4

Army Regulation 25–2

Information Management

Information Assurance

Headquarters
Department of the Army
Washington, DC
24 October 2007

UNCLASSIFIED

SUMMARY of CHANGE

AR 25-2
Information Assurance

This administrative revision, dated 24 October 2007--

- Updates required warning notification and consent banners used with Department of Defense telecommunications systems and devices (para 4-5*m*).

- Corrects administrative and typographical errors (throughout).

Headquarters
Department of the Army
Washington, DC
24 October 2007

*Army Regulation 25–2

Effective 13 November 2007

Information Management

Information Assurance

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
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 provides Information Assurance policy, mandates, roles, responsibilities, and procedures for implementing the Army Information Assurance Program, consistent with today's technological advancements for achieving acceptable levels of security in engineering, implementation, operation, and maintenance for information systems connecting to or crossing any U.S. Army managed network.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Also, it applies to all users, information systems, and networks at all information classification levels; program executive officers; direct reporting program managers; strategic, tactical, and non-tactical environments or installations; internal or external organizations, services, tenants, or agencies (for example, DOD, sister Services, U.S. Army Corps of Engineers (USACE); contractors working on Army information systems pursuant to Army contracts; Army and Air Force Exchange Service (AAFES); morale, welfare, and recreation activities; educational institutions or departments (for example, DOD schools, the U.S. Military Academy at West Point); and Army affiliated or sponsored agencies (for example, Western Hemisphere Institute for Security Cooperation). During mobilization, the proponent may modify chapters and policies contained in this regulation.

Proponent and exception authority. The proponent of this regulation is the 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, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include a 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.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated (see appendix C).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Chief Information Officer, G–6 (SAIS–ZA), 107 Army Pentagon, Washington DC 20310–0107.

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

Distribution. Distribution of this publication is available in electronic media only and is intended for command levels B, C, D, and E for the Active 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)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Army Information Assurance Program • 1–4, *page 1*

*This publication supersedes AR 25–2, dated 3 August 2007.

UNCLASSIFIED

Contents—Continued

Overview • 1–5, *page 1*

Chapter 2
Responsibilities, *page 3*
Chief Information Officer/G–6 • 2–1, *page 3*
Principal Headquarters, Department of the Army officials and staff • 2–2, *page 4*
Administrative Assistant to the Secretary of the Army • 2–3, *page 4*
Assistant Secretary of the Army for Acquisition, Logistics, and Technology • 2–4, *page 4*
The Deputy Chief of Staff, G–2 • 2–5, *page 5*
The Deputy Chief of Staff, G–3/5/7 • 2–6, *page 5*
The Deputy Chief of Staff, G–4 • 2–7, *page 5*
Commanders of Army Commands; Army Service Component Commands; Direct Reporting Units; U.S. Army Reserve; Army National Guard; program executive officers; direct reporting program managers; Regional Chief Information Officers; Functional Chief Information Officers; and the Administrative Assistant to the Secretary of the Army • 2–8, *page 6*
Commander, 1st Information Operations Command • 2–9, *page 6*
Commanding General, Network Enterprise Technology Command/9th Signal Command (Army) • 2–10, *page 7*
Commanding General, U.S. Army Training and Doctrine Command • 2–11, *page 7*
Commanding General, U.S. Army Materiel Command • 2–12, *page 7*
Commanding General, U.S. Army Intelligence and Security Command • 2–13, *page 8*
Commanding General, U.S. Army Criminal Investigation Command • 2–14, *page 8*
Chief, Army National Guard • 2–15, *page 8*
Chief, Army Reserve • 2–16, *page 8*
U.S. Army Reserve Command Chief of Staff • 2–17, *page 8*
U.S. Army Corps of Engineers Chief of Engineers • 2–18, *page 9*
U.S. Army Corps of Engineers Chief Information Officer • 2–19, *page 9*
Commanding General, Eighth Army • 2–20, *page 9*
Commanding General, U.S. Army Europe • 2–21, *page 9*
Commanding General, U.S. Army Medical Command • 2–22, *page 9*
Program executive officers and direct reporting program/project managers • 2–23, *page 9*
Commanders, directors, and managers • 2–24, *page 10*
Garrison commanders • 2–25, *page 10*
U.S. Army Reserve major subordinate command • 2–26, *page 11*
Army National Guard state DOIM/J6/CIO • 2–27, *page 11*
Regional Chief Information Officer • 2–28, *page 11*
Army Reserve command/unit/activity G–6 • 2–29, *page 11*
Director of Information Management • 2–30, *page 11*

Chapter 3
Army Information Assurance Program Personnel Structure, *page 12*
Personnel structure overview • 3–1, *page 12*
Information assurance personnel structure • 3–2, *page 12*
Information assurance support personnel • 3–3, *page 15*

Chapter 4
Information Assurance Policy, *page 18*

Section 1
General Policy, page 18
Policy overview • 4–1, *page 18*
Funding • 4–2, *page 19*
Information assurance training • 4–3, *page 20*
Mission assurance category, levels of confidentiality, and levels of robustness • 4–4, *page 21*
Minimum information assurance requirements • 4–5, *page 22*

Contents—Continued

Section II
Software Security, page 29
Controls • 4–6, *page 29*
Database management • 4–7, *page 29*
Design and test • 4–8, *page 30*

Section III
Hardware, Firmware, and Physical Security, page 30
Hardware–based security controls • 4–9, *page 30*
Maintenance personnel • 4–10, *page 30*
Security objectives and safeguards • 4–11, *page 31*

Section IV
Procedural Security, page 31
Password control • 4–12, *page 31*
Release of information regarding information system infrastructure architecture • 4–13, *page 32*

Section V
Personnel Security, page 32
Personnel security standards • 4–14, *page 32*
Foreign access to information systems • 4–15, *page 35*

Section VI
Information Systems Media, page 37
Protection requirements • 4–16, *page 37*
Labeling, marking, and controlling media • 4–17, *page 37*
Clearing, purging (sanitizing), destroying, or disposing of media • 4–18, *page 38*

Section VII
Network Security, page 38
Cross-domain security interoperability • 4–19, *page 38*
Network security • 4–20, *page 38*

Section VIII
Incident and Intrusion Reporting, page 43
Information system incident and intrusion reporting • 4–21, *page 43*
Reporting responsibilities • 4–22, *page 43*
Compromised information systems guidance • 4–23, *page 43*

Section IX
Information Assurance Vulnerability Management, page 44
Information assurance vulnerability management reporting process • 4–24, *page 44*
Compliance reporting • 4–25, *page 44*
Compliance verification • 4–26, *page 45*
Operating noncompliant information system • 4–27, *page 45*

Section X
Miscellaneous Provisions, page 45
Vulnerability and asset assessment programs • 4–28, *page 45*
Portable electronic devices • 4–29, *page 46*
Wireless local area networks • 4–30, *page 47*
Employee–owned information systems • 4–31, *page 47*
Miscellaneous processing equipment • 4–32, *page 47*

Contents—Continued

Chapter 5
Certification and Accreditation, *page 48*
Certification and accreditation overview • 5–1, *page 48*
Certification • 5–2, *page 48*
Tailoring • 5–3, *page 49*
Accreditation • 5–4, *page 49*
Recertification and re–accreditation • 5–5, *page 49*
Accreditation documentation • 5–6, *page 50*
Connection approval process • 5–7, *page 50*
Designated approving authority • 5–8, *page 50*
Lead agent of the certification authority • 5–9, *page 51*
System owner • 5–10, *page 52*

Chapter 6
Communications Security, *page 52*
Communications security overview • 6–1, *page 52*
Protected distribution systems • 6–2, *page 53*
Approval of protected distribution systems • 6–3, *page 53*
Radio systems • 6–4, *page 54*
Telecommunication devices • 6–5, *page 54*

Chapter 7
Risk Management, *page 54*
Risk management process • 7–1, *page 54*
Information operations condition • 7–2, *page 55*

Appendixes

A. References, *page 56*

B. Sample Acceptable Use Policy, *page 61*

C. Management Control Evaluation Checklist, *page 65*

Table List

Table 4–1: MDEP MS4X, Information Assurance Phased Funding Utilization Plan/Actual Execution Report (RCS: CSIM–62)
For period ending 092009 (MMYYYY), *page 19*
Table 4–2: Investigative levels for users with privileged access (IT–I) to ISs, *page 34*
Table 4–3: Investigative levels for users with limited privileged access (IT–II) to ISs, *page 34*

Figure List

Figure B–1: Acceptable use policy, *page 62*
Figure B–1: Acceptable use policy—Continued, *page 63*
Figure B–1: Acceptable use policy—Continued, *page 64*

Glossary

Chapter 1
Introduction

1–1. Purpose

This regulation establishes information assurance (IA) policy, roles, and responsibilities. It assigns responsibilities for all Headquarters, Department of the Army (HQDA) staff, commanders, directors, IA personnel, users, and developers for achieving acceptable levels of IA in the engineering, implementation, operation, and maintenance (EIO&M) for all information systems (ISs) across the U.S. Army Enterprise Infostructure (AEI).

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Army Information Assurance Program

a. The Army Information Assurance Program (AIAP) is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by ISs, and is established to consolidate and focus Army efforts in securing that information, including its associated systems and resources, to increase the level of trust of this information and the originating source. The AIAP will secure ISs through IA requirements, and does not extend access privileges to special access programs (SAPs), classified, or compartmentalized data; neither does it circumvent need-to-know requirements of the data or information transmitted.

b. The AIAP is designed to achieve the most effective and economical policy possible for all ISs using the risk management approach for implementing security safeguards. To attain an acceptable level of risk, a combination of staff and field actions is necessary to develop local policy and guidance, identify threats, problems and requirements, and adequately plan for the required resources.

c. Information systems exhibit inherent security vulnerabilities. Cost-effective, timely, and proactive IA measures and corrective actions will be established and implemented to mitigate risks before exploitation and to protect against vulnerabilities and threats once they have been identified.

(1) Measures taken to attain IA objectives will be commensurate with the importance of the operations to mission accomplishment, the sensitivity or criticality of the information being processed, and the relative risks (the combination of threats, vulnerabilities, countermeasures, and mission impact) to the system. Implementation of an IA operational baseline will be an incremental process of protecting critical assets or data first, and then building upon those levels of protection and trust across the enclave.

(2) Statements of security requirements will be included in the earliest phases (for example, mission needs statements, operational requirements document, capstone requirement document) of the system acquisition, contracting, and development life cycles.

d. An operationally focused IA program requires the implementation of innovative approaches. Through the use of IA best business practices (BBPs) the best ideas, concepts, and methodologies acquired from industry and Army resources will be used to define specific standards, measures, practices, or procedures necessary to meet rapidly changing technology or IA requirements in support of Army policy requirements. IA BBPs allow rapid transitional implementation of IA initiatives to integrate, use, improve, or modify technological or procedural changes as required by policy. BBPs are located at https://informationassurance.us.army.mil.

e. The elements of the Defense in Depth (DiD) strategy focus on three areas: people, operations, and defense of the environment (the latter of which encompasses the computing environment, the networks, the enclave boundaries, and the supporting infrastructure).

f. The AIAP is not a stand-alone program, but incorporates related functions from other standards or policies such as; operations security (OPSEC), communications security (COMSEC), transmission security (TRANSEC), information security (INFOSEC), personnel security, and physical security to achieve IA requirements.

g. Failure to implement proactive or corrective IA security measures, guidance, policy, or procedures may prevent system or enclave accreditation, installation, or operation and may increase system vulnerability to foreign and domestic computer network operation (CNO) activities designed to deny service, compromise information, or permit unauthorized access to sensitive information. IA or network personnel may block access to ISs that reflect poor IA security practices or fail to implement corrective measures.

1–5. Overview

a. The AIAP applies to ISs including, but not limited to, computers, processors, devices, or environments (operating in a prototype, test bed, stand-alone, integrated, embedded, or networked configuration) that store, process, access, or transmit data, including unclassified, sensitive (formerly known as sensitive but unclassified (SBU)), and classified data, with or without handling codes and caveats. ISs used for teleworking, telecommuting, or similar initiatives; contractor owned or operated ISs; ISs obtained with non-appropriated funds; automated tactical systems (ATSs);

automated weapons systems (AWSs); distributed computing environments (DCEs); and systems processing intelligence information are required to adhere to the provisions of this regulation.

b. Commanders of activities requiring limited access by any local foreign national (FN) officials or personnel (including information technology (IT) positions) will follow the provisions of this regulation.

c. This regulation applies equally to the operation, safeguarding, and integrity of the infrastructures (for example, power, water, air conditioning), including the environment in which the IS operates.

d. While no regulation or policy on security measures can ever provide a 100 percent solution, implementation of the concepts, procedures, and recommendations in this regulation will drastically reduce the manageability requirements of assets, and minimize the effects of unauthorized access or loss. The cornerstone philosophy of IA is to design, implement, and secure access, data, ISs, and data repositories; increase trust and trusted relationships; employ technical and operational security mechanisms; deny all unauthorized accesses; and permit necessary exceptions to support Army, DOD, and Joint interagency and multinational (JIM) tactical and sustaining-base operations.

e. Army information constitutes an asset vital to the effective performance of our national security roles. While all communication systems are vulnerable to some degree, the ready availability of low-cost IT, freely distributed attack tools, increased system connectivity and asset distribution, and attack-standoff capabilities make computer network attacks (CNAs) an attractive option to our adversaries. Information Assurance capabilities and actions protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense (CND). Management of Army information is imperative so that its confidentiality, integrity, availability, and non-repudiation can be ensured, and that users of that data can be properly identified and authenticated.

f. The AEI architecture requires the establishment, verification, and maintenance of trusted enclaves, trusted connectivity, and trusted information and information sources along with the capability to access and distribute that information by leveraging technology and capabilities to amplify that trust.

g. To accomplish these foundational objectives, this regulation establishes requirements as follows:

(1) Provides administrative and systems security requirements, including those for interconnected systems.

(2) Defines and mandates the use of risk assessments.

(3) Defines and mandates the DiD strategy.

(4) Promotes the use of efficient procedures and cost-effective, computer-based security features and assurances.

(5) Describes the roles and responsibilities of the individuals who constitute the IA security community and its system users, and outlines training and certification requirements.

(6) Requires a life cycle management approach to implementing IA requirements.

(7) Introduces the concepts of mission assurance category, levels of confidentiality, and levels of robustness of information.

(8) Implements DODD 8500.1, DODI 8500.2, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 to align IA goals and requirements to support the DOD Information Management Strategic Plan.

(9) Mandates procedures to document the status of accreditations for all ISs fielded by DOD organizations, Army chartered program managers (PMs), and HQDA staff proponents.

(10) Mandates that DOD and Army-level designated approving authorities (DAAs) meet the system accreditation requirements of this regulation before fielding or testing any system that requires connection to an Army network.

(11) Requires the implementation of a configuration management (CM) process.

(12) Describes the Continuity of Operations Plan (COOP).

(13) Provides the foundation for the Networthiness Certification Program in AR 25–1.

h. Other policies, procedures, or directives also govern certain systems. In the event of conflicts among these policies, procedures, or directives, the more stringent requirement will take precedence. When the most stringent policy cannot be determined, the affected Army component will submit a request for a policy decision through their supporting regional chief information officers/functional chief information officers (RCIOs/FCIOs) to the Chief Information Officer/G–6 (CIO/G–6).

i. The mention of commercial products in this regulation does not imply endorsement by either DOD or the Army.

j. Military and civilian personnel may be subject to administrative and/or judicial sanctions 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 bolded text included in the following paragraphs 3–3, 4–5, 4–6, 4–12, 4–13, 4–16, 4–20, and 6–5.

k. These provisions may be punished as violations as follows:

(1) 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.

(2) 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).

(3) 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 designee, 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.

Chapter 2
Responsibilities

2–1. Chief Information Officer/G–6

The CIO/G–6 will—

a. Establish and issue IA policy and procedures and serve as the focal point for IA programs and funding.

b. Develop, review, and coordinate DA input into DOD IA policy documents.

c. Establish and maintain Army standardized evaluations and test methodology certification procedures and security requirements as part of the accreditation process.

d. Document, develop, coordinate, present, prioritize, and defend IA resource requirements in the planning, programming, and budgeting process.

e. Coordinate with the Deputy Chief of Staff, G–2 (DCS, G–2) for the policy, development, dissemination, support, tactics, techniques, and procedures for the design, implementation, and operation of the key management infrastructure (KMI) and systems to support Army encryption requirements.

f. Provide program oversight for Army implementation of the KMI and funding aspects of the Electronic Key Management System (EKMS).

g. Prepare the annual IA readiness report.

h. Provide technical and operational assistance and support to the U.S. Army Audit Agency (USAAA) in its audits and reviews of ISs.

i. Evaluate technological trends in IA and establish a methodology to integrate advancements.

j. Provide IA guidance to Army elements in identifying and incorporating requirements consistent with the KMI requirements in project development.

k. Act as the certification and accreditation (C&A) designated approving authority (DAA) for ISs with the exceptions found in paragraph 5–8*m*.

l. Provide a point of contact (POC) with the Defense Information Systems Agency/Center for Information Systems Security (DISA/CISS) for advice and assistance and implementation of certification tests and programs for Army operated ISs.

m. Serve as the Army member of the Committee on National Security Systems (CNSS) and the Subcommittees for Telecommunications Security (STS) and Information Systems Security (SISS).

n. Provide an Army voting member to the Key Management Executive Committee (KMEC) and Joint Key Management Infrastructure Working Group (JKMIWG).

o. Provide policy, guidance, and oversight on the employment of National Institute of Standards and Technology (NIST) approved cryptography for the protection of unclassified and sensitive information.

p. Appoint the chairperson and alternate chairperson for the Tier 1 System Management Board (TSMB), which has operations management responsibilities for the Tri-Service EKMS Common Tier 1 System (CT1S).

q. Participate with the DCS, G–2; U.S. Army Intelligence and Security Command (INSCOM); Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC (A); 1st Information Operations (LAND) Command (1st IO CMD (LAND)); and the U.S. Army Criminal Investigation Command (CID) in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

r. Appoint, formally, by name and organization the DAA for ISs that process Army data, upon request, through formal signed memo or digitally signed e-mail. This appointment will be consistent with paragraph 5–8*g* through *k*.

s. Ensure the concepts of, and strategies within, this regulation are utilized as the basis for networthiness certification per AR 25–1.

t. Provide technical and operational assistance and support to the Army Web Risk Assessment Cell (AWRAC).

u. Provide program oversight of Communications Security Logistics Activity (CSLA) for an Army cryptographic applications certification process (when developed).

v. Appoint the Director, Office of Information Assurance and Compliance (OIA&C), NETCOM/9th SC (A), as the Army senior information security officer under the provisions of the Federal Information Systems Management Act (FISMA).

w. Coordinate with the DCS, G–2 on C&A issues of sensitive compartmented information (SCI) systems and INSCOM/G–6 for SIGINT systems, as applicable.

x. See additional responsibilities at paragraph 2–2, below.

2–2. Principal Headquarters, Department of the Army officials and staff

Principal HQDA officials and staff will—

a. Implement IA requirements within their respective functional areas.

b. Develop, coordinate, supervise, execute, and allocate the research, development, test, and evaluation (RDT&E) procurement resources in support of IA program requirements as required in their functional area.

c. Participate collectively with other IA stakeholders in the enterprise planning, acquisition, and operation of IA strategies.

d. Integrate approved IA tools, doctrine, procedures, and techniques into all ISs under their purview.

e. Establish internal procedures for reporting security incidents or violations and report incidents and events to the servicing regional computer emergency response teams (RCERTs) in accordance with Section VIII, Incident and Intrusion Reporting, consistent with paragraphs 4–21 and 4–22, below.

f. Support the Army's Information Assurance Vulnerability Management (IAVM) Program notification and correction processes. IAVM notification and correction are DOD and Army operational requirements.

g. Develop and implement local acceptable use policy (AUP) for all users authorized access to HQDA ISs (app B presents a sample AUP).

h. Ensure all systems, for which the principal HQDA Army office is the system owner (SO) are accredited, annually revalidated, and re–accredited in accordance with the interim DOD Information Assurance Certification and Accreditation Process (DIACAP).

i. Ensure the C&A package is submitted to the Army certification authority (CA) in sufficient time for a review and operational IA risk recommendation in support of DAA authorization decision prior to operations or tests on a live network or with live Army data.

j. Request appointment as the DAA for information systems, as appropriate, from the CIO/G–6 through the OIA&C consistent with paragraph 5–8.

k. Appoint appropriate IA personnel per chapter 3 of this regulation and provide CIO/G–6 a copy of the appointment orders.

l. Identify personnel and procedures at all organizational and subordinate levels, as required, to implement a Configuration Management Board (CMB) or Configuration Control Board (CCB) to effect control and management mechanisms on all ISs, devices, configurations, and IA implementations. Include IA personnel as members of the board.

m. Incorporate related OPSEC, COMSEC, and INFOSEC policies and requirements into a comprehensive IA management program.

2–3. Administrative Assistant to the Secretary of the Army

The AASA will—

a. Serve as the commander for Pentagon Information Technology Services (ITS).

b. Request appointment, from the CIO/G–6 through the OIA&C, as the DAA for the Pentagon ITS and IS connected to the Pentagon Common Information Technology (CIT) Enterprise, associated swing space, and alternate COOP sites through the national capital region (NCR).

c. Appoint, once authorized, General Officer (GO), Senior Executive Service (SES) or equivalent within AASA purview as DAAs, when they are the SOs or have life cycle responsibility for the IS, as appropriate. Provide a copy of the appointments to the OIA&C through iacora@us.army.mil.

d. Coordinate connectivity requirements to the Department of Defense Intelligence Information System (DODIIS) IT SCI enterprise backbone within the Pentagon CIT enterprise.

e. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–4. Assistant Secretary of the Army for Acquisition, Logistics, and Technology

The ASA (ALT) will—

a. Forward to National Security Agency (NSA) and HQDA approved materiel requirements for IA tools and equipment (including cryptographic equipment), along with requests for RDT&E efforts to fulfill those needs.

b. Designate an Army materiel developer to conduct and update threat analyses as outlined by AR 381–11.

c. Monitor NSA, other Service COMSEC, and IA RDT&E projects that are of interest to the Army. Designate Army program managers as defined in AR 70–1 for each project having potential application for Army use. Require the designated manages to maintain a liaison between the developing agency and interested Army agencies of the progress of such projects.

d. Establish coordination with NSA concurrent life cycle management milestones for development of cryptographic equipment in support of IA initiatives.

e. Conduct research and acquire basic knowledge of the techniques and the circuitry required to provide an effective CND capability in appropriate types of Army equipment.

f. Ensure application of capabilities to perform IS risk analysis, reduction, and management.

g. Ensure that Army program executive officers (PEOs) and direct reporting PMs include IA in all systems development activities.

h. Ensure Army PEOs and direct-reporting PMs obtain C&A approval to operate prior to system operations on the Army network or with Army data.

i. See additional responsibilities at paragraph 2–2.

2–5. The Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Coordinate the development and dissemination of DOD, national, theater, and DA-level IA threat information to the Army.

b. Coordinate with the CIO/G–6 for the policy, development, dissemination, support, tactics, techniques, and procedures for the design, implementation, and operation of the KMI and systems to support Army encryption requirements.

c. Develop policy and approve procedures for safeguarding and controlling COMSEC and controlled cryptographic item (CCI) material.

d. Ensure all intelligence systems, for which the DCS, G–2 is the Army proponent or sponsor, are accredited or re-accredited in accordance with Director, Central Intelligence Agency Directive (DCID) 6/3.

e. Ensure that the DODIIS Program is implemented and guidance is published.

f. Serve as the approval authority for external IS penetration and exploitation testing of operational networks.

g. Participate with the CIO/G–6, INSCOM, NETCOM/9th SC (A), 1st IO CMD (LAND), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

h. Act as the Service Certifying Organization and DAA for DODIIS processing SCI on the Joint World Wide Intelligence System (JWWICS).

i. Act as the CA for SCI systems processing information at Protection Level (PL) 4.

j. Act as the DAA for SCI systems processing information up to PL 3.

k. See additional responsibilities at paragraph 2–2.

2–6. The Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Support the CIO/G–6 in the accomplishment of IA responsibilities.

b. Ensure IA training is integrated and conducted throughout the Army.

c. Support audits and reviews of ISs and networks through operational and technical assistance, as required.

d. Provide guidance, requirements, and oversight for information operations condition (INFOCON) alerting and implementation measures.

e. Provide guidance, requirements, and oversight for OPSEC measures to support an IA management policy.

f. See additional responsibilities at paragraph 2–2.

2–7. The Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Develop, as the Army independent logistician, logistics policies (including integrated logistics support policy), concepts, procedures, and guidance for logistics support of IA equipment used in support of all Army missions.

b. Prescribe execution of NSA or DOD logistics management directives that apply to classified COMSEC and CCI materiel.

c. Prescribe and supervise the implementation of procedures for property control and the accounting of CCI materiel during distribution, storage, maintenance, use, and disposal. All guidance will conform to the security standards developed by the DCS, G–2 for safeguarding COMSEC and CCI materiel.

d. Supervise logistics support planning to ensure the availability of materials and publications needed for repair, test measurement, and diagnosis of IA equipment and systems.

e. Provide continuous logistical support for fielded IA material and test equipment.

f. See additional responsibilities at paragraph 2–2.

