial of authorization to operate
AO determination that an IS or PIT system cannot operate because of an inadequate design or failure to implement assigned RMF controls. If the system is already operational, the operation of the system is halted.

Information system
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see CNSSI 4009). As part of the set of information resources, an IS includes its own operating system(s), firmware, hardware, or all of the above to support a single mission or a range of missions. An IS may include, but is not limited to, the products or deliverables of an acquisition program, such as those described in DODD 5000.01. ISs also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

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

Information systems security manager
Individual responsible for the information assurance of a program, organization, system, or enclave (see CNSSI 4009).

Information technology
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology (IT) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (see CNSSI 4009).

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

Platform information technology
IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Platform information technology system
A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Risk management
The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time.

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 IS. 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.

Security control assessment
The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security control assessor–Army
The individual, group, or organization responsible for conducting a security control assessment.

Senior Information Security Officer
Official responsible for carrying out CIO responsibilities under the FISMA of 2014 and serving as the CIO's primary liaison to the agency's AOs, ISOs, information systems security officers, and the agency security control assessor.

Section III

Special Abbreviations and Terms
The section contains no entries.