2–8. Commanders of Army Commands; Army Service Component Commands; Direct Reporting Units; U.S. Army Reserve; Army National Guard; program executive officers; direct reporting program managers; Regional Chief Information Officers; Functional Chief Information Officers; and the Administrative Assistant to the Secretary of the Army

Commanders of ACOMs; ASCCs; DRUs; U.S. Army Reserve; ARNG; Chief, CAR ; PEOs; direct reporting PMs; RCIOs/FCIOs; and the AASA are responsible for ensuring that their units, activities, or installations will—

a. Develop and implement an IA program with the hardware, software, tools, personnel, and infrastructure necessary to fill the IA positions and execute the duties and responsibilities outlined in this regulation.

b. Oversee the maintenance, documentation, and updating of the C&A requirements required for the operation of all ISs as directed in this regulation.

c. Implement and manage IT system configurations, including performing IAVM processes as directed by this regulation.

d. Appoint IA and other personnel (for example, alternates) to perform the duties in chapter 3 of this regulation and provide information assurance program manager (IAPM) and/or POC information to the RCIOs, supporting RCERTs/ Theater Network Operations and Security Centers (TNOSCs), and the Army Computer Emergency Response Team (ACERT). The ACOMs/ASCCs IAPMs will also provide reports to the RCIO of the region in which the headquarters is physically located.

e. Appoint DAAs only as authorized in section II and paragraph 5–8.

f. Establish an oversight mechanism to validate the consistent implementation of IA security policy across their areas of responsibility.

g. Ensure annual security education, training, and awareness programs are developed and conducted that addresses, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

h. Oversee the implementation of IA capabilities.

i. Incorporate IA and security as an element of the system life cycle process.

j. Develop and implement an acceptable use policy for privately owned equipment (for example, cell phones, personal digital assistants (PDAs), wireless devices, and removable media) and ISs prohibited during training exercises, deployments, and tactical operations. Incorporate, as a minimum, the prohibition of utilizing such devices or the limitations of acceptable use, as well as the threat of operational exposure represented by these devices in garrison, pre-deployment staging, tactical, and operational areas.

k. Develop procedures for immediate notification and recall of IA personnel as assigned.

l. Adhere to and implement the procedures of the networthiness certification process per AR 25–1.

m. Program, execute, and report management decision packages (MDEPs) MS4X and MX5T resource requirements.

n. See additional responsibilities at paragraph 2–2.

2–9. Commander, 1st Information Operations Command

The Commander, 1st IO CMD (LAND) will—

a. Exercise command and control of the ACERT and all of its components (including RCERTs).

b. Establish tactics, techniques, and procedures (TTPs) for the ACERT, RCERTs, and Local Computer Emergency Response Teams (LCERTs) (if established) as required.

c. Integrate, in conjunction with NETCOM/9th SC (A), computer emergency response, IA, and CND service provider activities into network operations (NETOPS), network management, and information dissemination.

d. Integrate, in coordination with the DCS, G–3/5/7, CND, OPSEC, and INFOCON activities into information operations (IO).

e. Support the Army CND service provider as the focal point for security incidents and violations.

f. Develop and publish incident response guidelines, checklists, and procedures in coordination with law enforcement (LE) and counterintelligence (CI) agencies.

g. Provide status reports per directives on unusual activities occurring on Army networks worldwide.

h. Support the IA security tool repository and provide recommendations for including new tools.

i. Provide tools, methodologies, procedures, and oversight for the vulnerability assessment program and perform vulnerability assessments through approved programs.

j. Develop and maintain an Army CND vulnerability database for trend analysis.

k. Support and maintain Army IAVM message staffing, notification, distribution, and resolution.

l. Develop TTPs for a threat warning and notification process.

m. Develop procedures to issue CND lessons learned identified from incidents, intrusions, analyses, or other technical processes.

n. Maintain Army computer network situational intelligence awareness, including network threat analysis and Internet network intelligence.

o. Participate with the CIO/G–6, DCS, G–2, INSCOM, NETCOM/9th SC (A), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

p. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–10. Commanding General, Network Enterprise Technology Command/9th Signal Command (Army)

The CG, NETCOM/9th SC (A) will—

a. Request appointment from the CIO/G–6 as the DAA for the Army enterprise.

b. Appoint, once authorized, the Director, Enterprise Systems Technology Activity (ESTA) as the DAA for the Army enterprise.

c. Operate, manage, monitor, administer, and defend the Army portion of the global information grid.

d. Perform configuration and patch management for all Army network components and systems.

e. Execute Computer Network Defense Service Provider (CNDSP) and NETOPS missions and functions.

f. Review, coordinate, evaluate, and approve proposed policies, procedures, directives, standards, doctrinal publications, plans, materiel requirement documents, life cycle management documents, basis-of-issue plans, and system certification and accreditation documents for all systems fielded, or planned to be fielded, to Army installations as well as similar documents that have implications for adherence to policy.

g. Establish TTPs to integrate IA/CND service provider activities with system and network management and information dissemination.

h. Provide timely flows of NETOPS data to maintain an analysis view at all levels.

i. Ensure an operational assessment of IA products is conducted before incorporation into systems under NETCOM/9th SC (A) management.

j. Maintain a repository of the status and availability of Army critical systems and networks.

k. Manage the DiD security architecture environment, strategies, connections, and configurations against unauthorized access, manipulation, or destruction.

l. Manage the AEI Technical CCB responsible for the Army security architecture. Establish baseline configuration management guidelines and technical and operational TTPs; and review, approve, prioritize, and manage change to the AEI.

m. Conduct quarterly vulnerability assessments of top level architecture (TLA) critical assets, devices, servers, and IA implemented devices.

n. Participate with the CIO/G–6, DCS, G–2, INSCOM, 1st IO CMD (LAND), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

o. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–11. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

a. Integrate approved IA tools, doctrine, procedures, legalities, and techniques into applicable programs of instruction for TRADOC schools.

b. Develop timely Armywide IA training literature and training aids, leveraging secure electronic distribution and remote access capabilities.

c. Develop, test, and recommend operational and organizational concepts and doctrine to achieve IA goals.

d. Develop and provide IA requirements to the materiel developers and ensure compliance with AR 381–11 and this regulation.

e. Conduct or participate in operational tests of IA implementations as part of system-wide operational tests, as directed.

f. Integrate IA practices into pre-milestone A activities and events as required.

g. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–12. Commanding General, U.S. Army Materiel Command

The Commanding General, U.S. Army Materiel Command will—

a. Provide Armywide materiel developer IA support for RDT&E and production.

b. Assist IS functional proponents in identifying security requirements for proposed and existing sustaining base, tactical, and weapons systems.

c. Maintain a repository of tactical IA tools, and distribute tools to fielded tactical systems, as needed. Coordinate with 1st IO CMD to integrate tactical and sustaining-base toolboxes into a seamless repository for Army users.

d. Provide a DA authorized (that is, CSLA) cryptographic advisor to the certification authority (CA) throughout the DIACAP process.

e. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–13. Commanding General, U.S. Army Intelligence and Security Command

The Commanding General, INSCOM will—

a. Serve as the Army Service Cryptologic Element (SCE) and point of contact for ISs under the purview of the NSA.

b. Provide CI support to Army elements on IA matters and advise accreditation authorities on the foreign intelligence threat.

c. Coordinate the C&A for all cryptographic systems and conduct C&A for all Army cryptographic systems at PL 2 (DCID 6/3) and below.

d. Participate with the CIO/G–6, DCS, G–2, 1st IO CMD (LAND), NETCOM/9th SC (A), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

e. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–14. Commanding General, U.S. Army Criminal Investigation Command

The Commanding General, CID will—

a. Operate the Computer Crime Investigative Unit (CCIU).

b. Conduct criminal investigations involving intrusions into Army networks and computers.

c. Provide criminal and technical intelligence analyses of vulnerabilities, methodology, tools, techniques, or practices obtained from computer crimes or forensic intrusion analyses to support CND, C&A, and program developers or managers.

d. Participate in IAVA Compliance Verification Team (CVT) inspections.

e. Conduct crime prevention surveys to identify crime-conducive conditions involving Army networks and systems.

f. Serve as chief enforcer of Federal laws governing the investigation of criminal offenses involving networks and systems, serve as the sole entity for LE investigation determinations, and serve as the sole Army interface with Federal and civilian LE agencies.

g. Participate with the CIO/G–6, DCS, G–2, INSCOM, NETCOM/9th SC (A), and 1st IO CMD (LAND) in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures will be directed.

h. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–15. Chief, Army National Guard

The Chief, ARNG will—

a. Request appointment as the DAA for the ARNG and GuardNet XXI from the CIO/G–6.

b. Appoint, once authorized, the ARNG state Director of Information Management (DOIM)/J6/CIO for individual states in accordance with paragraph 5–8. General officers within the ARNG are state employees not Title 10 or Title 32 Soldiers, therefore, the state DOIM/J6/CIO will be appointed as DAAs. Provide a copy of these appointments to the CIO/G–6 through the OIA&C.

c. Set the ARNG IA priorities, provide oversight, and ensure the coordination and compliance of the ARNG IA program is accomplished with the CG, NETCOM to leverage Army technical authority standards and ensure compliance with this regulation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–16. Chief, Army Reserve

The CAR will—

a. Request appointment as the DAA for the U.S. Army Reserve (USAR) from the CIO/G–6.

b. Appoint, once authorized, the Army Reserve Command (USARC) Chief of Staff (COS) as the Army Reserve Network (ARNET) DAA when the COS meets the requirements of paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. Set the USAR IA priorities, provide oversight, and ensure the coordination and compliance of the USAR IA program with the CG, NETCOM to leverage Army technical authority standards and ensure compliance with this regulation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–17. U.S. Army Reserve Command Chief of Staff

The USARC COS will—

a. Request appointment as the ARNET DAA, as applicable, from the CAR.

b. Appoint, once authorized, the major subordinate command (MSC) Commander as DAA for command/unit/activities non-ARNET system/network implementations when the MSC meets the requirements of paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. Ensure all AR commands/units/activities, to include but not limited to, all off installation Government and non-Government satellites, facilities, and buildings, meet the requirements for connecting physically, logically, and/or virtually to the ARNET backbone.

d. Ensure MSC Commanders implement the AR IA program in accordance with CAR priorities and the CG, NETCOM via the applicable Army technical authority standards and ensure compliance with this regulation.

e. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–18. U.S. Army Corps of Engineers Chief of Engineers

The USACE Chief of Engineers (COE) will—

a. Set IA priorities, provide oversight, and ensure the coordination and compliance of the IA program throughout USACE.

b. Ensure the USACE CIO implements the USACE IA program in accordance with USACE priorities and the CG, NETCOM via the applicable Army technical authority standards and ensure compliance with this regulation.

c. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–19. U.S. Army Corps of Engineers Chief Information Officer

The USACE Chief Information Officer (CIO) will—

a. Request appointment as the DAA for the USACE Wide Area Network (WAN) and all corporate IS.

b. Appoint, once authorized, the USACE Division Commanders as DAA for USACE IS as applicable, when the Division Commander meets the requirements of paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–20. Commanding General, Eighth Army

The CG, Eighth Army will—

a. Request appointment as the DAA for Eighth Army from the HQDA CIO/G–6.

b. Appoint, once authorized, the Eighth Army CIO/G–6 as the DAA when the Eighth Army CIO/G–6 meets the requirements of paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. Ensure MSC commanders implement the Eighth IA program in accordance with Eighth Army priorities and the CG, NETCOM via the applicable Army technical authority standards and ensure compliance with this regulation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–21. Commanding General, U.S. Army Europe

The CG, USAREUR will—

a. Request appointment as the DAA for Army Europe from the CIO/G–6.

b. Appoint, once authorized, the DAAs for USAREUR backbone, tenant and MSC in accordance with the requirements of paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. Ensure tenant and MSC Commanders implement the USAREUR IA program in accordance with USAREUR priorities and the CG, NETCOM via the applicable Army technical authority standards and ensure compliance with this regulation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–22. Commanding General, U.S. Army Medical Command

The CG, MEDCOM will—

a. Request appointment as the DAA for MEDCOM from the CIO/G–6.

b. Appoint, once authorized, the DAA for individual Regional Medical Commands (RMC) Commander and MSCs in accordance with paragraph 5–8. Provide a copy of this appointment to the CIO/G–6 through the OIA&C.

c. Ensure RMC and MSC Commanders implement the MEDCOM IA program in accordance with MEDCOM priorities and the CG, NETCOM via the applicable Army technical authority standards and ensure compliance with this regulation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–23. Program executive officers and direct reporting program/project managers

Program executive officers (PEOs) and program/project managers (including PMs outside the PEO structure responsible for fielding systems to multiple Army organizations) will—

a. Acquire, operate, and support systems within their command or activity per this regulation.

b. Embed IA engineering and capabilities in all system RDT&E activities.

c. Appoint an IAPM to perform those duties listed in paragraph 3–2*b*.

d. Ensure that designated pre-deployment information assurance security officers (IASOs) effect continuous coordination with the organizational IA personnel for which the systems are demonstrated, tested, or fielded.

e. Request appointment as the DAA for named acquisition systems developed under their charter from the CIO/G–6 through the OIA&C.

f. Provide the C&A package to the CA for an operational IA risk recommendation supporting the DAA approval to operate decision prior to operational use or testing on a live network or with live Army data.

g. Ensure that the SO makes the C&A package available to the ACOM/ASCC, RCIO IAPM, and NETCOM, 30 days before initial operational test and evaluation (IOT&E) and before deployment of the system.

h. Integrate IA, COMSEC, and TEMPEST into entire system life cycle design, development, and deployment.

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

j. Integrate IA practices into pre-milestone A activities and events.

k. Perform acquisition and life cycle management of materiel in support of the IA strategy.

l. Report to HQDA CIO/G–6 the percentage of PEO/PM-programmed funding allocated to the AIAP. The report will include current and planned IA investments.

m. Accomplish all intelligence and threat support requirements outlined in AR 381–11 and this regulation.

n. Enforce IA standards and maintain/report an inventory of IS products, equipment, locations, and contact information.

o. Enforce IAVM compliance measures (for example, notifications, patch management) and incorporate them into life cycle management procedures.

p. Coordinate with CSLA to ensure cryptographic life cycle equipment management is a consideration during system design phase.

q. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–24. Commanders, directors, and managers

Commanders, directors, and managers will—

a. Be responsible for implementing the AIAP in their command or activity.

b. Acquire, operate, and maintain systems within their command or activity per this regulation.

c. Incorporate and define requests for new systems or changes to existing systems, including security requirements necessary for the system's concept of operation. Once validated, include these security requirements into the system design as defined in procurement contracts. Address the addition of IT/IA personnel (such as SAs or network security managers needed to operate the new or expanded system or network) as part of the development cost of stated system or network.

d. Include IO and IA requirements in submissions of commander's critical information requirements (CCIR) or priority intelligence requirements (PIR).

e. Ensure uses of market-driven/industry-developed (MDID), commercial-off-the-shelf (COTS), or other products are consistent with IA requirements and do not introduce an unacceptable risk.

f. Appoint appropriate IA personnel per chapter 3 of this regulation.

g. Ensure that designated pre-deployment IASOs effect continuous coordination with the organizational IA personnel for which the systems are demonstrated, tested, or fielded.

h. Ensure IA, COMSEC, and TEMPEST requirements are incorporated into life cycle planning.

i. Ensure implementation of this regulation is accomplished in compliance with all statutory and contractual labor relations obligations.

j. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–25. Garrison commanders

Garrison commanders will—

a. Implement the installation level IA program in accordance with the installation commander priorities and the CG, NETCOM via the applicable continental United States (CONUS) RCIO Army technical authority standards and to ensure compliance with this regulation.

b. Obtain approval to operate the garrison information systems from the first general officer or SES in the chain of command that has obtained the appropriate DAA appointment from the CIO/G–6.

c. Ensure the installation DOIM develops the installation C&A package, and obtains and maintains approval to operate the installation campus area network (ICAN) and any DOIM controlled or managed consolidated service locations (server farms).

d. Ensure all installation tenants, to include but not limited to, all off installation Government and non-Government satellites, facilities, and buildings, meet the requirements for connecting physically and/or virtually to the ICAN (that is, the installation backbone).

e. Coordinate with the supporting NETCOM/9th SC (A) component, ACOM/ASCC, IMA, and tenant organizations for IA implementation and compliance.

f. Acquire, operate, and maintain systems within their installation or activity per this regulation.

g. Maintain the CM of the garrison network and ensure that the installation-level CCB/CMB provides oversight support to the installation commander.

h. Monitor and manage the connection, access, and IA standards for standalone and networked ISs down to the workstation level across all installation and tenant organizations.

i. Manage and oversee the operation of the installation infrastructure throughout the system life cycle.

j. Provide technical and functional IA guidance and assistance in support of network management.

k. Review, before adoption, proposed changes that could affect the operation of the installation infrastructure's network security and operation (confidentiality, integrity, and availability).

l. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–26. U.S. Army Reserve major subordinate command

The USAR MSC will—

a. Request appointment as the non-ARNET system/network DAA, as applicable, from the USARC COS.

b. Implement a command/unit/activity level IA program in accordance with CAR priorities and ensure compliance with this regulation.

c. Ensure the command/unit/activity G–6 develops command/unit/activity level certification and accreditation for all non-ARNET system/network implementation.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–27. Army National Guard state DOIM/J6/CIO

The ARNG State DOIM/J6/CIO will—

a. Request appointment as the ARNG State DAA, as applicable, from the Chief ARNG. General officers within the ARNG are state employees not Title 10 or Title 32 Soldiers, therefore, the state DOIM/J6/CIO will perform the state DAA duties once appointed.

b. Implement the ARNG IA program in the state, as applicable, in coordination with the ARNG Chief to ensure compliance with this regulation.

c. Ensure all ARNG State tenants, to include but not limited to, all ARNG state government and non-Government satellites, facilities, and buildings, meet the requirements for connecting physically and/or virtually to the ARNG state and ARNG backbone (that is, GuardNet XXI).

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–28. Regional Chief Information Officer

The RCIO, as CG, NETCOM representative will—

a. Be responsible for ensuring the technical authority enterprise standards are reflected in the installation IA priorities and implemented through coordination with the appropriate IC, garrison commander and DOIM.

b. See additional responsibilities at paragraph 2–2, paragraph 2–8, and paragraph 3–2.

2–29. Army Reserve command/unit/activity G–6

The USAR command/unit/activity G–6 will—

a. Implement an IA program as directed by the USAR MSC Commander that reflects the CAR priorities and ensure compliance with this regulation.

b. Ensure USAR standards for connections to the ARNET are met.

c. Develop non-ARNET system/network implementations certification and accreditation, provide to the CA for an operational IA risk recommendation supporting the DAA approval to operate decision prior to operational use on a live network or with live Army data.

d. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

2–30. Director of Information Management

The DOIMs will—

a. Implement an IA program as directed by the garrison commander that reflects the IC priorities and with the CG, NETCOM via the applicable Army technical authority standards and is compliant with this regulation.

b. Ensure Army standards for connection to the ICAN are met.

c. Develop the installation certification and accreditation package, and provide to the Army CA for an operational IA risk recommendation in support of a DAA approval to operate decision.

d. Obtain and maintain approval to operate for the installation ICAN and any DOIM controlled or managed consolidated service locations (server farms) from the appropriate DAA.

e. See additional responsibilities at paragraph 2–2 and paragraph 2–8.

Chapter 3
Army Information Assurance Program Personnel Structure

3–1. Personnel structure overview

Commanders will establish an IA personnel structure to implement the AIAP. These personnel will be the focal points for IA matters within their commands or activities and will have the authority to enforce, with DAA concurrence, security policies and safeguards for their systems or networks. This authority includes recommending to the DAA suspension of system operations based on an identified security deficiency, poor security practice, or unacceptable risk. Position the IA staff in the organization to ensure operations do not negate system security, except as directed by the DAA. The IA staff will be involved in the acquisitioning and contracting for ISs or IS services.

3–2. Information assurance personnel structure

Commanders will position IA personnel organizationally to provide a balance between security and operational missions. The following is the AIAP personnel structure and activities to be performed.

a. RCIO. NETCOM/9th SC (A) RCIOs have the authority and responsibility to—

(1) Translate strategic plans and technical guidance provided into objectives, strategies, and architectural guidance.

(2) Exercise staff supervision and technical control for all IT organizations within their region and execute responsibilities for baseline services (communication and system support, visual information, documents management, IA, INFOCON, automation), either operationally or programmatically, as well as oversight of NETOPS.

(3) Provide all personnel operating on Army installations the IT baseline services in a manner consistent with policies and regulations.

(4) Provide administrative, financial, and managerial IT support to any Army installation located within their geographic region.

(5) Coordinate the management of outsourced IT services.

(6) Define the baseline and objectives, and establish specific service levels detailing contractual arrangements and satisfactory contractor performance.

(7) Lead enterprise-level initiatives that assure users' training requirements are considered and integrated into processes for developing, implementing, and maintaining capabilities and systems.

(8) Act as the focal point for command, control, communications, and computers for information management (C4IM) leadership and coordination of IT activities within the region.

(9) Execute the duties assigned under the NETCOM/9th SC (A) CONOPS for Service Level Agreements, Configuration Management, and Networthiness Certification Program.

(10) Ensure all ISs, networks, and devices are scanned quarterly as a minimum, including, but not limited to, scanning for vulnerabilities, poor security practices, noncompliance, backdoor connections, unauthorized modems, malicious logic, and unauthorized network connections; take actions to report all violations.

(11) Ensure implementation of AIAP policy and procedures within their region.

(12) Oversee the assignment of regional IA personnel and appoint a regional IAPM.

(13) Provide supported commands, organizations, and agencies with POC information, especially if geographically disbursed across several regions.

b. IAPM. The IAPM will be accountable for establishing, managing, and assessing the effectiveness of all aspects of the IA program within a region, command, or functional activity. A contractor will not fill the IAPM position. (Temporary assignment of contractor personnel for a specified time, as an exception, is authorized until the position can be properly filled.) The IAPM must be a U.S. citizen and hold a U.S. Government security clearance and access approval commensurate with the level of responsibility. Designate this position as information technology I (IT–I). The IAPM must be IA trained and certified, and maintain the certification. The IAPM will—

(1) Develop, manage, and maintain a formal IA security program that includes defining the IA personnel structure and ensuring the appointment of an information assurance network manager (IANM), information assurance network officer (IANO), information assurance manager (IAM), and an IASO at subordinate levels.

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

(3) Ensure that IA personnel implement vulnerability remediation bulletins and advisories that affect the security of their ISs.

(4) Ensure that all IA personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.

(5) Serve as the primary point of contact for IA-related actions. This includes IAVM reporting, compliance, vulnerability assessments, and feedback to Army staff on current and upcoming IA policies.

(6) As applicable, Regional and Command IAPMs will provide their supporting RCERT or TNOSC with guidance and priorities regarding IA/CND support to their regions, command, and subordinates.

(7) Manage the DIACAP program to ensure compliance with requirements.

(8) Ensure the development of system C&A documentation by reviewing and endorsing such documentation and recommending action to the DAA.

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

(10) Ensure DAAs maintain a repository for all systems' C&A documentation and modifications.

(11) Ensure that security violations and incidents are reported to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(12) Ensure that RCERT directed protective and corrective measures are implemented for vulnerabilities or incidents remediation.

(13) Identify data ownership (including accountability, access, and special handling requirements) for each IS or network within their authority.

(14) Conduct announced and unannounced IA assessments.

(15) Regional IAPMs will maintain liaison with appropriate Army theater and DOD activities, at a minimum including CIO/G–6, RCIO, DISA, NSA, the Defense Intelligence Agency (DIA), HQDA, 1st IO CMD, ACERT, supporting RCERT/TNOSC, CID, and INSCOM elements.

(16) Program, manage, execute, and report MDEPs MS4X and MX5T resource requirements.

(17) Administer an IA management control evaluation program separate from, or in support of, Force Protection Assessment Teams (FPATs).

(18) Serve as a member of the configuration board where one exists.

(19) In coordination with the DCS, G–3, DCS, G–2, and CIO/G–6, provide technical and non-technical information to support a commander's INFOCON program.

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

(21) The ACOM/ASCC/functional IAPMs will ensure that any ACOM/ASCC–sponsored or developed unique systems are fully accredited and certified prior to connection to the network. Ensure that any proposed distribution will meet Networthiness certification and the NETCOM/9th SC (A) connection approval process, and fulfill all requirements as a standard PM-developed fielding prior to distribution.

c. Regional IANM. The IANM (if appointed) may serve as the alternate IAPM. A contractor will not fill the IANM position. (Temporary assignment of contractor personnel for a specified period, as an exception, is authorized, until the position can be properly filled.) The IANM must be a U.S. citizen and hold a U.S. Government security clearance and access approval commensurate with the level of responsibility. This position will be designated IT–I. The IANM must be IA certified and maintain his or her certification. The IANM, under the purview of the IAPM, will—

(1) Provide direct support to the IAPM on matters of CND and the regional/command IA program.

(2) Develop and oversee operational (technical) IA implementation policy and guidelines.

(3) Advise the IAPM or DAA on the use of specific network security mechanisms.

(4) Evaluate threats and vulnerabilities to ascertain the need for additional safeguards.

(5) Assess changes in the network, its operational and support environments, and operational needs that could affect its accreditation.

(6) Ensure procurement actions, installations, and modifications to existing infrastructure comply with Army-approved IA architectural guidance.

(7) Develop and staff IA technical policy and procedures for all networks.

(8) Ensure that all networks on the installation or activity for which they are responsible, including tenant networks accessing the host installation's infrastructure, are planned, installed, managed, accredited, maintained, and operated per the security requirements of this regulation and the standards required for connectivity and classification of the network concerned.

(9) Develop and issue network security policy, guidance, and countermeasure implementation instructions to assigned and tenant activities.

(10) Oversee periodic use of authorized scanning and assessment tools.

(11) Assist the IAPM in monitoring and enforcing the IAVM and INFOCON processes.

(12) Serve as a member of the CMB where one exists.

d. IAM. Appoint IAMs at all appropriate levels of command. This includes subordinate commands, posts, installations, and tactical units. Appoint an IAM as needed for those Army activities responsible for project development, deployment, and management of command-acquired software, operating systems, and networks. A contractor will not

fill the MSC, installation, or post IAM positions and the person filling the position will be a U.S. citizen. Commands, activities, or organizations with multiple IAMs will appoint a senior IAM for their command, activity, or organization. In installations with multiple IAMs, the Installation IAM is the Senior IAM. All IAMs will hold a U.S. Government security clearance and access approval commensurate with the level of information processed by the system. This position will be designated IT–I, IT–II, or IT–III. The IAM must be IA trained and certified, and must maintain his or her certification. The IAM will—

(1) Develop and enforce a formal IA security and training program.

(2) Enforce IAVM dissemination, reporting, compliance, and verification procedures as described in CJCSM 6510.01.

(3) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(4) Conduct security inspections, assessments, tests, and reviews.

(5) Manage IASOs, as required, to establish the scope of responsibilities and the technical and security training requirements.

(6) Conduct semi-annual reviews of all ISs and networks to ensure no security changes have been made to invalidate the C&A.

(7) Negotiate C&A issues with the DAA, or his or her designated representative, for incoming systems and make recommendations to the commander on additional protection mechanisms necessary prior to operation of the incoming ISs.

(8) Maintain training and certification records for IA personnel and user IA awareness training records.

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

(10) Review all IA C&A support documentation packages and system fielding, operations, or upgrades requirements to ensure accuracy and completeness, and that they meet minimal risk acceptance standards.

(11) Maintain a repository for all systems C&A documentation and modifications, version control, and management of GOTS, COTS, and non-developmental items (NDIs) for his or her organization or site.

(12) Identify data ownership (including accountability, access, and special handling requirements) for each IS or network within their authority.

(13) Verify that all ISs within the scope of responsibility are properly certified and accredited in accordance with DIACAP and CM policies and practices before operating or authorizing the use of hardware and software on an IS or network.

(14) Serve as a member of an applicable CCB, where one exists.

(15) Ensure that IA personnel are maintaining and auditing access and log data.

(16) Assist the IAPM to identify and validate IA resource requirements.

(17) Provide input to the IAPM for management controls.

(18) The Installation IAM will provide policy and guidance to all IAMs on an installation.

(19) Tenant IAMs will assist and support Installation IAMs.

(20) Installation IAMs will provide reports to the RCIO IAPM.

e. IANM or IANO. The garrison commander or manager of the installation or activity responsible for the network will appoint an IANM for each installation or group of networks at all appropriate levels of command below ACOM and DA staff and field operating agencies, including subordinate commands, posts, installations, and tactical units. Appoint IANOs to assist IANMs as required. IANM and IANO positions will be designated IT–I or IT–II. A contractor will not fill the Installation IANM position. The IANM must be a U.S. citizen and hold a U.S. Government security clearance and access approval commensurate with the level of responsibility. Each IANM and IANO must be IA and vulnerability assessment technician (VAT) certified and must maintain his or her certification. The IANM and IANO, in addition to providing direct support to the IAM, will—

(1) Implement the IA program to ensure the AEI is operational and secure.

(2) Comply with and implement policy received from the appropriate network security manager or the IAM.

(3) Conduct reviews of the network architecture for vulnerabilities.

(4) Ensure measures and procedures used at network nodes support the security integrity of the network and comply with applicable directives.

(5) Develop, issue, and implement security procedures and protocols governing network operations per this regulation.

(6) Prepare, disseminate, and maintain plans, instructions, and standing operating procedures (SOPs) concerning network security.

(7) Conduct reviews of network threats and vulnerabilities per this regulation and the IAVM process.

(8) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(9) Review and evaluate the effects on security of changes to the network, including interfaces with other networks.

(10) Perform required monitoring of network resources per this regulation.

(11) Ensure the use of Army approved IA products from the IA Approved Products List.

(12) Implement IA and IAVM reporting and compliance procedures as set out in CJCSM 6510.01.

(13) Analyze and maintain network audit data.

(14) Ensure adequate network connectivity by making proper decisions concerning levels of confidentiality and robustness for the system.

f. IASO. The commander or manager/director of the activity responsible for the ISs will appoint an IASO for each IS or group of ISs. The same IASO may be appointed for multiple ISs. The IASO position will be designated IT–I, IT–II, or IT–III. A contractor may not fill MSC, installation, or post IASO positions at IT–I, if created. The IASO must be IA certified and maintain his or her certification. Appoint pre-deployment or operational IASOs for developmental systems with the applicable responsibilities. DOD uses the term IAO for IASO responsibilities. All IASOs will—

(1) Enforce IA policy, guidance, and training requirements per this regulation and identified BBPs.

(2) Ensure implementation of IAVM dissemination, reporting, and compliance procedures.

(3) Ensure all users meet the requisite favorable security investigations, clearances, authorization, need-to-know, and security responsibilities before granting access to the IS.

(4) Ensure users receive initial and annual IA awareness training.

(5) Ensure log files and audits are maintained and reviewed for all systems and that authentication (for example, password) policies are audited for compliance.

(6) Prepare, distribute, and maintain plans, instructions, and SOPs concerning system security.

(7) Review and evaluate the effects on security of system changes, including interfaces with other ISs and document all changes.

(8) Ensure that all ISs within their area of responsibility are certified, accredited and reaccredited.

(9) Maintain and document CM for IS software (including IS warning banners) and hardware.

(10) Pre-deployment or operational IASOs will ensure system recovery processes are monitored and that security features and procedures are properly restored.

(11) Pre-deployment or operational IASOs will maintain current software licenses and ensure security related documentation is current and accessible to properly authorized individuals.

(12) Tenant IASOs will support and assist tenant IAMs (or the installation IAM if no tenant IAM exists).

(13) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

3–3. Information assurance support personnel

In addition to the above described IA structure, other personnel have crucial responsibilities.

a. System or network administrators. System administrators (SAs) and network administrators (NAs) must be designated IT–I, IT–II, or IT–III (see para 4–14). Each SA/NA must be trained, experienced, IA certified, and currently certified on the ISs that they are required to maintain. The SA/NA should be a U.S. citizen and must hold a U.S. Government security clearance and local access approvals commensurate with the level of information processed on the system or network. SA/NA responsibilities include, but are not limited to, implementing the AIAP within their command, installation, or activity. SA/NAs will be designed on appointment orders and will—

(1) Enforce the IS security guidance policies as provided by the IAM and perform IASO duties if an IASO has not been appointed.

(2) Enforce system access, operation, maintenance, and disposition requirements.

(3) Ensure that personnel meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before granting access to the IS.

(4) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(5) Conduct required IAVM scanning and vulnerability assessments with approved software as authorized by their IAM/IASO. SAs/NAs are not limited to only IAVM scanning, but should be conducting comprehensive network assessments of their networks as authorized.

(6) Ensure CM includes all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, and service packs with IAM or IAPM approval.

(7) Ensure any system changes resulting from updating or patching are reported to the IAM/IASO.

(8) Record IAVM compliance in the Asset and Vulnerability Tracking Resource (A&VTR) database.

(9) Maintain current anti-virus (AV) engines and definitions on all ISs.

(10) Review and verify currency of user accounts, accesses, and logins. Remove departing users' accounts before departure. Terminate inactive accounts verified as no longer required that exceed 45 days.

(11) Suspend user accounts for the following types of actions: actions that knowingly threaten, damage, or harm the IS, network or communications security; revocation, suspension, or denial of security clearance or interim security clearance investigations; or unauthorized use of IS and networks per para 4–5.s.

(12) Remove or disable all default, guest, and service accounts in ISs or network devices, and rename administrative accounts as applicable.

(13) **Maintain and use at least 2 separate accounts for access to network resources, 1 for their privileged level access and a separate general user, non–privileged level account for routine procedures.**

(14) Review IS and network audit logs and log files, and report anomalous or suspicious information in accordance with Section VIII, Incident and Intrusion Reporting.

(15) Monitor IS performance to ensure that recovery processes, security features, and procedures are properly restored after an IS has been rebooted.

(16) Monitor IS performance to ensure that processes, security features, and operating system configurations are unaltered.

(17) Perform equipment custodian duties as necessary.

(18) Notify the IAM or IAPM when a system no longer processes sensitive or classified information, or when changes occur that might affect C&A, to obtain disposition or resolution instructions.

(19) Ensure CM for security-relevant IS software (including IS warning banners) and hardware is maintained and documented.

(20) Implement and test IS and data backup procedures for integrity.

(21) Prohibit attempts to strain or test security mechanisms or to perform network-line or keystroke monitoring without authorization.

(22) Establish audit trails, conduct reviews, and create archives as directed by the IAM.

(23) Will sign a Privileged-level Access Agreement (PAA) and a Non-Disclosure Agreement (NDA) as a prerequisite to maintaining their positions. Reference the IA BBP on PAA; AUP (https://informationassurance.us.army.mil).

b. Data owners. Data owners will, at a minimum, provide guidance or feedback to the System Owner (SO) concerning—

(1) The confidentiality of information under the data owner's purview.

(2) The DIACAP team's decision regarding the level of classification, confidentiality, integrity, availability, encryption, and protection requirements for the data at rest or in transit.

(3) Specific requirements for managing the owner's data (for example, incident response, information contamination to other system/media, and unique audit requirements).

(4) Whether FNs may access ISs accredited under this regulation. Access must be consistent with DOD, DA, and DIA governing directives (for example, AR 380–10 and DCIDs 1/7 and 5/6).

c. General users. Use of Government IS and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DiD strategy and their actions affect the most vulnerable portion of the AEI. Users must have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Users will—

(1) **Comply with the command's AUP for Government owned ISs and sign an AUP prior to or upon account activation.**

(2) Complete initial and/or annual IA training as defined in the IA training BBP (https://informationassurance.us.army.mil).

(3) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them with a valid need to know.

(4) Protect ISs and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(5) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(6) **Obtain prior approval for the use of any media (for example, USB, CD–ROM, floppy disk) from the SA/IAM.**

(7) **Scan all files, attachments, and media with an approved and installed AV product before opening a file or attachment or introducing media into the IS.**

(8) Report all known or suspected spam, chain letters, and violations of acceptable use to the SA, IAM, or IASO.

(9) Immediately stop using an infected IS; and report suspicious, erratic, or anomalous IS operations, and missing or added files, services, or programs to the SA/IASO in accordance with local policy.

(10) **Not disclose their individual account password or pass–phrase authenticators.**

(11) **Invoke password-protected screen locks on your workstation after not more than 15 minutes of non–use or inactivity.**

(12) **Logoff ISs at the end of each workday.**

(13) **Access only that data, control information, software, hardware, and firmware for which the user is authorized access.**

(14) Access only that data that they are authorized or have a need to know.

(15) **Assume only authorized roles and privileges as assigned.**

(16) Users authorized Government-provided IA products (for example, AV or personal firewalls) will be encouraged to install and update these products on their personal systems and may be required to do so as directed by the DAA and documented in the C&A package for any approved remote access.

d. COMSEC custodians and inspecting personnel. Execute responsibilities as required per this regulation and AR 380–40.

e. TEMPEST personnel. Execute responsibilities as required in AR 381–14.

f. Intelligence personnel. Senior intelligence officers (SIOs) or command intelligence officers (DCSINT/G2s/S2s) will—

(1) Ensure the command statement of intelligence interest (SII) (AR 381–10 and AR 381–20) registers requirements for the receipt of validated intelligence adversely affecting the integrity and reliability of ISs.

(2) Provide assistance in the identification of threat factors affecting the risk management approach for implementing security safeguards.

g. Force protection officers. Execute responsibilities as required by AR 525–13.

h. Information operations officers. Execute responsibilities as required by FM 3–13.

i. OPSEC officers. The primary OPSEC vulnerability is information made publicly accessible through Web sites and Web-enabled applications. Commanders and Directors will develop and implement an OPSEC review plan as part of their inspection programs. All content placed on a Web site will be reviewed for OPSEC sensitive information. Additionally, execute responsibilities as required per AR 530–1.

j. Public affairs officers (PAOs). Execute IA responsibilities as required per this and AR 25–1.

k. Acquisition officers. Include IA requirements in the acquisition phases and execute responsibilities as required by DOD 5000.2–R and NSTISSP No. 11.

l. DOIMs. Execute responsibilities per this regulation and AR 25–1.

m. DAAs (see para 5–8).

(1) The DAA will—

(a) Be a U.S. citizen.

(b) Hold a U.S. Government security clearance and access approvals commensurate with the level of information processed by the system under his or her jurisdiction.

(c) Be an employee of the U.S. Government and meet the grade requirements identified in paragraph 5–8.

(d) Complete the DAA Basics Computer Based Training prior to performing the duties of DAA.

(e) Request appointment from the CIO/G–6 for IS by name.

(f) Ensure the DAA position is designated as an IT–I, based on the duties assigned and the expected effects on the Army mission.

(g) Meet training and certification requirements in accordance with NSTISSI No. 4012.

(h) The DAA will understand the operational need for the systems and the operational consequences of not operating the systems. The DAA will have an in-depth knowledge of DiD to drive state-of-the-art acquisition, focus a robust training program, and institute executable policy across the IA enterprise.

(2) The DAA will ensure the following as a minimum—

(a) Proper C&A based on systems environment, mission assurance category (MAC) level, confidentiality level, and security safeguards in accordance with this regulation and the Interim DIACAP.

(b) Issue written memo or digitally signed e-mail IA C&A authorization statements (that is, interim approval to operate (IATO), interim authorization to test (IATT), approval to operate (ATO), denial of authorization to operate (DATO)), after receipt of CA recommendation.

(c) Maintain records (including use of IA tools) for all IS C&A activities under his or her purview.

(d) Accomplish roles and responsibilities as outlined in this regulation during each phase of the accreditation process and for each IS as required.

(e) Ensure operational IS security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.

(f) Incorporate security, C&A, and Networthiness as an element of the life cycle process.

(g) Ensure data owner requirements are met before granting any FN access to the system.

(h) Consider and acknowledge CI and criminal intelligence activities during the C&A process.

(i) Report security-related events to affected parties (for example, data owners, all involved DAAs). DAAs must coordinate with investigative activities (for example, CCIU, RCERT) before making notifications.

(j) Assign written security responsibilities to the individuals reporting directly to the DAA (for example, IAM or an IASO if an IAM does not exist).

(k) Appoint a CA for each IS (or group of ISs) and network.

(l) Ensure CSLA certification of cryptographic applications occurs during the C&A process.

n. CA. Authority and responsibility for certification is vested in the Army FISMA Senior IA Officer (SIAO). The

Director OIA&C, NETC–EST–I, was appointed FISMA SIAO by the CIO/G–6 and will be the single Army certification authority (see para 5–2).

o. Agent of the certification authority (ACA). (See also para 5–9). The Army CA will maintain a list of qualified Government organizations and labs, as Agents of the CA (ACA), to perform the certification activities. The ACAs, funded by the SOs, are available to provide SOs with certification capabilities. Organizations can request appointment as an ACA by following the process in the ACA BBP.

p. SO. A Government SO will be identified for each IS used by or in support of the Army. The SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented. and provided as an artifact to the accreditation package (see para 5–10).

q. Host and tenant responsibilities. Army tenant units or activities must comply with the IA requirements of their parent ACOM/ASCC and their supporting installation. Army and non-Army tenant operations must comply with the host installation's IA policy if they connect to the installation's information infrastructure. Army tenant units or activities and units based in or under operational control (OPCON) of an ACOM/ASCC other than their parent will comply with the IA requirements of both parent and host commands. Address unresolved conflicts of IA policy per this regulation through local command channels and RCIOs to HQDA, CIO/G–6. Until CIO/G–6 resolves the conflict, the provisions of this regulation will apply, including those pertaining to the use of gateways or information management resources as pathways to connect their ISs. If the non-Army tenant uses any part of the host installation infrastructure, the installation IAM will require the use of CM controls consistent with the installation's information management and CM process. All tenant activities will—

(1) Identify and coordinate all system upgrades, fieldings, pilots, tests, and operations of new or upgraded systems with the installation IAM, DAA, and DOIM.

(2) Identify ISs and provide the approved C&A documentation to the installation IAM.

(3) Identify their security support requirements to the installation IAM and provide technical assistance, as required.

(4) Identify appropriate IA personnel to the installation IAM.

(5) Support installation IA efforts and requirements, and identify constraints in sufficient time to permit coordination and preparation of a viable IS security solution.

(6) Coordinate and conduct vulnerability assessments or compliance scanning, and report completion and results as required.

Chapter 4
Information Assurance Policy

Section I
General Policy

4–1. Policy overview

This chapter provides policy to implement IA requirements developed to respond to the IA challenge, as defined in Public Law, National Security, DOD, and Army directives, policies, and regulations.

a. Implement all security analyses, security engineering, and security countermeasures to protect ISs within the framework of risk management and adherence to public laws, DOD directives, and Army regulations.

b. Define a security policy and a protection profile for ISs during concept development. Consider security requirements based on these items throughout the IS life cycle.

c. The IS developer will ensure the early and continuous involvement of the functional proponent, threat and risk assessors, users, IA personnel, data owners, certification authorities, and DAAs in defining and implementing security requirements of the IS.

d. Statements of security requirements will be included in the acquisition and procurement specifications and contracts for ISs, products, and services. Purchases will be in accordance with Army contracting and acquisition guidelines, Blanket Purchase Agreements (BPAs), and IA-approved products. NIST Special Publication 800–64 REV.1 may be referenced for specification, tasks, and clauses that are used in writing contracts. The statements will reflect an initial risk assessment and will specify the required protection level per DODD 8500.1 and DODI 8500.2.

e. The ACOMs, ASCCs, DRUs, direct reporting PMs, or functional proponents will not field, and commanders will not accept, systems—

(1) That do not meet minimum security standards stated in the acquisition and procurement specifications.

(2) For which a C&A authorization has not been obtained from the appropriate DAA.

f. Commanders are responsible for ensuring that ISs under their purview are operated in a manner consistent with the system C&A package and this regulation.

g. Development and modification to existing ISs will be performed in a manner that makes security an integral part of the development, acquisition, fielding, and operational processes.

h. All ISs will be subjected to the acquisition life cycle per AR 70–1.

i. AR 525–13 prescribes policies and procedures for the Army antiterrorism program and assigns responsibilities for including defensive information operations.

4–2. Funding

HQDA will manage and provide annual IA initiatives funding guidance and support required for Management Decision Packages (MDEPs) MS4X and MX5T, and others as appropriate. Funding guidance will change from year to year, and CIO/G–6 will publish annual guidance on the submission of IA requirements and the CIO/G–6 validation processes of those submitted requirements. This funding and budgeting process will continue under the Army Information System Security Program (AISSP) direction and guidance. This annual guidance provided to IAPMs and other appropriate personnel will identify valid IA submission requirements and the type of information required. CIO/G–6 will present validated IA requirements to the appropriate Program Evaluation Group (PEG).

a. Reporting requirements. The RCIOs and ACOMs/ASCCs will provide the MDEP MS4X Report (illustrated in table 4–1) to the HQDA, CIO/G–6, as indicated below—

(1) Submit fiscal year (FY)-phased execution plans to the CIO/G–6 no later than 10 August of each year.

(2) Funded commands must provide a detailed midyear and yearend actual execution report.

(a) The midyear actual execution report is due to the CIO/G–6 not later than 10 May of each fiscal year.

(b) The yearend actual execution report is due to the CIO/G–6 not later than 10 October of each fiscal year.

(c) Both the midyear and yearend actual execution reports must be tied to phased execution plans and reconciled with the official Execution Database Summary (218) report.

(d) Review execution reports for unauthorized expenditures and unauthorized fund reprogramming.

(e) HQDA, CIO/G–6 will monitor program execution on a regular basis.

(f) Commands receiving MDEP MS4X funds will submit semi-annual reports. (Reporting Requirements (RCS: CSIM–62).)

Table 4–1
MDEP MS4X, Information Assurance Phased Funding Utilization Plan/Actual Execution Report (RCS: CSIM–62)
For period ending 092009 (MMYYYY)

Project execution data (09/09)	Phased Fund Utilization Plan Item (for example, training (what type and number of participants); specific equipment items)	Estimated cost ($000)	Actual obligation ($000)	Date obligated ($000) (09/08)	Actual execution Remarks: (for example, status of procurement action, explanation for non-execution of funds in line with execution plan; explain what specific equipment items will be used for)

b. MDEP MX5T funds. MDEP MX5T funds are used in centralized procurement of COMSEC and IA equipment within the Army. The following guidance is provided:

(1) Commanders are responsible for developing their respective command and combatant command-level MX5T requirements. Inputs will be staffed through their local IA channels and provided to the RCIO and HQDA for all their sub-activities and subordinate commands.

(2) Garrison commanders and tenant activities will report INFOSEC, COMSEC, and IA requirements to their respective RCIOs.

(3) PEOs are responsible for developing, managing, and providing input to the HQDA for all their PMs.

(4) A PM that reports directly to HQDA is responsible for developing requirements and providing his or her input to HQDA.

(5) Forecast data over a 15-year period for the purpose of short-term, mid-term, and long-term funding projections. Provide this data to the CSLA database located at Fort Huachuca, Arizona. Provide the following minimum data:

(a) Name of INFOSEC, COMSEC, or IA system, equipment, or product needed.

(b) Name of system requiring INFOSEC, COMSEC, or IA systems, equipment, or products.

(c) Quantity of each type of INFOSEC, COMSEC, or IA equipment needed starting with the first year of the program objective memorandum (POM).

(d) Name of the approving authority.

(e) Point of contact's name, mailing address, and e-mail and Defense Message System (DMS) addresses.

(f) Name of operational requirements document (ORD) and date approved.

(g) Short description of system.

(h) Other information as directed by HQDA CIO/G–6 or DCS, G–3.

(6) Submission of un-resourced requirements will be to CIO/G–6, Attention: NETC–ESTA–I.

4–3. Information assurance training

All individuals appointed as IA or network operations personnel must successfully complete an IA security training certification course of instruction equivalent to the duties assigned to them. Individuals must also be certified in accordance with the DOD baseline requirements of DOD 8570.1M. Personnel with privileged access must sign a privileged level user agreement.

a. Requirements.

(1) IAPM will—

(a) Complete the Army IAM course within 6 months of appointment.

(b) Methods of training are an Army IAM course, Army E-learning modules, or other Service or agency equivalent.

(c) Provide completion date to the A&VTR compliance-reporting database within 2 weeks of course completion.

(d) Complete applicable DOD baseline management certification.

(2) IANM will—

(a) Comply with paragraphs *a*(1)(a), *a*(1)(c), and *a*(1)(d), above.

(b) Complete the SA/NM security course (at Fort Gordon or a mirror site) within 6 months of appointment.

(3) IAM will comply with paragraphs *a*(1)(a), *a*(1)(c), and *a*(1)(d), above.

(4) IANO will comply with paragraphs *a*(1)(a), *a*(1)(c), and *a*(1)(d), above.

(5) IASO will—

(a) Complete an IASO Course within 6 months of appointment. Methods of training are Web based (http://ia.gordon.army.mil), DISA Information Assurance Policy and Technology (IAP&T) Web Based Training at http://iase.disa.mil/eta/index.html), Army E–Learning/CBT IA modules, command (or other Service) course, or the IAM course.

(b) Comply with paragraphs *a*(1)(c) and *a*(1)(d), above.

(6) SAs will—

(a) Complete introductory training (Level I) within 6 months of assuming position. SAs will be certified to Level I as a minimum. Methods include the IASO Course online at Fort Gordon, IAM Course, Army E–Learning modules, DISA Information IAP&T CDROMs, or the equivalent command or other Service IASO- or IAM-level courses. RCIOs or command IA personnel (as applicable) will determine if limits on SA duties warrant certification to Level I only.

(b) Complete technical training (Level II) SA Security Course (schedules available at http://ia.gordon.army.mil) or a Command-equivalent course within 6 months of assuming position.

(c) Complete advanced training (Level III) at the National Guard Bureau (NGB) Computer Emergency Response Team Operational Training Experience (CERT OTE) or USAR Computer Network Defense Course (CNDC) courses, or other Service or agency equivalents as required.

(d) Complete applicable DOD technical and computing environment baseline certifications.

(e) Comply with paragraph*a*(1)(c), above.

(7) Contracting officer's representatives (CORs). Contracting officer's representatives will compare contractor qualifications to the statement of work/ performance work statement requirements to ensure contractor-nominated IA and SA positions meet minimum requirements before acceptance for employment. If the personnel provided are non-compliant with the statement of work requirements, the COR will notify the Contracting Officer for implementation of contract remedies.

(8) IA user awareness training. IAMs, SAs, and IASOs will ensure that a user-training program is in place for all users in the command. Online user training courses can be found
http://ia.gordon.army.mil and http://usarmy.skillport.com.

(a) All users must receive IA awareness training tailored to the system and information accessible before issuance of a password for network access. The training will include the following:

1. Threats, vulnerabilities, and risks associated with the system. This portion will include specific information regarding measures to reduce malicious logic threats, principles of shared risk, external and internal threat concerns, acceptable use, privacy issues, prohibitions on loading unauthorized software or hardware devices, and the requirement for frequent backups.

2. Information security objectives (that is, what needs to be protected).

3. Responsibilities and accountability associated with IA.

4. Information accessibility, handling, and storage considerations.

5. Physical and environmental considerations necessary to protect the system.

6. System data and access controls.

7. Emergency and disaster plans.

8. Authorized systems configuration and associated CM requirements.

9. Incident, intrusion, malicious logic, virus, abnormal program, or system response reporting requirements.

10. INFOCON requirements and definitions.

11. AUP requirements.

(b) Users will receive annual refresher training as a minimum or as conditions warrant.

(9) Vulnerability assessment certification. IA personnel conducting vulnerability assessments on ISs must achieve VAT certification through their supporting RCERT or TNOSC. (This is not equivalent to the IAVM program assessment procedures.) Additional guidance and procedures in accordance with the policy can be found on the IA BBP Web site.

b. Refresher training. Refresher training for IAPMs, IAMs, IANMs, IASOs, and SAs/NAs will be attendance at an IA workshop every 18–24 months, attendance at DOD-sponsored IA workshops, completion of modules in Army E–Learning IA learning path, or approved commercial courses. Baseline certifications will be maintained in accordance with the requirements of the certifying body.

c. Substitutions or equivalencies.

(1) IAPMs, IAMs, IASOs, and IANMs can substitute other Service or Agency courses to fulfill these requirements. Identify the substitute course, duration, and sponsor when tracking completion dates and A&VTR input.

(2) SAs and IANMs can substitute courses to fulfill the technical training (Level II) requirement.

(3) Substitute coursework must include all topics of the SA Security Course managed by Fort Gordon. For approval of substitute coursework, send an e-mail request to NETCOM/9th SC (A), OIA&C.

(4) Successful completion of the Level III course managed by NGB or the USAR will fulfill Level II certification requirements.

4–4. Mission assurance category, levels of confidentiality, and levels of robustness

a. Mission assurance category. All ISs will be assigned a mission assurance category that reflects the importance of the information relative to the achievement of DOD goals and objectives. The IS mission assurance category will be determined by the DOD or Army proponent and agreed upon by the DIACAP team. The MAC level is used to determine the IA Controls for integrity and availability in accordance with DODI 8500.2. Refer to DODI 8500.2 (http://iase.disa.mil/policy.html) for additional detailed guidance and procedures for defining or assigning mission assurance categories.

(1) MAC I is a high integrity, high availability for DOD ISs handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability is unacceptable and could include the immediate and sustained loss of mission effectiveness.

(2) MAC II is a high integrity, medium availability for DOD ISs handling information that is important to the support of deployed and contingency forces. The consequence of loss of integrity is unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time.

(3) MAC III is a basic integrity, basic availability for DOD ISs handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness.

b. Confidentiality levels. All ISs will be assigned a confidentiality level based on the classification or sensitivity of the information processed. The confidentiality level is used to establish acceptable access factors and to determine the DODI 8500.2 IA Controls applicable to the information system. DOD has defined the following three confidentiality levels:

(1) Classified — Information designated top secret, secret or confidential in accordance with Executive Order 12356.

(2) Sensitive — Information the loss, or unauthorized access to or modification of could adversely affect the national interest or conduct of Federal programs, or Privacy Act information. Includes, but is not limited to For Official Use Only (FOUO), Privacy data, unclassified controlled nuclear information, and unclassified technical data.

(3) Public – Information has been reviewed and approved for public release.

c. Levels of robustness. All ISs will employ protection mechanisms that satisfy criteria for basic, medium, or high levels of robustness per DODI 8500.2 and Federal Information Processing Standard (FIPS) 140–2. Each IS will be managed and operated to achieve the appropriate level of protection for the applicable functional security requirements.

(1) *High robustness.* High robustness is the security services and mechanisms that provide the most stringent protection and rigorous security countermeasures. Generally, high robustness technical solutions require NSA-certified high-robustness solutions for cryptography, access control and key management, and high assurance security design as specified in NSA-endorsed high robustness protection profiles, where available.

(2) *Medium robustness.* Medium robustness is security services and mechanisms that provide for layering of additional safeguards above good commercial practices. Medium robustness technical solutions require, at a minimum, strong (for example, crypto-based) authenticated access control, NSA-approved key management, NIST FIPS-validated cryptography, and the assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for medium robustness.

(3) *Basic robustness.* Basic robustness is the security services and mechanisms that equate to best commercial practices. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPS-validated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness.

d. Level of total system exposure. The appropriate level of protection for each functional security requirement will be determined using a combination of the mission assurance category, level of confidentiality, and level of robustness.

(1) Each IS will be reviewed against the mission assurance category definitions provided in DODI 8500.2, Enclosure 2, and assigned to a mission assurance category.

(2) Each IS will be assigned a confidentiality level based on the classification or sensitivity of the information processed, stored, or transmitted.

(3) Determine the applicable IA controls from DODI 8500.2.

(4) The identified controls for the level of total system exposure serve as the baseline IA requirements for C&A or reaccredidation and will be reassessed and revalidated every 3 years as a minimum.

4–5. Minimum information assurance requirements

All required risk analyses will evaluate and identify possible vulnerabilities and adverse security effects on associated ISs and networks. Although manual procedures are acceptable when an automated safeguard is not feasible, IA personnel will embed automated security safeguards into the design and acquisition of ISs to ensure a secure infrastructure.

a. Prohibited activities. In addition to the prohibited activities listed in AR 25–1, the following activities are specifically prohibited by any authorized user on a Government provided IS or connection:

(1) **Use of ISs for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.**

(2) **Installation of software, configuration of an IS, or connecting any ISs to a distributed computer environment (DCE), for example the SETI project or the human genome research programs.**

(3) **Modification of the IS or software, use of it in any manner other than its intended purpose, or adding user–configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications.** These applications create exploitable vulnerabilities and circumvent normal means of securing and monitoring network activity and provide a vector for the introduction of malicious code, remote access, network intrusions or the exfiltration of protected data.

(4) **Attempts to strain, test, circumvent, or bypass network or IS security mechanisms, or to perform network or keystroke monitoring.** RCERTs, Red Team, or other official activities, operating in their official capacities only, may be exempted from this requirement.

(5) **Physical relocation or changes to configuration or network connectivity of IS equipment.**

(6) **Installation of non-Government-owned computing systems or devices without prior authorization of the appointed DAA including but not limited to USB devices, external media, personal or contractor-owned laptops, and MCDs.**

(7) Release, disclose, transfer, possess, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380–5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

(8) **Sharing personal accounts and authenticators (passwords or PINs) or permitting the use of remote access capabilities through Government provided resources with any unauthorized individual.**

(9) **Disabling or removing security or protective software and other mechanisms and their associated logs from IS.**

b. Accreditation. ISs and networks will be accredited in accordance with interim DOD and Army DIACAP documentation and Army supplemental networthiness guidance.

c. Access control. IA personnel will implement system and device access controls using the principle of least privilege (POLP) via automated or manual means to actively protect the IS from compromise, unauthorized use or access, and manipulation. IA personnel will immediately report unauthorized accesses or attempts to their servicing RCERT in accordance with Section VIII, Incident and Intrusion reporting. Commanders and DAAs will—

(1) Enforce users' suspensions and revocation for violations of access authorization or violation in accordance with para 3–3*c*(13).

(2) Develop the approval processes for specific groups and users.

(3) Validate individual security investigation (or approve interim access) requirements before authorizing IS access by any user.

(4) Verify systems are configured to automatically generate an auditable record or log entry for each access granted or attempted.

(5) Validate that systems identify users through the user's use of unique user identifications (USERIDs).

(6) Validate that systems authenticate users through the use of the CAC as a two-factor authentication mechanism. The CAC has certificates on the integrated circuit chip (ICC), and will be used as the primary user identifier and access authenticator to systems.

(7) Validate system configurations to authenticate user access to all systems with a minimum of a USERID and an authenticator when the systems are incapable of CAC enablement until these are replaced. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.

(8) Verify that system configurations use password-protected screen savers, screen locks, or other lockout features to protect against unauthorized access of ISs during periods of temporary non-use. Ensure such mechanisms automatically activate when a terminal is left unattended or unused. The DOD activation standard is established at 15 minutes. Establish a shorter period when IS are used in a multinational or coalition work area. In instances where the unattended lockout feature hinders operations, for example; standalone briefing presentation systems, medical triage devices, or operating room systems status; the DAA and SO can approve longer timeouts as an exception only when it imposes a minimum of risk, other control mechanisms are enabled to mitigate these risks, and documented in the C&A package. However the timeout feature will never be disabled and the system will never remain unattended during this extended use period. Exceptions will never be granted for matters of convenience or ease of use.

(9) Validate that system configurations prohibit anonymous accesses or accounts (for example, Student1, Student2, Patron1, Patron2, anonymous).

(10) Prohibit the use of generic group accounts. Permit exceptions only on a case-by-case basis when supporting an operational or administrative requirement such as watch-standing or helpdesk accounts, or that require continuity of operations, functions, or capabilities. IAMs will implement procedures to identify and audit users of group accounts through other operational mechanisms such as duty logs.

(11) Verify that system configurations limit the number of user failed log-on attempts to three before denying access to (locking) that account, when account locking is supported by the IS or device. If IS-supported, the system will prevent rapid retries when an authenticator is incorrectly entered and gives no indications or error messages that either the authenticator or ID was incorrectly entered (for example, implement time delays between failed attempts).

(12) Verify that system configurations generate audit logs, and investigate security event violations when the maximum number of authentication attempts is exceeded, the maximum number of attempts from one IS is exceeded, or the maximum number of failed attempts over a set period is exceeded.

(13) Reinstate accesses only after the appropriate IA (for example, SA/NA) personnel have verified the reason for failed log-on attempts and have confirmed the access-holder's identity. Permit automatic account unlocking, for example, after an established time period has elapsed, as documented in the C&A package and approved by the DAA, based on sensitivity of the data or access requirements.

(14) If documented in the C&A package and authorized by the DAA, time-based lockouts (that is, access is restricted based on time or access controls based on IP address, terminal port, or combinations of these) and barriers that require some time to elapse to enable bypassing may be used. In those instances the DAA will specify, as a compensatory measure, the following policies:

(a) Implement mandatory audit trails to record all successful and unsuccessful log-on attempts.

(b) Within 72 hours of any failed log-on and user lockout, IA personnel will verify the reason for failure and implement corrective actions or report the attempted unauthorized access.

(c) The SA will maintain a written record of all reasons for failure for 1 year.

(15) Enforce temporary disabling of all accounts for deployed forces on garrison networks unless the accounts are operationally required.

(16) Create and enforce procedures for suspending, changing, or deleting accounts and access privileges for deployed forces in the event of capture, loss, or death of personnel having network privilege-level access.

(17) Create and enforce access auditing, and protect physical access control events (for example, card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts as required.

d. Remote access (RA).

(1) Systems being used for remote access must meet security configurations to include IAVM, certification and accreditation standards, and will employ host-based security, for example a firewall and IDS, with AV software before authorization to connect to any remote access server. Security configurations will be reviewed quarterly.

(2) Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

(3) Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

(4) Users will protect RA ISs and data consistent with the level of information retrieved during the session.

(5) Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

(6) Remote access users will read and sign security and end-user agreements for remote access annually as a condition for continued access.

e. Remote access servers (RASs).

(1) Secure remote terminal devices consistent with the mode of operation and sensitivity of the information and implement non-repudiation measures when necessary.

(2) Any IS that provides RAS capabilities will employ host-based firewalls and intrusion detection systems to detect unauthorized access and to prevent exploitation of network services.

(3) Any RAS being accessed remotely will employ a "Time-Out" protection feature that automatically disconnects the remote device after a predetermined period of inactivity has elapsed, dependent on classification level of the information, but no longer than 10 minutes.

(4) Remote access users will be required to authenticate all dial-in operations with a unique USERID and password, compliant with the remote authentication dial-in user system (RADIUS) standard.

(5) All RAs will terminate at a centrally managed access point located within a demilitarized zone (DMZ) that is configured to log user activities during a session.

(6) Prohibit all RA (that is, virtual private network (VPN), dial-in) to individual ISs within an enclave (that is, behind the DMZ firewall).

(7) DOIMs and IAMs must ensure all remote access servers (RASs) undergo CM and C&A processes.

(8) Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable dial-in modems.

(9) Physical security for the terminal will meet the requirements for storage of data at the highest classification level received at the terminal and must be implemented within a restricted access area.

(10) Data between the client and the RAS will be encrypted to provide confidentiality, identification, non-repudiation and authentication of the data. The CAC provides the user with an official certificate.

(11) Approved telework or telecommuting access will be in accordance with established DOIM, RCIO, and NETCOM/9th SC (A) C&A access procedures from a Government provided system only. Ad hoc telework access (defined as one-time, informal, or on an infrequent basis) will be through existing and approved external access methods or portals such as Terminal Server Access Control System (TSACS) or the Army Knowledge Online (AKO) Web site.

(12) Outside the continental United States (OCONUS) telework procedures and authorization will be approved by the DAA and RCIO on a case-by-case basis and documented in the C&A package.

(13) Audit all RAS connections at a minimum weekly.

(14) Review RAS devices biweekly for security configuration, patches, updates, and IAVM compliance.

f. Configuration management requirements. The following policy will be the minimum used for the CM of all systems:

(1) All CM plans will include a maintenance and update strategy to proactively manage all IS and networks with the latest security or application updates. While IAVM is part of a CM strategy, it is not all-inclusive for every IS in use in the Army. All ISs will have a vulnerability management strategy for testing and maintaining patches, updates, and upgrades.

(2) Hardware and software changes to an accredited IS, with an established baseline, will be effected through the CM process.

(3) The CCB or the CMB for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without the express written consent of the IAM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate commander or manager will provide the consent on the advice of the cognizant IA official.

(4) Modifying, installing, or downloading of any software on any computer system may affect system C&A and must be evaluated and approved by the IAM with the local CMB, CCB, and DAA.

(5) Configuration management controls, including version controls, will be maintained on all software development efforts; RDT&E activities; follow-on test and evaluation (FOT&E) activities; and other related tests by the software designer. A CM "baseline image" will be created, documented, kept current, and maintained by network and system administration personnel for all ISs within their span of control. Exceptions to this baseline image will be documented in the C&A package and approved by the DAA.

(6) The minimum baseline configuration for ISs will be the published Security Technical Implementation Guide (STIG) requirements or the common criteria protection profiles for IA products, as available or supplemented and

published by DOD and NETCOM/9th SC (A), with any changes documented. STIGS are located at: http://iase.disa.mil/stigs/index.html.

(7) Prohibit default installations of "out of the box" configurations of COTS purchased products. COTS purchased products will require system CM and IAVM compliance as a minimum. Comprehensive vulnerability assessments of the test IS will be conducted and documented before and after installation of any COTS products under consideration for CM review or approval.

(8) Upon acceptance for operational use (whether developmental, GOTS, or COTS), keep software under close and continuous CM controls to prevent unauthorized changes.

(9) ISs must meet minimum levels of total system exposure. See paragraph 4–4 and DODI 8500.2 to establish IA baseline requirements.

g. Assessments. Commanders will verify that IA personnel conduct initial and continual assessments to detect IS and network vulnerabilities using approved tools, tactics, and techniques to facilitate the risk management process and to ensure compliance with network management, CM, IAVM requirements, and security policies and procedures. Commanders and IA personnel will ensure that all networks and networked ISs undergo a self-assessed, vulnerability assessment scan quarterly. Prohibit the use of commercial scanning services or vendors without the CIO/G6's chief information security officer's (CISO) approval.

h. Auditing. SAs will configure ISs to automatically log all access attempts. Audits of IS will be either automated or manual means. SAs will implement audit mechanisms for those ISs that support multiple users.

(1) Use audit servers to consolidate system audit logs for centralized review to remove the potential for unauthorized editing or deletion of audit logs in the event of an incident or compromise.

(2) Commands, organizations, tenants, activities, and installations will support centralized audit server implementations in the enterprise.

(3) Centralized audit servers logs will be maintained for a minimum of 1 year.

(4) Conduct self-inspections by the respective SA/NA or IA manager.

(5) Enable and refine default IS logging capabilities to identify abnormal or potentially suspicious local or network activity—

(a) Investigate all failed login attempts or account lockouts.

(b) Maintain audit trails in sufficient detail to reconstruct events in determining the causes of compromise and magnitude of damage should a malfunction or a security violation occurs. Maintain system audit logs locally for no less than 90 days.

(c) Retain classified and sensitive IS audit files for 1 year (5 years for SCI systems, depending on storage capability).

(d) Provide audit logs to the ACERT, Army–Global Network Operations and Security Center (A–GNOSC), LE, or CI personnel to support forensic, criminal, or counter-intelligence investigations as required.

(e) Review logs and audit trails at a minimum weekly, more frequently if required, and take appropriate actions.

i. Contingency planning. A contingency plan is a plan for emergency response, backup operations, transfer of operations, and post-disaster recovery procedures maintained by an activity as a part of its IA security program. Commanders will create and practice contingency plans for each IS (a single IS or local area netwrok (LAN)) for critical assets as identified by the data owner or commander to support continuity of operations planning (COOP). See DA Pam 25–1–2 for additional guidance and procedures for developing contingency plans. Exercise contingency plans annually.

j. Data integrity.

(1) Implement safeguards to detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data.

(2) Implement safeguards to ensure that security classification levels remain with the transmitted data.

(3) DAA will identify data owners for each database on their networks. Only the original classification authority (OCA) is authorized to change the data classification.

(4) DAA will develop and enforce policies and procedures to routinely or automatically backup, verify, and restore (as required) data, ISs, or devices at every level. These policies and procedures will be captured in the C&A package.

(5) Use data or data sources that have verifiable or trusted information. Examples of trusted sources include, but are not limited to, information published on DOD and Army sites and vendor sites that use verified source code or cryptographic hash values.

(6) Protect data at rest (for example, databases, files) to the classification level of the information with authorized encryption and strict access control measures implemented.

k. C&A package. The C&A package will be available to the site-assigned IASO for the life of each IS or LAN, including operational, prototype, test, or developmental systems. This C&A package will include at a minimum the System Identification Profile (SIP), Scorecard, and plan of action and milestones (POA&M).

l. IA product acquisition. All security-related COTS hardware, firmware, and software components (excluding cryptographic modules) required to protect ISs will be acquired in accordance with public law and will have been

evaluated and validated in accordance with appropriate criteria, schemes, or protection profiles (http://www.nia-p.nist.gov/) and this regulation. IA products listed on the CSLA managed Army approved products list will be evaluated/selected first, and then procured through managed Army Blanket Purchase Agreement (BPA) contract vehicles before other IA products are evaluated. For PEO/PM's, the CSLA BPA requirements only applies to the procurement of COMSEC devices. All GOTS products will be evaluated by NSA or in accordance with NSA-approved processes. NETCOM/9th SC (A) and CIO/G–6 may approve exceptions to IA products evaluations when no criteria, protection profile, or schema exists or is under development, and the removal or prohibition of such an IA product would significantly degrade or reduce the ability of personnel to secure, manage, and protect the infrastructure.

m. Notice and consent procedures. Commanders will verify that all computers under their control, independently, prominently and completely display the Notice and Consent Banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services access.

(1) General Notification: Army users of DOD telecommunications systems or devices are advised that DOD provides such systems and devices for conducting authorized use. Users are subject to telecommunications monitoring, including their personal communications and stored information.

(2) Using Government telecommunications systems and devices constitutes the user's consent to monitoring.

(3) Users will be advised that there is no expectation of privacy while using ISs or accessing Army resources.

(4) The user must take a positive action to accept the terms of the notice and consent warning banner before a successful logon is completed.

(5) Post appropriate warning banners and labels in accordance with this regulation.

(6) The following access warning banner replaces the warning banner in AR 380–53 and will not be modified further. The banner to be posted on Army networks, systems, and devices will state—

(7) "WARNING! This computer is the property of the United States Department of Defense and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department may monitor any official or personal activity or communication on this system and retrieve any information stored within this system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for any lawful purpose, including, but not limited to. 1) a properly authorized law enforcement or counterintelligence investigation. 2) information systems security monitoring. 3) an Inspector General inspection, investigation, or inquiry. or 4) or other authorized administrative investigation. Users have no expectation of privacy with respect to any information, either official or personal, transmitted over, or stored within this system, including information stored locally on the hard drive or other media used with this computer to include removable media or hand-held peripherals devices."

(8) For those personal computing devices, such as PDAs, that have technical limitations to the full banner, then the only approved solution will be "Contents subject to search. See AR 25–2, 4–5*m*(7)."

(9) For media devices, services, protocols, and other limited text input requirements other than PDA devices requiring access, such as routers, firewalls, bannered access ports, and so forth. This banner will be "Subject to Army Warning banner in AR 25–2, 4–5*m*(7)."

n. Virus protection. Implement the virus protection guidance provided below on all ISs and networks, regardless of classification or purpose—

(1) Users and SAs will scan all files, removable media, and software, including new "shrink-wrapped" COTS software, with an installed and authorized AV product before introducing them onto an IS or network. Files, media and software found to be infected with a virus will be reported by users to the SA.

(2) To minimize the risks of viruses, implement the following countermeasures:

(a) SAs will configure all ISs with a current and supportable version of the AV software configured to provide real-time protection from the approved products list with automated updates and reporting enabled.

(b) IA personnel should take the multilevel approach to virus detection by installing one AV package on the workstations and a different AV package on the servers.

(c) SAs will update virus definitions at a minimum weekly, or as directed by the ACERT for immediate threat reduction. Virus definition availability is based on vendors' capabilities. IA personnel will institute automated antivirus definition updates as published or available from authorized DOD or Army sites.

(3) IA personnel will train users to recognize and report virus symptoms immediately.

(4) IAMs will implement virus-reporting procedures to support DOD and Army reporting requirements.

o. Mobile code.

(1) Mobile code is executable software, transferred across a network, downloaded, and executed on a local system without notification to, or explicit installation and execution by, the recipient.

(2) Mobile code has the potential to severely degrade operations if improperly used or controlled. The objective of the mobile code security policy is to deny untrusted mobile code the ability to traverse the Army enterprise. As a minimum, the Army mobile code mitigation policy will be implemented to support the DOD mobile code policy. Untrusted mobile code will not be allowed to traverse the enterprise unless NETCOM/9th SC (A) CCB-approved mitigating actions have been emplaced.

p. Layering.

(1) Layering is a process of implementing similar security configurations or mechanisms at multiple points in an IS architecture. Doing so eliminates single points of failure, provides redundant capabilities, increases access granularity and auditing, and implements an effective computer or network attack detection and reaction capability.

(2) The Army enterprise IA security DiD structure requires a layering of security policies, procedures, and technology, including best practices such as redundant capabilities or use of alternative operating systems, to protect all network resources within the enterprise. Layered defenses at the boundaries, for example, include, but are not limited to using inbound and outbound proxy services, firewalls, IDSs, IPSs, and DMZs.

q. Filtering. Filtering policies will block ingress and egress services, content, sources, destinations, ports, and protocols not required or authorized across the enterprise boundary. Router and firewall access control lists (ACLs) provide a basic level of access control over network connections based on security or operational policy.

(1) Filtering at the enterprise boundary is the primary responsibility of the NETCOM/9th SC (A) TNOSCs using tools and techniques applied at the enterprise level.

(2) At all levels subordinate to NETCOM/9th SC (A), filtering policies and technology will be implemented and layered throughout the architecture and enforced at all capable devices. Audit and system or device generated event logs will be provided to NETCOM/9th SC (A). These policies should be complementary.

(3) Filtering products and techniques are intended to proactively reduce ingress and egress security threats to enterprise systems and information without targeting specific individuals. The most common threats are associated with malicious content, misuse, security policy violations, content policy violations, or criminal activity. Threat mitigation policies will be incorporated, configured, and monitored to reduce or identify these threats and include, but are not limited to, ACL configuration on routing devices to prevent access to unauthorized sites, AV installations, cache or proxy servers (to maintain connection state), firewalls, mail exchange configurations (for example, auto-deletion of attachments), network monitoring software such as IDS or Intrusion Prevention System (IPS) configured to terminate suspicious traffic, content management, or web filtering applications.

r. AUP.

(1) Commanders and Directors will implement an AUP for all user accesses under their control (see the sample AUP at appendix B).

(2) Users will review and sign an AUP prior to or upon account activation. Digital signatures are authorized.

(3) IA personnel will maintain documented training records.

(4) DOD policy states that Federal Government communication systems and equipment (including Government-owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only.

(5) Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a theater commander for Soldiers and civilian employees deployed for extended periods away from home on official business.

(6) Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include limited personal use established by appropriate authorities under the guidelines of the Joint Ethics Regulation (DOD 5500.7–R).

(7) Certain activities are never authorized on Army networks. AUPs will include the following minimums as prohibited. These activities include any personal use of Government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

s. Monitoring networks.

(1) Network monitoring includes any of a number of actions by IA personnel aimed at ensuring proper performance and management. When any of these monitoring activities involve intercepting (capturing in real time) the contents of wire or electronic communications, they must fall within the limits of the service provider exception to the Federal wiretap statute. The service provider exception allows system and network administrators to intercept, use, and disclose intercepted communications as long as the actions are conducted in the normal course of employment and the SA/NA is engaged in an activity that is necessary to keep the service operational or to protect the rights or property of the service provider. Therefore, IA personnel must consult with legal counsel to ensure that their activities involving systems management and protection are properly authorized.

(2) IA personnel performing ingress and egress network monitoring or filtering activities are authorized to use CIO/G–6-approved automated monitoring tools maintained and configured by NETCOM/9th SC (A) as network devices to aid in the performance and management. It is important to recognize that the SA/NA does not have unlimited authority in the use of these network monitoring tools. The approved tool may contain technical capabilities beyond those tasks for which the tool was approved; as such the IA personnel must ensure that approved tools are used only for their intended purpose.

(3) **IA personnel will not use unapproved IA tools, use IA tools for unapproved purposes, or misuse automated IA tools**. Violations will be reported through appropriate command channels to the CIO/G–6. Exceptions to the configuration of these devices will be approved on a case-by-case basis by NETCOM/9th SC (A).

(4) In general terms, IA personnel and SAs/NAs do not engage in blanket network monitoring of internal communications. However, the Army reserves the right at any time to monitor, access, retrieve, read, or disclose internal communications when a legitimate need exists that cannot be satisfied by other means pursuant to para 4–5*t*, below.

(5) As a matter of normal auditing, SAs/NAs may review web sites logs, files downloaded, ingress and egress services and similar audited or related information exchanged over connected systems. Supervisors and managers may receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and authorized.

(6) As a matter of normal auditing, SAs/NAs may store all files and messages through routine back ups to tape, disk, or other storage media. This means that information stored or processed, even if a user has specifically deleted it, is often recoverable and may be examined at a later date by SAs/NAs and others permitted by lawful authority.

(7) SA/NAs may provide assistance to Army supervisory and management personnel, under lawful authority, to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on ISs. This information may include personal data. Such examinations are typically performed to assure compliance with internal policies; support the performance of administrative investigations; and assist in the management and security of data and ISs.

(8) When IA personnel discover information during the course of their normal activity that indicates a violation of acceptable use or a possible criminal offense, they will immediately report the finding to their Commander. The commander will immediately report known or suspected criminal activity to LE and will consult with legal counsel concerning activities that appear merely to violate acceptable use. IA personnel will retain and provide information related to the matter to LE when required.

(9) **With the exceptions of the SA/NA as identified below, Army personnel and contractors are prohibited from browsing or accessing other user's e-mail accounts.**

(10) The SA/NA may only intercept, retrieve, or otherwise recover an e-mail message and any attachments thereto, only under the following circumstances:

(a) With consent (expressed or implied) of a party to the communication involved.

(b) In response to a request for technical assistance from:

1. LE/CI personnel pursuant to a properly authorized LE/CI investigation.

2. A supervisor as part of a non-investigatory management search in accordance with paragraph 4–5*t*, below.

3. An investigating officer pursuant to a properly authorized administrative investigation (for example, a preliminary inquiry under Rule for Courts-Martial 303, an informal investigation under AR 15–6, or a preliminary inquiry under AR 380–5).

4. Information systems security monitoring personnel pursuant to properly authorized IS security monitoring activities.

5. Inspector General personnel pursuant to an authorized inspection, investigation, or inquiry.

(11) The SA/NA may remove any e–mail, file, or attachment that is interfering with the operation of an IS without consent of the originator or recipient. The SA/NA will notify the originator and recipient of such actions.

(12) The SA/NA is not authorized to use techniques or software to penetrate or bypass user's information protections (for example, content restrictions or read-only protections used to maintain or enforce document integrity, version control, or need-to-know enforcement).

t. Management search. In the absence of the user (for example, TDY, extended hospital stay, incapacitation, emergency operational requirement), only the SA/NA is authorized limited access to the user's files to support administrative management searches to provide the requested information as required for official purposes. When such access is requested, the SA will—

(1) Brief the supervisor as to the limits of accessing the user's data files.

(2) Limit the scope of the authorized search to those files reasonably related to the objective of the search (that is, e-mail access would not be reasonable when searching for a word document file).

(3) Limit the search to the time necessary to locate the required data in the most relevant file location.

(4) Inform the individual of requested file access as soon as possible after such requests, and document this access in a memorandum.

(5) SAs/NAs will not grant unrestricted supervisory access to individual information, data files, or accounts.

(6) SA/NAs will not access individual information or data files unless conducting a management search, an authorized administrative search, or supporting a LE/CI authorized investigation.

(7) SA/NAs may conduct an authorized investigative or management search of assigned IS upon an individuals' termination of employment, death, or other permanent departure from the organization to retrieve data and files associated with the organizational mission.

Section II
Software Security

4–6. Controls

a. IA personnel will implement controls to protect system software from compromise, unauthorized use, or manipulation.

b. The DAA, materiel developer, CIO, or IAM will document all software used for control purposes in the C&A package as a minimum.

c. PEOs, PMs, and functional proponents will require vendors seeking to support the AEI to submit SF 328 (Certificate Pertaining to Foreign Interests).

d. All COTS software used on ISs will be fully licensed (under U.S. Copyright Law).

e. Incorporate IAVM compliance, patch management, IA, and AV software into contracts with software developers regardless of the software's purpose (for example, medical devices).

f. Program managers and DAA will restrict systems used or designated as "test platforms" from connecting to operational network. PM and DAAs can authorize temporary connections to conduct upgrades, download patches, or perform vulnerability scans when off-line support capabilities are insufficient and protections have been validated. Remove the "test platform" IS immediately upon completion of the action until it has been operationally accredited and is fully compliant.

g. Use of "shareware" or "freeware" is prohibited unless specifically approved through IA personnel and by the DAA for a specific operational mission requirement and length of time when no approved product exists. Notify RCIOs and the supporting RCERT/TNOSC of local software use approval.

h. Use of "open source" software (for example, Red Hat Linux) is permitted when the source code is available for examination of malicious content, applicable configuration implementation guidance is available and implemented, a protection profile is in existence, or a risk and vulnerability assessment has been conducted with mitigation strategies implemented with DAA and CCB approval and documentation in the C&A package. Notify RCIOs and the supporting RCERT/TNOSC of local software use approval.

i. Use of data assurance and operating systems integrity products (for example, public key infrastructure (PKI), Tripwire, Internet protocol security (IPSec), transmission control protocol/Internet protocol (TCP/IP) wrappers) will be included in product development and integrated into end-state production systems.

j. IAMs and developers will transition high-risk services such as, but not limited to, ftp or telnet to secure technologies and services such as secure ftp (sftp) and secure shell (ssh).

k. **Army personnel, including contractors, will not introduce classified or sensitive information into an IS until the data confidentiality level and protection level of the IS has been certified, the appropriate IS protection mechanisms are operational, and the DAA approval or waiver has been obtained.** The data owner will approve entering the data, where applicable. Data will not exceed the security classification level for which the IS has been approved.

4–7. Database management

a. Databases store information and will be managed to ensure that the data is accurate, protected, accessible, and verifiable so that commanders at all levels can rely on trusted information in the decision making process. Commanders will appoint a database administrator (DBA) for each operational database.

b. The DBA will be certified through either training or experience in the database being managed.

c. The DBA will develop and implement controls to protect database management systems from unauthorized schema modifications.

d. The DBA will develop and implement access and auditing controls to protect database management systems from unauthorized accesses, queries, input or activity.

e. The DBA will conduct weekly backups of the database and schema, as a minimum, or more often as directed by the IAPM or IAM.

f. The SO will protect databases from direct Internet access using filtering and access control devices (for example, firewalls, routers, access control lists (ACLs)).

g. Data owners will identify the classification or confidentiality level of data residing in the database and special controls, access requirements, or restrictions required to be implemented by the DBA.

h. The SO will place databases on isolated and dedicated servers with restricted access controls. DBAs will not install other vulnerable servers or services (for example, web servers, ftp servers) that may compromise or permit unauthorized access of the database through another critical vulnerability identified in the additional servers or services.

i. Databases should be hosted on trusted military IS or networks. As part of the C&A process, the CA and DAA will review and approve a detailed risk management process as documented in the C&A package before operational implementation of databases located in contractor owned, operated, or managed networks.

j. Before the DAA grants an approval to operate (ATO), the following minimum requirements will be addressed in a security compliance plan:

(1) DBA certifications and experience in the proffered system(s) and application(s).

(2) Security background investigation(s) of the administrator(s) and verification procedures equivalent to the IT position held by the DBA and the classification of the system.

(3) Control measures for encrypted privileged-level, root, administrator, and user accesses in accordance with Army access standards.

(4) Control measures to protect database(s) and management systems from unauthorized queries, input, or activity for example; data input validation and exception routines.

(5) Control measures for database(s) and server update, management, backup, and recovery procedures.

(6) Control measures and procedures for audits, analysis, incident and intrusion response.

(7) Control measures to protect database(s) servers and interfaces from direct, unauthorized, or un-authenticated Internet access using filtering and access control devices or capabilities (for example, firewalls, routers, ACLs).

(8) Control measures to protect database(s) servers and interfaces from physical access threats.

(9) Control measures to protect database(s) servers and interfaces from logical threats.

(10) For contractor owned, operated, or managed databases, the contractor will conduct an initial comprehensive vulnerability assessment of the configuration, security, and network upon which the servers reside, and provide the complete results to authorized Army representatives.

(11) For contractor owned, operated, or managed databases, the contractor will conduct quarterly comprehensive vulnerability assessments and evaluations and furnish the results to authorized Army representatives.

k. Data owners and DBAs will implement and support DOD data/meta-data tagging requirements as initiatives, software, procedures, and methodologies are developed and implemented.

4–8. Design and test

a. All information systems will be designed to meet the IA controls as identified in DODI 8500.2 and be configured in compliance with the applicable DISA STIG or baselined system with identified changes documented as part of the accreditation process.

b. All information and information-based systems will incorporate embedded software security solutions throughout the system life cycle.

c. System developers will contact CSLA during initial design to determine COMSEC device requirements (if required) in system design.

d. Before fielding, all information and information-based systems will be tested per an approved Test and Evaluation Master Plan (TEMP) that contains current, validated threats to each IS. The systems will demonstrate successful completion of all required test and evaluation events at each acquisition decision milestone.

e. Conduct vulnerability assessments on all systems before fielding or installing systems to identify residual vulnerabilities and provide risk mitigation strategies for those vulnerabilities that are operationally required.

Section III
Hardware, Firmware, and Physical Security

4–9. Hardware–based security controls

Consider hardware security, COMSEC, and IA requirements in the concept, design, development, acquisition, fielding, and support of ISs.

a. System developers will incorporate controls to protect hardware and firmware from compromise and unauthorized use, removal, access, or manipulation.

b. After initial fielding and installation of hardware or firmware, proposed additions must go through an Installation configuration management board for approval before installation and operation. The CCB Chair or responsible Information Management (IM) official will notify the DAA, Army CA, materiel developer, CIO, IAM, RCIO, DOIM, or authorized IM officer before installation and operation, as applicable. Proposed additions may require revalidation or re-accreditation of the system's security posture and accreditation approval.

c. The C&A will include an inventory of all identifiable hardware, firmware, and software that are parts of the system.

d. Maintain CM controls for all hardware and firmware test and evaluation, follow-on test and evaluation, and other related activities by the materiel developer.

e. IAPMs, IAMs, or system developers will contact CSLA to review applicable IA BPAs (both from DOD and the Army) before initiating requisition actions.

4–10. Maintenance personnel

The Commander will verify or validate the following:

a. Clearances. Maintenance personnel will be cleared to the highest level of data handled by the IS. Clearance requirements will be included in maintenance contracts, statements of work, and specified on the DD Form 254 (Department of Defense (DOD) Contract Security Classification Specification), in accordance with AR 380–49, where applicable.

b. Restrictions. Escort and observe uncleared maintenance personnel at all times by a cleared and technically qualified individual. Non-U.S. citizens will not perform maintenance on ISs that process TOP SECRET (TS), Sensitive Compartmented Information (SCI), Special Intelligence (SI), Single Integrated Operational Plan-Extremely Sensitive Information (SIOP–ESI), or SAP information.

c. Use of non-U.S. citizens. When non-U.S. citizens are employed to maintain ISs, address such use as a vulnerability in the risk assessment and identify and employ appropriate countermeasures.

d. Maintenance by cleared personnel. Personnel who perform maintenance on classified systems will be cleared and indoctrinated to the highest classification level of information processed on the system. Appropriately cleared maintenance personnel do not require an escort. Need-to-know requirements may be inherent to adequately perform maintenance or take corrective actions. An appropriately cleared and technically knowledgeable employee will be present or review the system during maintenance to assure adherence to security procedures.

e. Maintenance by uncleared (or lower-cleared) personnel. If cleared maintenance personnel are unavailable, individuals with the technical expertise to detect unauthorized modifications will monitor all uncleared maintenance personnel.

(1) Uncleared maintenance personnel will be U.S. citizens. Outside the U.S., where U.S. citizens are not available to perform maintenance, use FNs as an exception, with DAA approval and documentation in the C&A package.

(2) Before maintenance by uncleared personnel, the IS will—

(a) Be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured.

(b) When a system cannot be cleared, IAM-approved procedures will be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive information that is contained on the system.

(3) A separate, unclassified copy of the operating system (for example, a specific copy other than the copies used in processing information), including any floppy disks or cassettes that are integral to the operating system, will be used for all maintenance operations performed by uncleared personnel. The copy will be labeled "UNCLASSIFIED–FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSAA/System Security Policy (SSP). Ensure that the media is write-protected before use in classified systems.

(4) Maintenance procedures for an IS using a non-removable storage device on which the operating system resides will be considered and approved by the IAM on a case-by-base basis.

(5) The use of commercial data recovery services will be documented in the C&A package and approved by the DAA with approval from the data owner and notification to the CIO/G–6 CISO.

4–11. Security objectives and safeguards

The Commander will verify or validate the following:

a. Secure removable media that process and store classified information in an area or a container approved for safeguarding classified media per AR 380–5.

b. Establish checks and balances to reduce the risk of one individual adversely affecting system or network operations.

c. Implement physical security requirements for ISs to prevent loss, damage, or unauthorized access.

d. Prohibited storage of portable ISs or personal electronic devices (PEDs) that contain classified information in personal residences. Exceptions will follow the guidance as prescribed in AR 380–5, paragraph 7–6, and authorized as an exception only when an operational requirement exists.

e. Include facilities or spaces housing critical systems (for example, e-mail servers, web servers) as part of the physical security program and restrict access.

Section IV
Procedural Security

4–12. Password control

a. Implement two-factor authentication techniques as the access control mechanism in lieu of passwords. Use CAC as the primary access credential, or biometric or single-sign on access control devices when the IS does not support CAC.

b. The IAM or designee will manage the password generation, issuance, and control process. If used, generate passwords in accordance with the BBP for Army Password Standards.

c. The holder of a password is the only authorized user of that password.

d. The use of one-time passwords is acceptable, but organizations must transition to secure access capabilities such as SSH or secure sockets layer (SSL). See remote access requirements in para 4–5*d*.

e. SAs will configure ISs to prevent displaying passwords in the clear unless tactical operations (for example, heads-up displays while an aircraft is in flight) pose risks to life or limb.

f. IAMs will approve and manage procedures to audit password files and user accounts for weak passwords, inactivity, and change history. IAMs will conduct quarterly auditing of password files on a stand-alone or secured system with limited access.

g. Deployed and tactical systems with limited data input capabilities will incorporate password control measures to the extent possible.

h. **IAMs and SAs will remove or change default, system, factory installed, function-key embedded, or maintenance passwords.**

i. IAMs and SAs will prohibit automated scripts or linkage capabilities, including, but not limited to, Web site links that embed both account and authentication within the unencrypted link.

j. SAs/NAs, with DAA approval, will implement procedures for user authentication or verification before resetting passwords or unlocking accounts in accordance with the C&A package.

k. SAs/NAs will conduct weekly auditing of service accounts for indications of misuse.

l. The use of password generating software or devices is authorized as a memory aid when it randomly generates and enforces password length, configuration, and expiration requirements; protects from unauthorized disclosure through authentication or access controls; and presents a minimal or acceptable risk level in its use.

4–13. Release of information regarding information system infrastructure architecture

a. **All Army personnel and contractors will protect and restrict access to all documentation (for example, maps, test and evaluation results, vulnerability assessments, audits, results, or findings) describing operational IS architectures, designs, configurations, vulnerabilities, address listings, or user information**. This information is a minimum of FOUO and will not be made publicly accessible. Evaluate Freedom of Information Act (FOIA) requests for such documents in these categories on a case-by-case basis.

b. All information or IS responses that document or display specific vulnerabilities of a system or network that would aid attempts by an adversary to compromise those critical systems or networks are OPSEC sensitive and will be protected, controlled, marked, or stored at the appropriate classification level for the system concerned. This information will not be made publicly available.

c. Protect and restrict access to information that is a collection of interrelated processes, systems, and networks that provides information on IA services throughout the Army; the KMI; or the incident detection and response infrastructure, capabilities, or configuration. This information should be marked FOUO and may be exempt from mandatory release pursuant to the FOIA. Coordinate with your servicing FOIA or Privacy Act office and servicing judge advocate or legal advisor before releasing or deciding to withhold such information.

Section V
Personnel Security

4–14. Personnel security standards

The following standards designate positions requiring access to IT and for processing information within IT systems. These security designations are required to distinguish potential adverse effects on Army functions and operations and, therefore, the relative sensitivity of functions performed by individuals having certain privileges. These positions are referred to as IT and IT-related positions. The requirements of this section will be applied to all IT and IT-related positions, whether occupied by DA civilian employees, military personnel, consultants, contractor personnel, or others affiliated with the DOD (for example, volunteers). Additional guidance is available in DOD 5200.2–R.

a. Basic requirements.

(1) Personnel requiring access to ISs to fulfill their duties must possess the required favorable security investigation, security clearance, or formal access approvals, and fulfill any need-to-know requirements.

(2) IT–I is—

(a) Defined as personnel in IA positions (for example, SAs/NAs for infrastructure devices, IDSs, VPNs, routers; SAs/NAs for classified systems and devices) with privileged-level access to control, manage, or configure IA tools or devices, individual and networked IS and devices, and enclaves.

(b) Favorable completion of a National Agency Check (NAC) (current within 180 days).

(c) Initiation of a Single Scope Background Investigation (SSBI) and favorable review of SF 85P (Questionaire For Public Trust Positions), SF 86 (Questionaire For National Security Positions), and Supplemental Questionnaire.

(3) IT–II is—

(a) Defined as personnel in IA positions (for example, operating system administration of common network applications or enclaves, back-up operators) with limited privileged-level access to control, manage, or configure ISs and devices, with very limited (single device) or no IA device access or management.

(b) A favorable review of local personnel, base/military, medical, and other security records as appropriate.

(c) Initiation of a National Agency Check with Credit Check and Written Inquiries (NACIC) (for civilians) or a

National Agency Check with Local Agency and Credit Checks (NACLC) (for military and contractors), as appropriate or favorable review of SF 85P and Supplemental Questionnaire.

(4) IT–III is—

(a) Defined as—

1. Personnel in IA positions, for example, power users or a SA on individual systems for configuration or management with limited privileged-level access to that IS(s) or device(s). This is a position of higher trust.

2. Personnel with roles, responsibilities, and access authorization of normal users with non-privileged level access to the IS or device.

3. Personnel with non-privileged level access authorization in the role of official or statutory volunteers. The provisions for statutory volunteers are covered in AR 608–1.

(b) A favorable review of local personnel, base and military, medical, and other security records, as appropriate.

(c) Initiation of a NACIC (for civilians) or national agency check (NAC) (for military and contractors), as appropriate and favorable review of SF 85P and Supplemental Questionnaire.

(5) IT–IV is—

(a) Defined as personnel in non-IT positions that are temporary, intermittent, or seasonal, for example, unofficial volunteers or summer hire positions, requiring restricted user-level access to unclassified, non-sensitive ISs only.

(b) Individual completes SF 85P and supplemental questionnaire.

(c) A favorable review of local personnel, base/military, medical, and other security records as appropriate. This investigation does not require submission to OPM.

(d) A favorable recommendation by the organization security manager, DAA, Commander, and installation commander, with notification to the RCIO/FCIO.

b. Personnel security controls.

(1) Personnel security controls, both technical and non-technical (for example, separation of duties, least privilege access, identification and authentication (I&A), digital signatures, and audits), will be incorporated into the IS and IS procedures, as appropriate.

(2) Individuals assigned to IT–I, IT–II, or IT–III positions who lose their clearance, or have access to classified systems suspended pending the results of an investigation, will be barred access to the ISs until favorable adjudication of that investigation. Waivers for continued access to unclassified systems will be justified in a written request, with the Commander's concurrence, to the DAA for approval. Access will be granted only upon DAA authorization. This request and approval will become part of the C&A package. Users designated in IT–I positions will be removed from these positions and this denial of access is non-waiverable.

(3) Waivers processed for IT–II and IT–III personnel only are valid for a period not to exceed 6 months. If a second waiver extension is required, one may be granted as long as a new request for waiver is submitted to the DAA and approved by the first general officer, or equivalent in position or civilian grade, in the Chain of Command.

(4) While the Commander and DAA have the discretion to process the waiver for IT–II and IT–III, it is important that this discretion is not without limits. The Commander and DAA are advised to proceed carefully and deliberately in making a determination on whether the individual constitutes a security risk. The IT–II/IT–III roles must be highly supervised. Any access to protective devices (for example, firewalls, VPNs, intrusion detection systems (IDSs), IPSs, and so on) will be prohibited until favorable adjudication.

(5) The servicing legal office should be consulted for advice concerning personnel, security, contract and labor relations issues that may impact the final determination. Recheck local records to identify any issues that may be a deciding factor in the waiver process.

(6) New, credible derogatory information revokes any standing waiver and results in immediate denial of access to IT systems (exceptions are for military only based on immediate supervision of the individual while on the IS).

(7) Contractor, FN or temporary individuals assigned to any IT positions who have their unclassified system or network accesses revoked or suspended for derogatory reasons, will be barred access to the ISs until favorable adjudication of that investigation. The organization's IASO/IANO/IAM (as appropriate) will identify any other official systems/networks for which that individual has an account (for example, AKO) and have it temporarily disabled or suspended.

(8) The required investigation levels for an IT–I position are outlined below in table 4–2.

Table 4–2
Investigative levels for users with privileged access (IT–I) to ISs

Privileged access—IT–I[1]					
User roles	**Foreign national**	**U.S. civilian**	**U.S. military**	**U.S. contractor**	**Conditions or examples**
DAA or IAPM	Not allowed	SSBI	SSBI	Not allowed	None
IANM	Not allowed	SSBI	SSBI	Conditional SSBI	With CIO/G–6 written approval, contractors may continue as IA personnel until replaced
IAM	Not allowed	SSBI	SSBI	Conditional SSBI	Contractor may not fill MSC, installation, or post IAM position
IASO/IANO	Not allowed	SSBI	SSBI	Conditional SSBI	Contractor may not fill MSC, installation, or post IASO/IANO position (if created)
Monitoring or testing	Not allowed	SSBI	SSBI	SSBI	None
SA/NA or Administrator (with IA privileged access) or maintenance of IA devices	Conditionally allowed—SSBI (equivalent) [2]	SSBI	SSBI	SSBI	Examples: administration of IA devices (for example, boundary devices, IDSs, routers, and switches)

Notes:
[1] Investigative levels are defined in DOD 5200.2–R. The term "Foreign National" (FN) refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.
[2] FN—under the immediate supervision of a U.S. citizen with written approval of CIO/G–6.

(9) The required investigation levels for an IT–II position are outlined below in table 4–3.

Table 4–3
Investigative levels for users with limited privileged access (IT–II) to ISs

Limited privileged access—IT–II[1]					
User roles	**FN (see note 2)**	**U.S. civilian**	**U.S. military**	**U.S. contractor**	**Conditions or examples**
IAM/IANM	Not allowed	NACI	NACLC	NACLC	None
IANO/IASO	Conditionally allowed—NACLC equivalent	NACI	NACLC	NACLC	FN—with DAA written approval, and documentation in the C&A package, direct or indirect hires may continue as IA personnel until they are replaced, provided they serve under the immediate supervision of a U.S. citizen IAM and have no supervisory duties
Supervisor of IT I or IT II positions	Not allowed	NACI	NACLC	NACLC	None
Administrator (with no IA privileged access) or maintenance of IA-enabled products	Conditionally allowed—NACLC equivalent[2]	NACI	NACLC	NACLC	Examples: IS administration, OS administration, end-user administration, and administration of common applications (for example, e-mail, word processing)

Notes:
[1] Investigative levels are defined in DOD 5200.2–R. FN refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.
[2] FN—under the immediate supervisor of a U.S. citizen.

c. Access by non-U.S. citizens.

(1) Minimize employment of non-U.S. citizens in IT positions. However, compelling reasons may exist to grant access to DOD IT resources in those circumstances in which a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DOD requirement and for which a suitable U.S. citizen is not available. Written compelling-reason justification, documentation in the C&A package, and DAA approval are required.

(2) Access to sensitive information by a non-U.S. citizen who is not a DOD employee will only be permitted in accordance with applicable disclosure policies (for example, National Disclosure Policy 1, DODD 5230.9, DODD 5230.25) and U.S. statutes (for example, the Arms Export Control Act, 22 USC 2551, et. seq.).

(3) If information to which the incumbent will have access is authorized for foreign disclosure, non-U.S. citizens assigned to DOD IT positions are subject to the investigative requirements outlined below.

(4) Non-U.S. citizens may hold IT positions under the conditions described in the paragraphs below and if the DAA that accredited the system and the data owners approve the assignment requirements in writing. The written approval must be on file and provided as an artifact to the C&A package, before requesting the required investigation. The required investigation must be completed and favorably adjudicated before authorizing access to DOD systems or networks. Interim access is prohibited.

(5) Assignment (including assignments due to accretion of duties) of current DOD employees, military personnel, consultants, and contractors to positions with different responsibilities or changed access privileges requires verification of the appropriate investigative basis and authority for holding a position of that level of sensitivity.

d. Interim assignments.

(1) Individuals including temporary, intermittent, or seasonal personnel—may be assigned to unclassified IT II and IT–III positions on an interim basis before a favorable completion of the required personnel security investigation only after the conditions specified have been met.

(a) Individual completes SF 85P and supplemental questionnaire.

(b) A favorable recommendation by the organization security manager, Commander or Director, DAA, and Installation Commander, with RCIO/FCIO notification.

(c) Initiation of security investigation has been submitted or is pending adjudication.

(d) Interim access is not authorized for non-U.S. citizens.

(2) The security manager at the requesting activity will make interim assignment approvals for civilian and military personnel.

(3) The Government sponsor's security manager or official will make the approval for volunteer access.

(4) The interim assignment of contractor personnel fulfilling IT positions will be restricted and implemented only upon documentation in the C&A package and acceptance of the DAA and the Contracting Officer evaluations on a case-by-case basis.

e. Adjudication.

(1) The provisions of this section apply only to contractor personnel. (Civilian employees, military personnel, consultants, volunteers, and seasonal, part-time, and intermittent employees will be favorably adjudicated by the appropriate DOD central adjudication facility.)

(2) OPM will adjudicate investigations for a trustworthiness determination using the national adjudicative guidelines for access to classified information. If the adjudication is favorable, OPM will issue a letter of trustworthiness to the requesting activity.

(3) If a favorable trustworthiness is indeterminate, OPM will forward the case to the Defense Office of Hearings and Appeals (DOHA) in Columbus, OH, for further processing under DODD 5220.6. A final unfavorable decision precludes assignment to an IT–I, II, or III position.

(4) Enter all OPM IT trustworthiness determinations of DOD contractor personnel into the OPM Security/Suitability Investigative Index (SII).

f. Reinvestigation. Individuals occupying an IT position will be subject to a periodic reinvestigation according to existing contract, labor relations, or personnel security policy.

4–15. Foreign access to information systems

a. To ensure standardized and appropriate access to the Unclassified but Sensitive Internet Protocol Routing Network (NIPRNET) by foreign officials, IA personnel will meet the requirements delineated below. Provide each authorized foreign official a .mil address on the unclassified network required for executing his or her foreign official duties as outlined in his or her respective certification. For each authorized foreign official, the local area network administrator will place a caveat or marker on the user account and all outgoing e-mails from that person identifying them as a foreign official from a specific country. In doing so, the local area network administrator will spell out the words "Foreign Official" and the country name of the foreign official and will not use an acronym for that country. In addition, the local area administrator will indicate the type of foreign official access that is granted. The required tags for each of the five categories of foreign officials would thus read as shown below (replace each hypothetical country name with the appropriate one).

(1) Foreign liaison officer (FLO): "Last Name, First Name Middle Initial-Foreign National-Germany-FLO." (Note: Local area network administrators will designate FLOs representing the United Kingdom, Canada, or Australia as STANREPs rather than as FLOs.)

(2) Cooperative Program personnel (CPP): "Last Name, First Name Middle Initial-Foreign National-Turkey-CPP".

(3) Engineer and Scientist Exchange Program (ESEP): "Last Name, First Name Middle Initial-Foreign National-Israel-ESEP".

(4) Standardization representative (STANREP): "Last Name, First Name Middle Initial-Foreign National-United Kingdom-STANREP".

(5) Military Personnel Exchange Program (MPEP): "Last Name, First Name Middle Initial-Foreign National-Italy-MPEP".

b. Limit access to foreign officials, exchange personnel, or representatives to computers that incorporate Army-mandated access and auditing controls. Approval to access the NIPRNET does not equate to authority to exchange data or access systems located on that network. The appropriate system DAA will approve access to foreign officials on an as needed basis and updating the documentation in the C&A package. Similarly, the designated release or disclosure authority will grant access to the information on ISs to foreign officials on an as-needed basis.

c. E-mail signature blocks will be automatically generated for all foreign personnel, and include the foreign individual's nationality and position.

d. If the organization where a foreign official is certified determines there is a need for the foreign official to have access to the NIPRNET beyond e-mail access (for example, an AKO account), submit an exception to policy through the DAA to the RCIO IAPM, to be forwarded to the CIO/G6. The approval will become part of the C&A package for the IS. This includes individuals granted access prior to the publication of this regulation. Commands will immediately evaluate each case and forward their exception recommendation. The exception will be reviewed by the appropriate HQDA Program Manager and the NETCOM/9th SC (A) OIA&C prior to disposition. The exception must include the following information——

(1) Request from the Commander that states the need to know, tied to the foreign official's certification and Delegation of Disclosure Authority Letter (DDL).

(2) Statements from the installation and command's IAM stating proper security procedures are in place. The DCS, G–2, Foreign Disclosure and Security Directorate will also review the exception before final disposition.

e. Official access to information residing on an IS or network will be limited to that controlled but unclassified information required to fulfill the terms of the contract or agreement provided minimum security requirements of this section are met.

f. Disclosure of classified military information to foreign governments and international organizations is limited and will be in accordance with AR 380–10, DODD 5230.11, and CJCSI 5221.01B.

g. International Military Students (IMS) who have been vetted and approved for U.S. Army training and Professional Military Education (PME) attending resident training or enrolled in the Army Distance Education Program (DEP) at U.S. Army and Army-managed schools/training activities will agree to comply with all U.S. MILDEP requirements. They are required to sign an AUP user agreement. There is no requirement for background investigations as described since in-country U.S. officials perform a security screening of each student before selection approval. To prevent inadvertent disclosure of information, international military students will be identified as students in their email address, display name and automated signature block (for example, john.i.smith.uk.stu@xxx.army.mil).

h. NIPRNET access policy and procedures for FNs in non-official positions as identified above, are as follows:

(1) Components or organizations will maintain records on access including the following information—

(a) Specific mission requirements for foreign access or connection.

(b) Justification for each individual FN.

(c) Confirmation that the minimum-security requirements of this section are enacted, including the user agreement discussed below.

(2) Before authorizing FN access to a specific IS on the NIPRNET or the Secret Internet Protocol Routing Network (SIPRNET), Army components will—

(a) Ensure the information is properly processed for disclosure.

(b) Ensure DAAs and data owners concur with the access.

(c) Ensure the C&A documentation for the system is updated to reflect FN access.

(d) Ensure security measures employed adhere to this policy.

(e) Validate the identity of each FN authorized access to ISs to ensure accountability of all actions taken by the foreign user.

(f) Ensure the FN follows appropriate security policies and procedures and that the IASO possesses the authority to enforce these policies and procedures. Before accessing any system, an FN will sign an AUP agreement that includes—

1. Acknowledgment of appropriate information security policies, procedures, and responsibilities.

2. The consequences of not adhering to security procedures and responsibilities.

3. Identification requirements when dealing with others through oral, written, and electronic communications, such as e-mail.

4. Department of the Army employees or contractors who are FNs and are direct or indirect hires, currently appointed in IA positions, may continue in these positions provided they satisfy the provisions of paragraph 4–14, DODD 8500.1, DODI 8500.2, and DOD 5200.2–R; are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA and captured in the C&A package.

5. FNs assigned into IT positions will be subject to the same (or equivalent) vetting as U.S. citizens.

6. FNs may hold or be authorized access to IT–II and IT–III positions provided the required background investigation has been completed or favorably adjudicated.

7. Additionally, an FN may be assigned to an IT–I position only after the DAA who owns the system and the data owner who owns the information sign a waiver and the assignment has been approved by the CIO/G–6. The approvals will become part of the C&A package. Sign and place the waiver in the individual's security file before requesting the required background investigation. The required background investigation must be completed and favorably adjudicated before authorizing IT–I access to DA systems/networks.

8. Do not assign FNs to IT–I, IT–II, or IT–III positions on an interim basis before a favorable adjudication of the required personnel security investigation.

i. Generally, an FN or official representative is not authorized access to the U.S. controlled SIPRNET terminal workspace. If an authorized foreign official or national working at a U.S. Army site has a requirement for accessing the SIPRNET, the commander will submit an exception to policy through the DAA to the RCIO IAPM, to be forwarded to the HQDA CIO/G–6, and reviewed by the DCS, G–2 Foreign Disclosure Directorate prior to disposition. CIO/G–6 will coordinate the request with the Army staff and forward to DISA. These requests will be staffed with the presumption of denial. Apply the procedures of this section after DISA's approval and any additional guidance provided by DISA on the connection process for FNs. E-mail signature blocks will be automatically generated for all FNs, and include the foreign individual's nationality and position. The approvals will become part of the C&A package.

Section VI
Information Systems Media

4–16. Protection requirements

a. All IS equipment and facilities used for processing, handling, and storing classified data will be operated and secured where applicable per the DCID 6/3, AR 380–5, this regulation, or Joint DODIIS Cryptologic SCI Information Systems Security Standards (JDCSISSS).

b. All Army personnel and contractors will mark, ship, store, process, and transmit classified or sensitive information in accordance with AR 380–5.

c. Control ISs containing non-removable, non-volatile media used for processing classified information.

d. Commanders, Directors, and IA personnel will verify procedures and train users, administrators and security personnel in processes for spillage incidents of higher-level or classified information to a lower-level IS.

e. SAs will configure ISs to apply security or handling markings automatically when possible or available.

f. **SAs will configure ISs to display the classification level on the desktop or login screen (for example, wallpaper, splash screen) when the device is locked, the user is logged off, or the IS is used in spanning multi-classification networks through the use of a KVM device.**

g. All Army personnel and contractors will not transmit classified information over any communication system unless using approved security procedures and practices including, encryption, secure networks, secure workstations, and ISs accredited at the appropriate classification level.

4–17. Labeling, marking, and controlling media

a. Unless write-protected or read-only, all personnel will protect and classify media inserted into a system at the highest level the system is accredited to process until the data or media is reviewed and downgraded by the IASO.

b. All personnel will clear removable media before reusing in ISs operating at the same or higher protection level.

c. All personnel will mark and control all media devices, peripherals, and ISs as follows:

(1) TS or SCI or intelligence data per DCID 6/3, DCID 1/7 and JDCSISSS as applicable.

(2) Classified media per AR 380–5 requirements.

(3) FOUO media per AR 25–55 requirements.

(4) Privacy Act media per AR 340–21 requirements.

(5) NATO information per AR 380–5 requirements.

d. All personnel will mark and control the media or IS after determination of the classification level of the data placed on the media. Implement media accountability procedures based on the type of media and the classification of the data as required above.

4–18. Clearing, purging (sanitizing), destroying, or disposing of media

a. Procedures for disposition of unclassified hard-drive media outside DOD custody will follow current guidelines addressed in the published BBP.

b. All personnel will purge media before reuse in a different environment than the one in which they were previously used (new users without a need-to-know for the original data) or with data at a different classification or sensitivity level or when the drives have met the end of their life cycle. Ensure custodial equipment transfer requirements are accomplished. IA personnel will verify that personnel are trained on local procedures. Purging electronic media does not declassify the media, as declassification is an administrative process.

c. IA personnel will conduct random security inspections for violations of removable media physical security measures quarterly.

d. IA personnel will purge unclassified media before consideration for release outside DOD control.

e. IA personnel will destroy media that has ever contained NSA Type 1 cryptographic or COMSEC materiel at end of life cycle in accordance with approved destruction processes.

f. IA personnel will destroy SCI media at end of life cycle in accordance with DCID 6/3 for DODIIS systems and NSA 130–1 and 130–2 for NSA Cryptologic systems in accordance with approved destruction processes.

g. IA personnel will destroy media that contained classified material or was involved in a classified spillage incident at end of life cycle in accordance with approved destruction processes.

h. When it is more cost effective, or to ensure absolute security, destroy media instead of purging or declassifying in accordance with approved destruction processes.

i. The IAM will establish procedures to periodically verify the results of any purging and IS release processes.

j. Spillage recovery procedures for data from higher-classified information to lower-classified systems are addressed in a separately published BBP.

Section VII
Network Security

4–19. Cross-domain security interoperability

The DOD Global Information Grid, Inter-connection Approval Process (GIAP) was created out of the need to provide a consistent way to simplify and consolidate the various connection approval processes. All DOD Services and agencies must comply with these processes when connecting networks of different classification levels. The Top Secret and Below Interoperability (TABI) and the Secret and Below Interoperability (SABI) processes provide an integrated, comprehensive, and consistent approach to addressing the shared risk associated with the connection of networks of different classification levels.

a. Organizations requiring a cross-domain solution must first complete the information on the GIAP Web site (https://giap.disa.smil.mil).

b. Organizations requiring a cross-domain solution will also contact the NETCOM/9th SC (A) Information Assurance Directorate, Cross-Domain Solutions Office to provide notification of the cross-domain process initiation.

c. The cross-domain process follows the DIACAP and requires that networks be fully certified and accredited and that all associated security devices be certified, tested, and evaluated (CT&E) in accordance with the NSA compliance standards. Approved standardized cross-domain solutions will be acquired through CSLA. Non-standard solutions will require an extensive engineering effort.

d. All Army organizations that maintain connections between networks of different classification levels must annually revalidate their connections in accordance with the SIPRNET DAA directives. Contact the SIPRNET Connection Approval Office for current guidance and requirements.

e. Manage all interconnections of DOD ISs to continuously minimize community risk by ensuring that one system is not undermined by vulnerabilities of other interconnected systems and that one system does not undermine other systems. All ISs within interconnected (or trusted networks) will meet networthiness certification.

4–20. Network security

a. Procedures. Commanders will establish procedures to manage and control access to all ISs, networks, and network equipment to ensure integrity, confidentiality, availability, non-repudiation, and authentication, regardless of classification level.

b. Requirements. Positive IA measures ensure all users satisfy the requirements specified before granting an individual access (including dial-up services and Internet access) to DOD and Army networks, systems, and stand-alone computers.

(1) *Individual.* Commanders will verify and IA personnel will deny physical and logical access to individuals who cannot meet access requirements.

(2) *Proponents.* Proponents for programs that require network services for family members, retirees, and other individuals serviced at Army installations for example, unofficial recreational activities; libraries; education centers; or Army-Air Force Exchange Service (AAFES) kiosks, should arrange for services through a commercial Internet service

provider (ISP) or other isolated connection capability. Proponents will coordinate with the installation DOIM for service and the IAM for IA requirements. These connections are unofficial communications and will be isolated either logically or physically from official DOD and Army NIPRNET networks.

(3) *MWR garrison activities.* MWR garrison activities dependent upon the Installation LAN for network connectivity in accordance with DODI 1015.10 and AR 215–1 to provide Executive Control & Essential Command Supervision (ECECS) in support of the Commanders Fiduciary responsibility, are authorized the use of NIPRNET connectivity to support Commander's MWR activities. Published BBPs describe the standards for acceptable connectivity and IA security requirements.

(4) *JIM networks.* JIM networks that have NETCOM/9th SC (A) provided connectivity will implement the most restrictive and isolating configuration and implementation management principles (inclusive of, but not limited to, separate enclaves and identifications, and tunneled or dedicated connectivity) to those that are absolutely required for military or support operations as necessary and in compliance with IA requirements in this and other applicable regulations. In order to be entirely separate, JIM networks must not—

(a) Utilize Army IP numbering for their end users, servers or network devices.

(b) Utilize army.mil as their logical extension.

(c) Connect to any local Army network on Army installations.

(d) Require Army network and systems management, systems administration, or maintenance and repair support as a standard level of service.

(e) Require Army to provide security oversight, management, or services from the Army as a standard level of service.

(f) Report IAVM compliance through Army channels.

(g) Receive Army funding for implementation at the location.

c. Restrictions. Supervisors and managers will—

(1) Ensure transmission of classified or sensitive information via applicable secure means.

(2) Authorize commercial ISP accounts per chapter 6, AR 25–1.

(3) Ensure there are no cross-connections directly between the Internet and NIPRNET of ISs. For example do not permit a modem connection (for example, multi-functional devices such as copier/fax/printer combinations) to a commercial ISP or service while the IS is also connected to the NIPRNET. NIPRNET connected systems will have this function disabled.

(4) Permit direct connections to the Internet to support electronic commerce when those systems will not connect to the NIPRNET or the SIPRNET.

d. Security protection between enclaves. (that portion of the network outside the installation's or activity's controls). Commanders and IA Personnel will utilize the following processes on routers, switches, firewalls, and other networking devices to provide protection from external networks.

(1) Firewalls. Configure firewalls with least-privilege access controls. Layer firewalls at the boundaries between border and external networks and as needed throughout the architecture to improve the level of assurance. NETCOM/9th SC (A) will approve firewall implementation guidance for use within the Army. Every information system should be protected by either an approved host-based or network-based (enclave) firewall.

(2) Access control lists. Update and manage access control lists (ACLs) through secure mechanisms and incorporate a "deny all, permit by exception" (DAPE) policy enforcement.

(3) Network configurations. IA personnel will implement network configurations to remove or block any unnecessary or unauthorized services, software, protocols, and applications such as: LanMan, gaming software, Gnutella, IRC, ICQ, Instant Messaging, peer-to-peer.

(4) Ports, Protocols, and Services Management (PPSM). Permit only ports, protocols, and services (PPS) as authorized. The Commander and network management personnel will:

(a) Restrict enterprise and enclave boundary firewalls and firewall-like devices to the usage of approved PPS in accordance with the DODI 8551.1 on PPSM. DOD considers PPSs not listed on the DOD PPS TAG list as "deny by default."

(b) PPSs designated as "high-risk" are unacceptable for routine use. Prohibit high-risk PPSs unless expressly approved for a specific implementation with defined conditions and risk mitigation strategies.

(c) PPSs designated as "medium-risk" have an acceptable level of risk for routine use when used with required mitigation strategies.

(d) PPSs designated as "low-risk" are recommended as best security practices and advocated for use by Army developers in future systems and applications. Not all low-risk PPSs are acceptable under all implementations and may require approval.

(e) The goal of NETCOM/9th SC (A) is the migration systems that use high- and medium-risk PPSs to low-risk PPSs as part of its life cycle management processes through system redesign while maintaining current standards-based applications and requirements (for example, port 21 for ftp, port 80 for Web).

(f) NETCOM/9th SC (A) is responsible for PPS management and will approve and publish Armywide mitigation strategies for PPSs.

(5) Domain name service (DNS). TNOSCs will monitor DNS servers for compliance and adherence to DNS policies. Owning organizations will provide host-based intrusion detection monitoring for these servers.

(6) Virtual private networks (VPNs). Virtual private networks will require approval to connect and operate from the RCIO using NETCOM/9th SC (A) CCB-approved and published implementation processes (when implemented) after documenting a well-defined acceptable use policy, security concept of operations, an SSAA risk analysis and management plan, and Networthiness certification, before implementation.

(7) Storage area configurations. As developing technologies (for example, storage area networks, collaborative environments, data sharing technologies, web-casting, or real/near-real time distribution capabilities) are implemented, they must incorporate secure IA principles. Minimum requirements include, but are not limited to the listed below requirements. Network management personnel will—

(a) Obtain approval for C&A, CAP, and Networthiness.

(b) Use approved NETCOM/9th SC (A) configuration-management implemented processes.

(c) Secure the information at rest and in transit and ensure that the configuration does not introduce additional risks or vulnerabilities.

(d) Use secure communication and access protocols.

(e) Implement security controls and validate all user supplied input.

(f) Implement extranet connections through a multi-tiered and layered approach requiring separate and distinct servers across the environment for each tier, and minimally include—

1. User access tier, usually through a Web site that offers static pages and will be SSL enabled as a minimum.

2. Application tier, authenticates authorized users, access, and interfaces between the user and the data.

3. Protection of the database or data tier (for example, flat files, e-mail), information that is accessed by the application on behalf of the user.

(g) Incorporate firewalls, filtering, protective, and monitoring devices (for example, IPSs, IDSs) at each enclave layer.

(h) Employ encryption, single-sign-on, tokens, or DOD authorized digital certificates equivalent to the level of data accessed or available and adequately passed through the application server to access the data requested.

(i) Employ data separation and authentication "need to know" measures and requirements.

e. Protection of internal networks. (portion of the network that is directly controlled by the installation or activity). Network management personnel will:

(1) Establish trusts in accordance with the installation C&A. There will be no trusted relationships established with any other domains or networks until both are Networthiness certified and approved by the respective DAAs and documented in the C&A package.

(a) The DAAs of the participating ISs and the DAA of the overall network (if designated) will sign a Memorandum of Understanding (MOU). The MOU becomes an artifact to the C&A package.

(b) The DAA's approval will include a description of the classification and categories of information that can be sent over the respective networks.

(2) Connection between accredited ISs must be consistent with the confidentiality level and any other restrictions imposed by the accredited ISs. Unless the IS is accredited for multilevel operations and can reliably separate and label data, the IS is assumed to be transmitting the highest level of data present on the system during network connection.

(3) Employ identification, authentication, and encryption technologies when accessing network devices.

(4) Employ layered protective, filtering, and monitoring devices (for example, firewalls, IDSs) at enclave boundaries, managed access points, and key connection points.

(5) Scan all installation assets and devices, implement protective measures, and report non-compliance to RCIOs/FCIOs as required (minimum is semi-annual).

(6) Proxy all Internet accesses through centrally managed access points and isolate from other DOD or ISs by physical or technical means.

f. E-mail security. All personnel will use e-mail systems for transmission of communications equivalent to or less than the classification level of the IS.

(1) IA personnel will—

(a) Promote security awareness. Train users to scan all attachments routinely before opening or downloading any file from e-mail.

(b) Configure ISs to use encryption when available or as part of the global enterprise to secure the content of the e-mail to meet the protection requirements of the data.

(c) Implement physical security measures for any information media and servers.

(d) Install and configure antiviral and protective software on e-mail servers and client workstations.

(e) Warn users to treat unusual e-mail messages the same way they treat unsolicited or unusual parcels; with caution.

(f) Use digital signatures to authenticate a message as needed (non-repudiation).

(g) Configure ISs to prevent opening attachments or executing active code directly from mail applications.

(2) **Personnel will not share their personally assigned e–mail accounts.**

(3) Commanders and Directors may allow the limited use of organizational or group e-mail accounts where operationally warranted.

(4) E-mail passwords will differ from the network password when used, until a global PKI initiative is available.

(5) All personnel will employ Government owned or provided e-mail systems or devices for official communications. The use of commercial ISP or e-mail accounts for official purposes is prohibited.

(6) **Auto-forwarding of official mail to non-official accounts or devices is prohibited.**

(7) Permit communications to vendors or contractors for official business and implement encryption and control measures appropriate for the sensitivity of the information transmitted.

(8) IA Personnel will configure systems so that authorized users who are contractors, DOD direct or indirect hires, FNs, foreign representatives, seasonal or temporary hires, and volunteers have their respective affiliations or positions displayed as part of their official accounts and e-mail addresses.

g. Internet, Intranet, Extranet, and WWW security.

(1) AR 25–1 outlines requirements and policy on the use of Government-owned or leased computers for access to the Internet.

(2) Users are authorized to download programs, graphics, and textual information to a Government-owned IS as long as doing so does not violate Federal and state law, regulations, acceptable use, and local policies (for example, CM, IA).

(3) Government-owned or leased ISs will not use commercial ISPs (for example, CompuServe, America on Line, Prodigy) as service providers, unless a Government-acquired subscription to such services is in place and the access is for official business or meets the criteria for authorized personal use as indicated in AR 25–1, paragraph 6–1.

(4) Network management and IA personnel will implement appropriate access, filtering, and security controls (for example, firewalls, restriction by IP address).

(5) Network management and IA personnel will implement and enforce local area management access and security controls. Publicly accessible web sites will not be installed or run under a privileged-level account on any web server. Non-public web servers will be similarly configured unless operationally required to run as a privileged account, and appropriate risk mitigation procedures have been implemented.

(6) Commercial ISP services are authorized to support those organizations identified in paragraph 4–20*b*(2), above, and no cross or direct connectivity to the NIPRNET will exist or be implemented.

(7) All personnel will protect information not authorized to be released for public disclosure.

(8) Extranet and intranet servers will provide adequate encryption and user authentication.

(9) Extranet servers and access will be approved through the installation IAM, documented in the C&A package, and approved by the appropriate DAA.

(10) Network managers and IA personnel will configure all servers (including Web servers) that are connected to publicly accessible computer networks such as the Internet, or protected networks such as the SIPRNET, to employ access and security controls (for example, firewalls, routers, host-based IDSs) to ensure the integrity, confidentiality, accessibility, and availability of DOD ISs and data.

(11) Commanders and supervisors will comply with Federal, DOD, and DA Web site administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all Web sites.

(12) Network managers and IA personnel will protect publicly accessible Army Web sites by placing them behind an Army reverse Web proxy server. The reverse proxy server acts as a proxy from the intranet to the protected server, brokering service requests on behalf of the external user or server. This use of a reverse proxy server provides a layer of protection against Web page defacements by preventing direct connections to Army Web servers.

(13) Publicly accessible Web sites not protected behind a reverse Web proxy (until moved) will be on a dedicated server in a DMZ, with all unnecessary services, processes, or protocols disabled or removed. Remove all sample or tutorial applications, or portions thereof, from the operational server. Supporting RCERTs and TNOSCs will conduct periodic vulnerability assessments on all public servers and may direct blocking of the site dependent on the inherent risk of identified vulnerabilities. Commanders or assigned IAMs will correct identified deficiencies.

(14) All private (non-public) Army Web sites that restrict access with password protection or specific address filtering will implement SSL protocols utilizing a Class 3 DOD PKI certificate as a minimum. NETCOM/9th SC (A) issues and manages these certificates.

(15) Commanders will conduct annual OPSEC reviews of all organizational Web sites and include these results in their annual OPSEC reports pursuant to AR 530–1.

(16) To verify compliance with Federal, DOD, and DA Web site administration policies, procedures, and best

practices, the AWRAC will continuously review the content of publicly accessible U.S. Army Web sites to ensure compliance. (See also AR 25–1 for Web site administrative policies.) AWRAC will provide results from these assessments to commanders for corrective actions.

h. Approved keyboard, video, mouse (KVM) (keyboard, monitor, mouse (KMM)) switches. These devices are primarily introduced to achieve a reduction of hardware on the desktop and do not provide any IA features.

(1) These devices are not authorized for use for cross-domain interoperability (NIPRNET-to-SIPRNET or SIPRNET-to-NIPRNET guarding solution) network connections. See BBPs documentation on the CIO/G–6 IA Web site for approved items and implementation guidelines (https://informationassurance.us.army.mil).

(2) IA personnel will configure systems to utilize screen-saver lockout mechanisms for KVM/KMM switch environments approved by the DAA.

i. Information assurance tools. All personnel will use only IA security software listed on the IA tools list on Army systems and networks. The list of Army approved IA tools is available through the IA Web site. Requests for consideration and approval for additional security software packages to be added to the IA tools list must be submitted through NETCOM/9th SC (A) channels ATTN: NETC–EST–I, ATTN: OIA&C to CIO/G–6.

(1) Installation IAM-designated and Army-certified IA personnel may conduct tests under stringent conditions coordinated with the installation DOIM, IAM, TNOSC, and RCERT, at a minimum.

(2) RCIO IAPM approval, and advance notification of the servicing RCERT and TNOSC, is required before certified IA personnel may utilize public domain vulnerability assessment tools (for example, Nessus, Nmap, Saint, or Titan).

(3) **Organizational IA personnel are prohibited from conducting penetration testing attempts on ISs utilizing unauthorized hacker tools or techniques**. This restriction is applicable to operational networks and does not apply to those personnel or techniques used in a testing environment for C&A, vulnerability assessments of developmental systems, or used in a training environment for personnel certifications on isolated networks.

(4) Organizational IAMs can request penetration testing of their networks. Subordinate organizations may request penetration testing through their ACOM/ASCC IAM to the installation IAM.

(5) **The use of "keystroke monitoring" software of any kind is prohibited, except by LE/CI personnel acting within proper legal authority**.

j. Networking security tools. The following policies apply to networking security tools used on ISs:

(1) Establish a security and implementation policy for each protection tool before purchase and implementation.

(2) Implement security tools within the security perimeter defensive architecture with NETCOM/9th SC (A) approval.

(3) Limit login access to internetworking devices to those individuals who operate and maintain those devices.

(4) Review configuration and audit files of security internetworking tools weekly.

(5) The NETCOM/9th SC (A), in coordination with CIO/G–6 and the ACERT, operates detection and protection devices for networks connected to the NIPRNET. Although NETCOM/9th SC (A) owns, operates, and maintains the enterprise devices, this does not preclude the Command, DOIM, or activity IA personnel from managing and analyzing local networks or data. Local management of an IDS/IPS is recommended with notification to the DOIM and/or TNOSC. The notification will document the operational requirement, the intent of monitoring, and the device utilized. Staff the notification to the RCIO IAPM and submit to the supporting DOIM and RCERT/TNOSC. The requesting activity is responsible for providing the hardware and software necessary. All independent installations of IDS/IPS technologies will be configured to also support enterprise sensing and warning management activities. Coordinate the configuration and reporting requirements with the supporting RCERT/TNOSC.

k. Tactical systems.

(1) Tactical systems, including weapon system and devices integral to weapon or weapon support systems, that include features normally associated with an IS will implement the requirements of this regulation, DODI 8500.2, and Interim DIACAP.

(2) When one or more of the minimum-security requirements are impractical or adversely impose risk of safety-of-use because of the function and design of the system, the situation will be addressed in the C&A package and considered by the CA and the DAA in determining the CA recommendation and the DAA authorization decision.

(3) Mechanisms must be available to render the IS inoperable in case of imminent capture by hostile forces.

(4) Tactical networks connecting to standard tactical entry point (STEP) sites, garrison, or other fixed networks must be compliant with all security requirements (for example, configurations, approved software, C&A) before connection. They will be protected by access controls and intrusion prevention and intrusion detection systems in the same manner as garrison network defenses described earlier and will implement a DiD strategy.

Section VIII
Incident and Intrusion Reporting

4–21. Information system incident and intrusion reporting

Incidents may result from accidental or deliberate actions on the part of a user or external influence. Evidence or suspicion of an incident, intrusion, or criminal activity will be treated with care, and the IS maintained without change, pending coordination with IA, ACERT/RCERT, and LE/CI personnel. Commanders and IA personnel will enforce the policies governing unauthorized use of computer resources. All personnel will report all potential or malicious incidents. Time-sensitive actions are necessary to limit the amount of damage or access. Commanders and IA personnel will report IS incidents to external agencies to assist LE or investigative agencies, and assist in compiling supporting evidence, impact assessments, associated costs, containment viability, and eradication and reconstruction measures to effectively manage the breach and provide evidentiary material for prosecution.

a. All personnel will protect IS incident reports as a minimum FOUO or to the level for which the system is accredited.

b. IA personnel will validate IS incident reporting procedures annually for all users.

c. All personnel will report IS incidents or events including, but not limited to—

(1) Known or suspected intrusion or access by an unauthorized individual.

(2) Authorized user attempting to circumvent security procedures or elevate access privileges.

(3) Unexplained modifications of files, software, or programs.

(4) Unexplained or erratic IS system responses.

(5) Presence of suspicious files, shortcuts, or programs.

(6) Malicious logic infection (for example, virus, worm, Trojan).

(7) Receipt of suspicious e-mail attachments, files, or links.

(8) Spillage incidents or violations of published BBP procedures.

d. A serious incident report (SIR) will be generated and reported per AR 190–45 under the following conditions—

(1) The incident poses grave danger to the Army's ability to conduct established information operations.

(2) Adverse effects on the Army's image such as Web page defacements.

(3) Access or compromise of classified, sensitive, or protected information (for example, Soldier identification information (SSN), medical condition or status, doctor-patient, or attorney-client privilege).

(4) Compromise originating from a foreign source.

(5) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the USACE).

(6) Loss of any IS or media containing protected or classified information.

4–22. Reporting responsibilities

a. An individual who suspects or observes an unusual or obvious incident or occurrence will cease all activities and will notify his or her SA/NA, IASO, or IAM immediately.

b. If the SA/NA, IASO, or IAM is not available, the individual will contact his or her supporting installation IAM and theater RCERT.

c. Any SA/NA, IASO, or IAM who observes or suspects an incident or intrusion, or receives information on an incident, will logically isolate the system, prohibit any additional activities on or to the system, and immediately notify his or her supporting RCERT/TNOSC. Take no additional actions to investigate the incident until directed by the RCERT.

d. Isolation includes physical isolation (unplugging the network connection), restricting any direct physical access, and logical isolation (blocking the IP at security routers or firewalls both inbound and outbound) from the network to the system.

e. If the RCERT is not available then the SA or IASO will contact the ACERT directly. In addition, report per local supervisory reporting policies in effect.

f. Each RCERT is responsible for collecting and recording all the required information, coordinating all incident response procedures between LE/CI personnel and the organization, and conducting all intrusion containment, eradication, and verification measures.

g. The IS incident reporting format and additional reporting requirements are available on the ACERT and supporting RCERT NIPRNET/SIPRNET Web sites.

4–23. Compromised information systems guidance

a. When directed by RCERT, all ISs determined to be compromised either through unauthorized access or malicious logic will be rebuilt from original media, patched, and scanned for compliance before reintroduction to the network.

b. IA personnel will scan all similar ISs or devices on the compromised network for configuration compliance or

vulnerability identification and immediately correct vulnerable systems. If during the course of this assessment additional ISs are identified as compromised, IA personnel will report these system as compromised and take no further action.

c. Networks may require re-accreditation, under the DIACAP, following any successful compromise.

d. Specific details and actions for a compromised system are available on the ACERT Web site.

Section IX
Information Assurance Vulnerability Management

4–24. Information assurance vulnerability management reporting process

a. General. The Information Assurance Vulnerability Management (IAVM) Program is the absolute minimum standard for all ISs, not the preferred end state which is a proactive methodology of maintaining, patching, and updating systems before notification or exploitation. IAVM requires the completion of four distinct phases to ensure compliance. These phases are—

(1) Vulnerability identification, dissemination, and acknowledgement.

(2) Application of measures to affected systems to make them compliant.

(3) Compliance reporting.

(4) Compliance verification.

b. Responsibilities. The CIO/G–6 will be the POC to acknowledge receipt (within five days) of DOD CERT issued IAVM messages, aggregate compliance and waiver data, and report (within 30 days or as directed) to DOD. Systems and processes for collecting detailed information and for implementing IAVM are the responsibility of every IA person.

c. Army implementation of IAVM. ACERT/A–GNOSC will serve as the Army's focal point for initiation of the IAVM process.

(1) *Vulnerability identification, dissemination, and acknowledgment.* ACERT/A–GNOSC will issue Army IAVM messages. There are three types of DOD IAVM messages: alert (IAVA), bulletin (IAVB), and Technical Advisory (TA). DOD has restricted the use of these terms to the IAVM program only.

(a) IAVAs will establish mandatory suspense dates for acknowledgement and compliance, corrective actions to negate vulnerabilities, and implementation of additional CND requirements.

(b) IAVBs will establish mandatory suspense dates for acknowledgement yet allow commanders and IA personnel flexibility for implementation of the corrective actions to negate vulnerabilities or implementation of CND requirements. Corrective actions are required to be completed, but not reported.

(c) Information Assurance Technical Tips (IATTs) (Army designation) allow commanders and IA personnel flexibility for acknowledgement and implementation to negate vulnerabilities or implement CND requirements. Acknowledgement and compliance are not reported. Corrective actions are required to be completed but not reported.

(d) All personnel responsible for implementing the IAVM process will join the Army IAVM Community Group on AKO to receive messages. Use only official e-mail accounts for this distribution list. IAVM messages are available on the asset and vulnerability tracking resource (A&VTR) Web site.

(2) *IAVM compliance.* Commanders, PEOs, PMs, and designated IA officers will disseminate implementation guidance and ensure compliance to IAVM requirements. Commanders or IA personnel will provide contractors, contracted support, or other personnel (as necessary) IAVM information as required to support compliance requirements.

4–25. Compliance reporting

a. The RCIOs, ACOMs/ASCCs/DRUs commanders, PEOs, PMs (or their IA officers), and garrison commanders will ensure that messages are acknowledged, corrective actions are implemented, extensions are requested, compliance is verified, and reporting information is entered into A&VTR. Within 10 calendar days from the date of the IAVM message, SA/NAs will conduct a baseline assessment scan for affected assets and enter identified assets into A&VTR. RCIOs will oversee IAVM compliance reporting for their regions or commands.

b. PEOs and PMs will implement corrective actions for IAVM vulnerabilities that apply to systems under their control. Tactical systems will document compliance methodology in a classified Scorecard and POA&M as part of their C&A package. DAAs will resolve compliance issues where it may result in safety or performance issues of a combat system that are operationally unacceptable.

c. If corrective actions required by issued alerts adversely affect operations, IAMs or their designated representatives (for example, affected SAs or IANMs) will conduct a risk assessment for the commander and contact their supporting RCIO, IAPM, or IAM. The RCIO, IAPM, or IAM will contact the CIO/G–6 through ACERT/ NETCOM/9th SC (A) to request an extension, not to exceed 180 days, and to develop and implement an acceptable alternative security solution. The alternative security solutions must be coordinated with the ACERT/ NETCOM/9th SC (A) before approval by the appropriate DAA. This extension request will include risk mitigation steps taken to reduce or eliminate the IAVM-

identified risks until an acceptable solution is implemented. The extension request will include a POA&M (get well plan) to be considered in the CA risk determination.

d. IAVM compliance reporting will be accomplished through the Army's A&VTR. To meet DOD requirements, register specific system/asset owners and SAs, including applicable electronic addresses, in A&VTR.

e. All IAVM compliance reporting of classified, tactical, or operationally sensitive ISs will be through the A&VTR when located on the SIPRNET.

4–26. Compliance verification

IAVA Compliance Verification Teams (CVTs) will conduct short-notice inspections of randomly selected units to verify compliance with IAVM messages.

a. Membership in the CVT may include a CIO/G–6 Team Chief; a vulnerability scan technician; U.S. Army Audit Agency representatives, operating under AR 36–2 and AR 36–5; and U.S. Army Criminal Investigation Command representatives operating under AR 195–2.

b. In addition to reporting requirements under AR 36–2, AR 36–5, and AR 195–2, the CVT will report to the inspected unit, the CIO/G–6, and the Senior Army Leadership. The CIO/G–6 will provide a copy to the appropriate ACOM, ASCC, PEO, and PM CIOs.

c. Findings require a reply by endorsement on the corrective actions taken by the inspected command.

4–27. Operating noncompliant information system

Commanders, organization directors and responsible individuals for example; DAAs, IAPMs, or IAMs, will operate noncompliant assets only with an approved Mitigation Action Plan (MAP) and POA&M. MAPs are temporary measures approved to permit additional time or develop solutions to bring noncompliant assets into compliance. The POA&M identifies the get well plan including the schedule. Noncompliant assets without an approved MAP will be disconnected, blocked, or otherwise have the vulnerability mitigated. Organizations and individuals operating noncompliant assets are accepting risks, accountability, and responsibility for internal and external impacts to the network in the event the system is compromised or the vulnerability is exploited.

a. Establish a capability to implement or effectively mitigate the risk posed by critical vulnerabilities as identified in IAVA notifications.

b. MAPs will address specific actions taken to mitigate risks identified in IAVA messages.

c. MAPs are tracked in A&VTR Database. Approvals and denials are granted at the appropriate DAA, DOIM, ACERT/A–GNOSC, and HQDA levels, and in some instances approvals are reserved only for the DCS, G–3/5/7.

d. MAPs focus on systems not able to comply within the period specified in the IAVA notification message. Organizations will first use all their available resources to ensure vulnerable systems are patched before requesting extensions. MAPs will reflect a detailed reason, operational impact statement, efforts to bring the systems into compliance, and a mitigation strategy.

e. First MAP requests: The DAA for the ICAN may approve MAPs up to 30 days from the compliance date on the IAVA message and includes the number of impacted systems not able to comply within period specified in the notification message. The First MAP begins the day after the original IAVA compliance suspense and is valid for up to 30 days. Approval will be based on a sound MAP that minimizes the risk of compromise to Army networks.

f. Second MAP requests: This MAP will be valid up to 60 days after the end date of the local DAA approved 30-days and will reflect the number of remaining systems not able to comply after the 30-day approval from the local DAA. The Director, NETCOM Office of Information Assurance and Compliance (OIA&C), approves second MAPs with ACERT/A–GNOSC A2TAG recommendations.

g. Third MAP requests: The CIO/G–6 approves third MAPs. They are reserved for rare cases where circumstances have prevented compliance with an IAVA during the timelines for first or second MAPs, to include mission required legacy systems. Third MAPs begin the day after the second MAP ends and runs for a period directed by the approval authority, for a maximum of 2 years.

h. The A&VTR keeps a history file of all MAP actions. Open MAPs will be reviewed and revalidated within A&VTR.

i. If an IAVA message states: DCS, G–3/5/7 approval only, then the MAP can only be approved by the DCS, G–3/5/7 with recommendations accepted from the local DAA, the NETCOM OIA&C Director, and the CIO/G–6.

Section X
Miscellaneous Provisions

4–28. Vulnerability and asset assessment programs

Several Vulnerability Assessment Programs and services are available throughout the Army. The ACERT/A–GNOSC provides comprehensive support in the areas of CND and IA Vulnerability Assessments; the U.S. Communications-Electronics Command (CECOM) provides assessments and support in the areas of platforms and IA architecture; the

Army Research Laboratory (ARL) may provide support in the areas of survivability and lethality; and CID provides comprehensive crime prevention surveys.

a. All scans will be coordinated within AOR between the initiating or oversight component and the supporting RCERT/TNOSC.

b. Prohibit scans across network segments protected by a TNOSC security router or IDS, unless specifically coordinated and approved by NETCOM/9th SC (A).

c. Only trained or product certified personnel will use assessment software.

d. Before conducting mapping or scanning of a network, war dialing, or war driving, the IAM will notify the DOIM and the servicing RCERT/TNOSC with the purpose, start, type and duration of the scanning activity.

e. Personnel will provide a copy of the assessment results to the servicing DOIM and RCERT/TNOSC.

f. Installations that do not have the expertise, requisite certification level, or resources to scan their own networks may request an assessment scan through their supporting RCERT/TNOSC.

g. Commanders, IA personnel and network management personnel will treat unannounced or unauthorized scanning of networks as potential intrusions and report when detected. Persons conducting unauthorized scans of Army networks may be subject to administrative actions or criminal prosecution.

h. IAMs and IASOs will establish procedures to scan their networks quarterly to identify assets; application, network, and operating system vulnerabilities; configuration errors; and points of unauthorized access.

i. Train all IA participants on approved scanning tools and assessors will sign an acknowledgment of complete understanding of the "rules of engagement" before conducting any scanning activity. For example—

(1) No reading of personal data on networks while conducting a vulnerability assessment.

(2) No penetration testing.

(3) No denial-of-service attacks or tests.

(4) No scanning outside local network enclave borders.

j. Utilize the Do-it Yourself Vulnerability Assessment Program (DITY VAP) to assess configurations, compliance, asset identification, unauthorized connectivity, and security vulnerabilities within local network enclave borders. DITY VAP assessments prohibit the use of data corruption, data manipulation, data denial, examination of data content, denial of service, or "hacking" and penetration tools and techniques.

k. Information Operations Vulnerability Assessments Division (IOVAD) Blue Team and Red Team Programs. The 1st IO CMD IOVAD offers assessment support in the areas of information management and security, in which focused efforts assess IA through the elements of OPSEC, COOP, INFOSEC, COMSEC, and CND. In addition, IOVAD Red Teams are available to challenge and assess readiness.

l. RCERTs and TNOSCs may conduct no-notice remote scanning across enterprise boundaries, including, but not limited to, IAVM support, threat or asset identification, or vulnerable systems and services identification, with or without coordination with commanders or IA personnel. Assessment scanning from authorized external organizations is normally conducted from documented and readily identified systems. IA personnel will implement verification procedures to validate, but not hinder or deny, these scanning activities. RCERTs and TNOSCs may block or deny access to vulnerable systems identified during these scans until corrections have been made.

4–29. Portable electronic devices

Portable electronic devices (PEDs) are portable ISs or devices with or without the capability of wireless or LAN connectivity. These include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (for example, Palm Pilots, Pocket PCs), laptops, memory sticks, thumb drives, and two-way radios. Current technologies (infrared, radio frequency, voice, video, microwave) allow the inclusion of numerous capabilities within a single device and dramatically increases the risks associated with IS and network access. Management of these devices will be as follows:

a. PEDs containing wireless communications or connectivity, audio, video, recording, or transmission capabilities will be prohibited from areas where classified information is discussed or electronically processed, unless specifically documented in the C&A package and permitted as an exception by the DAA and all classification, access, and encryption restrictions are enforced for the PED as they would be for a classified device.

b. Implement identification and authentication measures at both the device and network level if connectivity is approved. Voice does not require DOD PKI IA.

c. PEDs will support PKI, digital certificates, FIPS, or NSA validated crypto modules or data encryption standards appropriate for the classification level of the information processed.

d. Provide all PED users with security awareness training regarding the physical and information security vulnerabilities and policies of the device.

e. Contractor provided or owned PEDs (if approved) will be stated as mission essential in contracts, and will meet all C&A standards and are subject to inspections and IA requirements as any other IS.

f. Employee owned PEDs are prohibited for use in official communications or connections to Army networks.

4–30. Wireless local area networks

Wireless LANs are extensions of wired networks and will implement IA policies and procedures in accordance with this and other applicable regulations. Non-compliant wireless LANs will have migration plans documented in POA&Ms, that ensure the systems will meet the minimum requirements of this policy. The DAA will consider the POA&M in the authorization decision. All Army organizations and activities operating wireless local area networks (WLANs) will comply with the following and as supplemented in BBPs:

a. Pilot and fielded wireless LANs and PEDs with LAN connectivity will meet the same C&A and IA security requirements as wired LAN ISs in accordance with this regulation, AR 380–53, AR 25–1, and DODI 8500.2.

b. DOIMs and IAMs will verify the IA C&A authorization of WLANs that connect to the installation.

c. SOs will configure and install wireless solutions to preclude backdoors.

d. Where wireless LANs are implemented or proposed, thorough analysis, testing, and risk assessments must be done to determine the risks associated with potential information intercepts or monitoring, TEMPEST emanations, and network vulnerability.

e. The use of AV software on wireless-capable ISs and devices is required.

f. Users will be authenticated to the devices authorized for WLAN.

g. DOIMs and IAMs will control, monitor, and protect wireless access gateways with firewalls and IDS devices.

h. Certify all wireless devices procured with Army funds for spectrum supportability through the Military Communications Electronics Board (MCEB) per DODD 5000.1 and AR 5–12. Submit spectrum supportability requests to NETCOM/9th SC (A), ATTN: NETC–EST–V, Suite 1204, 2461 Eisenhower Avenue, Alexandria, VA 22331–0200.

i. DOIMs and IAMs will terminate wireless access points at a boundary device in the DMZ, not in the internal enclave.

j. Certify that WLAN frequencies meet any host nation or Government restrictions.

4–31. Employee–owned information systems

a. Prohibit the use of employee-owned information systems (EOISs) for classified or sensitive information.

b. The use of an EOIS for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with IAM, DAA, or commander approval. Requirements for use and approval are included in AR 25–1.

c. If approved for ad hoc use, EOISs processing official data will comply with all security provisions of this regulation. Computer owners will implement IA countermeasures required by this regulation, specifically AV and IA software and updates, or be prohibited from such activity. All processed data will be removed from the EOIS and personnel will sign compliance statements that the data was removed.

d. Include security requirements and authorized software availability for the use and safeguarding of EOISs in security training.

e. Contractor-owned and operated ISs will meet all security requirements for Government-owned hardware and software when operating on the AEI, managing, storing, or processing Army or DOD data or information, or conducting official communications or business.

f. Scan all data processed from an EOIS before inclusion or introduction into the network.

g. Prohibit all remote access for remote management from any EOISs.

4–32. Miscellaneous processing equipment

There is a variety of non-COMSEC-approved miscellaneous process equipment (MPE) involved with classified or sensitive information. This includes copiers, facsimile machines, peripherals, electronic typewriters, word processing systems, and others. Activities must identify those features, parts, or functions used to process information that may retain all or part of the information. Security procedures must prescribe the appropriate safeguards, in accordance with AR 380–5, chapter 7 to prevent unauthorized access to either the information or equipment.

a. Digital copiers, printers, scanners, faxes, and similar IS devices employ embedded hard-drives or other media that may retain residual classified or sensitive information. Include these devices as part of the C&A process.

b. Destroy replaced equipment parts per classification level when removed.

c. Cleared and technically qualified personnel will inspect equipment before equipment removal from protected areas.

d. Peripheral devices (for example, printers, copiers) are subject to IAVM compliance and accreditation.

e. Peripheral devices (for example, printers, copiers) are subject to sanitizing, purging, or disposition restrictions as published.

Chapter 5
Certification and Accreditation

5–1. Certification and accreditation overview

a. This chapter outlines the policies governing the Information Assurance Certification and Accreditation (IA C&A) of ISs which includes networks in accordance with DODD 8500.1, DODI 8500.2, P.L. 100–235, OMB Circular A–130, DODD 5220.22, DOD 5220.22M, DOD 5220.22–M–SUP, and 44 USC 3541 as it pertains to C&A. The goal of IA C&A is to understand the vulnerabilities, determine the risk introduced through operations or connections of the system, and provide appropriate information for the DAA to consider the IA risk in contemplating an approval to operate decision. This section streamlines some of the process to enable those risk determinations to be made consistently, economically and timely.

b. C&A policy is found in this regulation and is supported by the guidelines located in the C&A BBP—

(1) The IA C&A Process BBP.

(2) The IA C&A DAA BBP.

(3) The IA C&A Certification Authority (CA) BBP.

(4) The IA C&A Agents of the Certification Authority (ACA) BBP.

c. All ISs will be certified and accredited in accordance with the Interim DIACAP documenting compliance, at a minimum, with this regulation, and DODI 8500.2 IA controls associated with the specific MAC and confidentiality level. C&A will be performed according to the type accreditation process or by the site-based accreditation process. The IS being accredited may be considered as a single system, system of systems, enclave or network.

d. Army DODIIS systems will be certified and accredited by the DCS, G–2 for PL 1, 2 and 3 in accordance with DCID 6/3.

e. Information systems currently operating under an ATO will not need to redo the accreditation under this new process until such time as the approval expires or is otherwise revoked. This could be the result of 3 years expiration, annual revalidation results, caveat in the ATO, major change in the system, its environment or operations, or as required by the DITSCAP.

f. Tactical IS must address their tactical and garrison configuration and environment (if they intend to operate in garrison on a live network or with live data) during the C&A process.

g. Tactical IS that are subject to deployment must have a "fly away" package of IA information to provide to their network service provider as required. Refer to the C&A BBP for details on the composition of the fly away package.

h. A Government SO will be identified for each IS used by or in support of the Army. The SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented and provided as an artifact to the accreditation package.

i. If the SO can not be identified, then the IS should be deemed unnecessary and removed from Army inventory.

j. When selecting software, priority should be given to software with vendor integrity statements (VISs) that verify that vendor software will not affect the integrity of operating systems when utilized.

k. When selecting software priority should be given to corporations that develop, manufacture and manage software that are U.S. owned, controlled or influenced.

l. Foreign-Ownership, Control, or Influence (FOCI) will be taken into account prior to software development, integration, or purchase and identified in the IS C&A package.

m. Published or established NETCOM/9TH SC (A) CCB and Networthiness certification requirements will be incorporated during the C&A process.

5–2. Certification

a. Authority and responsibility for certification is vested in the Army Federal Information Security Management Act (FISMA) Senior IA Officer (SIAO). The Director OIA&C, NETC–EST–I, was appointed as the FISMA SIAO by the DA CIO/G–6 and will be the single Army CA. The Army CA is the single authority for CA recommendations to all Army DAAs with the exception of IS completing C&A under the DODIISS Program.

b. The Army CA will maintain a list of qualified Government organizations and labs, as trusted Agents of the CA (ACA), to perform the certification activities. The reimbursable ACAs are available to provide SOs with certification capabilities. While the lead ACA will report the results of the certification activities to the CA, only the CA will make the operational IA risk recommendation to the DAA in support of an approval to operate decision.

c. Organizations can request appointment as an ACA by following the process in the IA C&A ACA BBP.

d. It is the responsibility of the SO to plan and budget for IS certification and accreditation efforts.

e. It is the responsibility of the SO to select from the approved ACA list an ACA organization that best supports the program requirements, such as those of cost and schedule.

f. IA certification considers—

(1) The IA posture of the IS itself, that is the overall reliability and viability of the IS plus acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself.

(2) How the system behaves in the larger information environment (for example, does it introduce vulnerabilities to the environment, does it correctly and securely interact with the information environment management and control services).

g. The ACA certification determination is based on actual results of the validation and the risk introduced by non-compliance with stated requirements.

h. Certification represents proof of compliance with this regulation and the DODI 8500.2 IA controls for the appropriate MAC level and the Confidentiality level, at a minimum. Non-compliance will require the creation of a POA&M to bring the IS into compliance.

i. DCS, G–2 is the Service Certifying Organization for the Army DODIIS Program up to PL 4.

5–3. Tailoring

a. The time and labor expended in the C&A process must be proportional to the system mission assurance category (MAC) level, confidentiality level, and number of users.

b. The activities defined in the DIACAP are mandatory. However, implementation of these activities and their output should be tailored as appropriate and integrated with other acquisition activities and documentation where applicable.

c. Compliance with Information Assurance controls is not a tailorable factor. All applicable IA controls must be met either by incorporation, inheritance, waiver or exception.

5–4. Accreditation

a. Accreditation is the official management authorization to operate an IS or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements. The C&A statement affixes security responsibility associated with operational IA risk with the accrediting authority.

b. Accreditation must address each operational environment of the IS for both fixed and deployable configurations. For example, an IS may operate at one confidentiality level in a standalone mode and connect to a global network at another confidentiality level. The C&A must clearly establish procedures for transition between the two environments. Multiple operational environments can result in multiple accreditations for a single IS if different DAAs are involved. However, in the concept of the operations document, a single accreditation that addresses all variations is sufficient. Refer to the C&A BBPs for further guidance and procedures on IS accreditation.

c. Site-based accreditations are appropriate for a single unit or for a LAN with appropriately accredited ISs generally performing similar functions with similar equipment.

d. Type accreditations are appropriate for IS fielded to multiple users under the PEO/direct–reporting PM structure to multiple locations. Additionally, type accreditations are appropriate whenever a single office or agency is responsible for fielding an IS to multiple Army users at multiple locations. Type accreditations must indicate whether they are a generic accreditation of centrally fielded IS or an operational accreditation of IS that are procured or obtained locally, and whether a single identifiable system or group of similar systems is covered.

5–5. Recertification and re–accreditation

a. Information systems will be recertified and reaccredited once every three years. Each of the IA Controls assigned to the information system must be revalidated. The results of validation tests of IA Controls conducted during an annual review may be used in the recertification and re-accreditation of the information system if performed within one year.

b. Not less than annually, the SO will provide a written statement or digitally signed e-mail to the CA that either confirms the effectiveness of assigned IA Controls and their implementation, or recommends changes or improvements to the implementation of assigned IA controls, the assignment of additional IA controls or changes or improvements to the design of the IS itself.

c. This annual revalidation may be performed as a self assessment. However, a third party independent evaluator must perform the validation every 3rd year, at a minimum.

d. The CA will review the written statement and make a recommendation to the DAA.

e. The DAA will evaluate the recommendation, mission, and information environment indications, and determine a course of action.

f. The DAA may use any favorable annual review to re-authorize processing under the current authorization termination date (ATD) or adjust the ATD for an additional year.

g. The DAA may use any unfavorable annual review to downgrade the accreditation status to:

(1) An IATO and reset ATD to 180 days. The SO will prepare a POA&M executable within the 180 days.

(2) Denial of authorization to operate (DATO). Operation of the IS will be halted until the IS is brought into compliance.

h. The results of the annual reviews will be reported in the Army Portfolio Management Solution, as appropriate, and become part of the IS accreditation package until the IS is decommissioned.

5–6. Accreditation documentation

a. The SO will forward to the receiving ACOM/ASCC, installation, and/or activity DAA and applicable NETCOM RCIO, a copy of the accreditation decision, supporting C&A documentation and Certificate of Networthiness (CON). The DAA or representative, together with the command functional user representative and NETCOM RCIO, will review the C&A package and either accept the accreditation decision as is or implement additional measures or procedures to meet the needs of their unique operating environment. Such additional measures will be appended to the system accreditation and provided to the CA for consideration in the operational IA risk recommendation to the gaining DAA for approval in that unique environment.

b. SCI systems will not obtain a CON, but will follow the DCID 6/3 requirements.

c. There are four potential DAA accreditation decisions: ATO, IATO, IATT, and DATO.

d. The ATO decision which will specify an authorization termination date (ATD) that is within three years of the authorization date.

e. The IATO decision which will specify an ATD that is within 180 days of authorization, limited to no more than one IATO extension. IATO requests must be accompanied by a POA&M, with corrective actions funded and achievable within the authorization period.

f. The IATT decision which will specify an ATD the is consistent with the completion of the test. The IATT establishes the agreed upon test duration and any special considerations or constraints.

g. The DATO decision will specify and effective date. The DATO is effective until the DAA believes the IA posture of the IS has been raised to an acceptable level.

5–7. Connection approval process

a. Army organizations requiring network access to the Defense Information Systems Network (DISN) will prepare a CAP package requesting connection approval. Army organizations requiring network access to the DISN will prepare a CAP for submission to the proper DISA IA office. The DISA IA office will review the CAP package and approve/disapprove customer for access to the DISN. Approval will be granted with an interim authority to connect (IATC) authority to connect (ATC) letter.

b. Interconnection of two or more enclaves requires DAA approval through MOUs or Memoranda of Agreement (MOAs) between all DAAs. MOUs/MOAs will address interconnection requirements as outlined in DODI 8500.2.

c. All IS must obtain CON as approval to connect through the Networthiness process prior to becoming operational within the Army.

d. An enclave's MAC level and security domain remain fixed during interconnection to other enclaves; they do not inflate to match the MAC level or security domain of an interconnecting enclave. Enclaves with higher MAC levels connecting to enclaves with lower MAC levels are responsible for ensuring that the connection does not degrade the availability or integrity of the higher enclave.

e. Interconnections that include or impact the DISN or JWICS are subject to DISN or JWICS connection management requirements and processes.

f. Interconnections that cross security domains are subject to DOD policy and procedures for controlled interfaces and cross domain solutions (CDS) as appropriate.

g. Adjunct networks that rely on the installation network for NIPRNET and SIPRNET services will provide their C&A documentation to the installation DAA for approval prior to connecting to the ICAN.

h. Interconnections that include or impact the JWICS are subject to DIA connection approval process management requirements.

5–8. Designated approving authority

a. The DAA is vested with the authority to formally assume responsibility for operating an IS at an acceptable level of risk. The DAA must weigh the operational need for the systems capabilities, the protection of personal privacy, the protection of the information being processed, and the protection of the information environment, which includes protection of the other missions and business functions reliant on the shared information environment.

b. The DAA may rely on the Army CA operational IA risk recommendation and may authorize operation through the approval of an ATO, IATO, IATT, or deny operations through a DATO. Absent an accreditation decision an IS is considered unaccredited and will not be operated within or in support of the Army.

c. A DAA may downgrade or revoke their initial Accreditation Decision any time risk conditions or concerns so warrant.

d. A DAA will be identified for each information system operating within or on behalf of the DA, to include outsourced business processes supported by private sector IS and outsourced IT (for example, Government owned, Contractor Operated (GOCO) and Contractor Owned, Contractor Operated (COCO).

e. DAA responsibility must reside with the organization that maintains funding, management and operational control

over the IS while in development, and once deployed, as applicable. In the instance of type accreditation these may be different organizations but will have documented MOUs when the transfer is made.

f. The CIO/G–6 will remain the DAA for Army information systems, with the exception of Army SCI systems.

g. The CIO/G–6 will appoint in writing, or digitally signed e–mail, all Army DAAs with the exceptions noted below. Existing appointments or delegations will become invalid within 90 days of the approval date of this AR 25–2 C&A update. Requests for appointment must be submitted to the OIA&C for processing during these three months. DAA responsibility can be assigned to a position in the organization; however, appointments will always be to named individuals. DAA appointment will be for specific named systems or networks. The OIA&C, NETC–EST–IC, will coordinate the DAA appointments on behalf of the CIO/G–6.

h. All DAAs will be at the General Officer, Senior Executive Service or equivalent level regardless of the confidentiality level at which the IS operates. This appointment will not be further delegated or appointed downward except as noted below or as approved by the CIO/G–6.

i. All DAAs will be U.S. citizens, DOD employees, hold a U.S. Government security clearance and formal access approvals commensurate with the level of information processed by the IS under their jurisdiction, or a Secret clearance, which ever is higher.

j. All DAAs will have a level of authority commensurate with accepting in writing the risk of operating DA IS under their purview.

k. All DAAs will complete IA training consistent with the Army Training BBP. A copy of the completion training certificate must be provided to CIO/G–6 through the OIA&C prior to assuming DAA duties.

l. DAA appointment must be requested of the CIO/G–6. Requests for appointments should be consistent with the following examples when compliant with 5–8*h* through *k*, above:

(1) The Commanding General (CG), NETCOM for the Army enterprise with the authority to appoint the Director NETCOM ESTA for the Army enterprise.

(2) PEOs or direct-reporting PM for acquisition systems developed under their charter except as noted below.

(3) Principal Army Staff officers for Army Staff unique systems that remain under that office's control and management after deployment, except as noted below.

(4) CAR for the USAR, with the authority to appoint the USAR COS for the ARNET.

(5) Chief, ARNG for the ARNG and GuardNet XXI, with the authority to appoint ARNG state DOIM/J6/CIO for individual states, as appropriate.

(6) The AASA as the ACOM/ASCC commander for Pentagon ITS, to include IS connected to the Pentagon CIT enterprise, associated swing space, and alternate COOP sites through the national capital region (NCR) with the authority to appoint those GO, SES or equivalent within AASA purview that are the SOs or have life cycle responsibility for the IS, as appropriate.

(7) The MEDCOM Commander, with the authority to appoint the MEDCOM RMC/MSC Commanders for medical, dental and veterinary activities and treatment facilities, as appropriate.

(8) The USACE CIO for the USACE WAN and corporate IS, with the authority to appoint the USACE Division Commanders for USACE IS, as applicable.

(9) The Commander USAREUR, with the authority to appoint DAAs for tenant and MSC commanders within USAREUR, as appropriate.

m. The following C&A DAA positions remain in place:

(1) The CIO/G–6 for Army Special Access Programs.

(2) The CIO/G–6 for classified systems developed by DA staff agencies.

(3) The DCS, G–2 for DODIIS processing SCI at Protection Level 1, 2, and 3.

(4) The Director, National Security Agency for cryptographic solutions used to protect classified information.

(5) The Director, Joint Staff is the DAA for systems that process SIOP–ESI data.

(6) Commander, INSCOM for signals intelligence (SIGINT) systems within the Army.

n. Questions concerning DAA requests or appointments should be directed to the OIA&C at iacora@us.army.mil.

o. DAAs may assign members of their staff to act as their representative during the C&A process. However, signature authority will remain with the individual appointed by the CIO/G–6. Following the chain of command the DAA may authorize a member of his/her staff to "sign for" him/her, but the signature block and responsibility will remain with the CIO/G–6 appointed individual. A copy of the authorization memo will be submitted to the CIO/G–6 through iacora@us.army.mil.

5–9. Lead agent of the certification authority

a. Lead ACA and ACA organizations will be designated by the CA through the process documented in the IA C&A ACA BBP.

b. The lead ACA will be, at a minimum, a Government employee, a U.S. citizen, at least a LTC, GS–14, or equivalent, and be appropriately cleared (Secret at a minimum). Refer to the ACA BBP for further details.

c. The lead ACA will be responsible for preparation, planning and conducting the certification testing.

d. The reimbursable ACA will perform the following, at a minimum:

(1) Prepare IA Certification Event Test Plans.

(2) Conduct IA Certification Test Events and STE as appropriate.

(3) Prepare IA Certification Test Event Reports.

(4) Prepare IA Scorecards.

(5) Prepare IA Risk Assessments from the IA Certification Test Event findings, at a minimum.

(6) Provide the IA certification results and any supporting documentation to the Army CA for consideration in the IA operational risk recommendation.

e. ACA organizations may perform other functions as negotiated by the SO.

f. The ACA concept does not apply to DODIIS and SIGINT systems. Certification of these systems will be conducted in accordance with DCID 6/3.

5–10. System owner

a. A Government SO will be identified for each IS used by or in support of the Army. The SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person, organization or agency, and such transfer is appropriately documented and provided as an artifact to the accreditation package.

b. The SO is responsible for the certification and accreditation of the IS and will provide the C&A package to the Army CA in sufficient time for review and determination of operational IA risk recommendation in support of DAA approval to operate decision prior to operational use or testing on a live network or with live Army data.

c. The SO will ensure that the C&A package and the SSAA are provided to the ACOM/ASCC, RCIO IAPM, and NETCOM prior to IOT&E on/or before deployment of the system.

d. If the SO can not be identified, then the IS should be deemed unnecessary and removed from the Army inventory.

e. It is the responsibility of the SO to plan and budget for IS certification efforts.

f. It is the responsibility of the SO to select the ACA that best supports his requirements, such as those of cost and schedule.

g. Not less than annually all SO will provide a written statement or digitally signed e-mail to the Army CA that either confirms the effectiveness of assigned IA Controls and their implementation, recommends changes or improvements to the implementation of assigned IA controls, or assigns additional IA controls, changes or improvements to the design of the IS itself.

h. The system owner will forward to the receiving ACOM/ASCC, installation and activity DAA a copy of the accreditation decision, supporting C&A documentation and CON.

Chapter 6
Communications Security

6–1. Communications security overview

This chapter provides DA policy for the acquisition, implementation, and life cycle management of cryptographic systems, products, and services used to protect sensitive and classified national security information, systems, and networks. All tactical ISs are considered critical to the direct fulfillment of military or intelligence missions, and therefore are regarded as national security systems. With the exception of those systems approved by NSA and endorsed by HQDA CIO/G–6, at no time will U.S. classified national security information be protected by foreign cryptographic systems or products, or by a NIST/NIAP common criteria testing laboratory evaluated product. Exceptions will be re-approved on an annual basis. Use of any unapproved product to protect classified national security information will be considered as a reportable communications security incident under AR 380–40, paragraph 7–3*b*

a. Protection of classified information and systems whether national security systems (NSS) or non-NSS. Only NSA-approved cryptographic systems will be used to protect classified national security information and national security systems.

(1) Classified national security information will be protected in transmission by NSA approved cryptography.

(2) Tactical information systems will be protected by NSA approved cryptography.

(3) Requirements for NSA-approved cryptographic systems will be identified and validated in the AIAP and managed by the Army IAD.

(4) NSA cryptographic systems will be centrally acquired and managed by the CSLA.

(5) Only keying material produced by NSA or generated by NSA-approved key generators will be used to key cryptographic systems that protect classified national security information.

(6) All cryptographic systems employed in the tactical force structure that protect classified national security

information must be Army Electronic Key Management System/Key Management Infrastructure (EKMS/KMI) compliant. Each approved cryptographic system will have a NSA approved key management plan.

b. Protection of unclassified and sensitive information and systems. NIST/NIAP approved cryptographic systems will only be used to protect Unclassified or Sensitive information. NIST/NIAP approved cryptographic systems or foreign cryptographic systems to be employed in the tactical force structure will be approved on a case-by-case basis by the HQDA CIO/G–6. Company and Below Units may use NIST/NIAP approved cryptographic systems for protecting Non-Mission/Non-Operational unclassified or sensitive information. Cryptographic systems or products intended for the protection of unclassified or sensitive information or systems will—

(1) Be evaluated by a NIAP-certified common criteria testing laboratory, and at a minimum, meet all requirements of Evaluation Assurance Level (EAL) 3 and the common criteria controlled access protection profile.

(2) Be validated under the NIST Cryptographic Module Validation Program (CMVP) that, at a minimum meet, level 2 security requirements of the Federal Information Processing Standard 140–2 (FIPS 140–2).

(3) Products that exceed minimum FIPS 140–2 security requirements and common criteria evaluation assurance levels will be given preference when considered for procurement.

(4) NIST/NIAP-approved cryptographic systems intended to protect unclassified sensitive information will be identified in the AIAP and managed by the Army IAD. Funding for these systems will be the responsibility of the organization or activity identifying the requirement.

(5) All NIST/NIAP-approved cryptographic systems will be centrally acquired and managed through CSLA.

(6) Each NIST/NIAP-approved cryptographic system will have a key management plan that describes in detail all activities involved in the handling of cryptographic keying material for the system, including other related security parameters (such as IDs and passwords). The plan will describe accountability over the keying material over the entire life cycle of the system's keys from generation, storage, distribution, and entry into the system through use, deletion, and final destruction.

c. Data Encryption Standard (DES). All implementations of FIPS 46–2 DES are prohibited within the Army.

d. Advanced Encryption Standard (AES). The implementation of AES in products intended to protect classified national security information and systems must be reviewed and certified by NSA, and approved by HQDA CIO/G–6 prior to their acquisition through CSLA.

e. Public key cryptography. Systems that employ public key (asymmetric key) technology to protect unclassified sensitive or classified national security information and systems will be approved by the CIO/G–6. Asymmetric keys will be obtained through authorized DOD or Army certificate authorities operating under current DOD-approved Certificate Practice Statements.

f. Approved Cryptographic Systems and Algorithms. The CSLA will maintain a list of approved cryptographic systems and algorithms for use in the Army. All cryptographic products must be procured through CSLA to be valid for use on an Army system. CSLA managed Army Approved Product List (APL) is available by calling the CSLA customer support help desk at 1–800–662–2123 or from the CSLA Web page (when established).

6–2. Protected distribution systems

a. A protected distribution system (PDS) will be used only if cost-effective and sufficiently controlled to prevent covert penetration and interception.

b. Any IS that includes a PDS to transmit data will not be operationally accredited until the PDS has been approved.

6–3. Approval of protected distribution systems

a. PDSs must be constructed per criteria contained in NSTISSI No. 7003 and supplemented with IA procedures in this regulation.

b. Authority to approve a PDS for the clear text transmission of classified information within fixed plant and garrison installations is delegated as follows:

(1) Principal HQDA officials for activities under their staff supervision, direction, or control.

(2) Garrison commanders for their organic activities.

c. Requests for approval of a PDS to transmit TS information must include an evaluation by the appropriate support element. Approval authorities may request technical assistance from INSCOM, 902nd MI Group, Fort Meade, MD 20755, in applying security criteria and processing the approval action for other PDSs.

d. Commanders of battalion and higher echelons may approve circuits for clear text electrical transmission of SECRET and CONFIDENTIAL information in tactical environments. Under combat conditions, commanders may delegate this authority to the company level. Tactical PDSs will not be approved for clear text transmission of TS information.

e. Once a PDS has been approved, no changes in installation, additions, or use may be made until the approval authority has granted approval for such changes.

f. Requests to approve a PDS will be submitted through channels to the installation IAM and DAA. Requests will be classified at least CONFIDENTIAL and will contain the following information:

(1) Full identification and location of the requesting organization.

(2) A statement of the classification of information to be transmitted on the PDS.

(3) A copy of the building floor plan (or a diagram of the field area as appropriate) designating the following:

(a) Proposed cable route and location of subscriber sets, distribution frames, junction boxes, and any other components associated with the circuit.

(b) Other wiring along the PDS route.

(4) Description of the cable installation (for example, 24 pairs of shielded cable in rigid steel conduit, 6 pairs of shielded cable in floor, or fiber optic cable). Indicate the cable length.

(5) Description and nomenclature of terminal and subscriber equipment to be used.

(6) Clearance of individuals having access to the circuit.

(7) Type of guards (for example, U.S. military, U.S. civilian, foreign civilian) and their security clearance or access authorization status.

(8) Description of access control and surveillance of uncleared personnel who may be allowed entry into the area housing any part of the PDS.

(9) Identification of the power source to be used for the PDS and a statement of the distance to the nearest point where undetected tampering would be possible.

(10) A justification for using the proposed PDS.

(11) A statement concerning any deviations from the established PDS criteria and an evaluation of their security implications.

(12) For PDSs to be used with TS information, a copy of the security evaluation.

(13) The request and approval must become part of the C&A package.

6–4. Radio systems

a. Protect all voice or data military radio systems and COTS-implemented cellular or wireless communications devices and services to the level of sensitivity of the information.

b. Use electronic, auto-manual, or manual crypto-systems to provide the needed security for existing radio systems that do not have embedded or electronic crypto-systems. However, all future procurements must comply with paragraph 6–1, above.

c. Prohibit the use of commercial non-encrypted radio systems in support of command and control functions.

d. Radios used for public safety communications with civil agencies or to communicate on civil aviation channels are excluded from the requirements of paragraphs *a* and *b*, above. This exclusion does not apply to communications dealing with aviation combat operations.

6–5. Telecommunication devices

a. **All personnel are prohibited from using Government-owned receiving, transmitting, recording, and amplification telecommunications equipment in restricted areas; such as classified work areas, mission essential vulnerable areas (MEVAs), or staging areas before deployment unless authorized in writing by the commander.** The DAA remains the accreditation authority for telecommunication devices in restricted areas.

b. All personnel will use NSA or CIO/G–6 approved secure telephones to discuss classified information telephonically.

c. **All personnel are prohibited from possessing or using any privately owned PED (for example, cell phones, TWED) within the confines of classified, restricted, or open storage areas designated by the commander.**

Chapter 7
Risk Management

7–1. Risk management process

a. Absolute confidence in the information accessed or available in the Army enterprise is unachievable; as such, the Army and DOD will approach increasing that level of trust through the implementation of a risk management process. With technological advances and capabilities, training, and IA-focused processes to reduce identifiable threats, the level of trust of information and ISs is significantly increased. Establish a risk management process containing the following phases as a minimum for all ISs. The process outlined in this chapter is based, in principle, on the risk management doctrine as defined by FM 5–19—

(1) Identify threats such as those posed by default designs or configurations, architecture deficiencies, insider access, and foreign or nation-state interests, ownership and capabilities.

(2) Assess threats to determine risks.

(a) What information is accessible?

(b) What information will be stored electronically and secured, for example self generated, prototype, research and development, electronic forms and documents, calendars, operational logs?

(c) What will be the stored format of the information and the naming or identification mechanism?

(d) Who has authorization to access and share the information?

(e) What is the potential adverse effect of loss, access, or manipulation of the data?

(f) What are the OPSEC issues of data availability?

(g) What are the data owner's requirements and length of required storage or access?

(h) What legacy operating systems or applications are required for stored information? What hardware is required to access and read the storage media?

(i) What are the backup and disaster recovery plans?

(j) What is the plan to migrate legacy data to current application capabilities?

(3) Develop controls and make risk management decisions. How do you protect the information access, and infrastructure?

(4) Implement controls, countermeasures, or solutions. Choose the correct IA tools, controls and countermeasures to defend against adversarial attacks on IS and networks.

(5) Implement a capability to monitor for compliance and success.

(6) Supervise, evaluate, review, and refine as necessary.

b. Commanders, Directors, combat developers, and materiel developers will integrate the risk management process in the planning, coordination, and development of ISs.

c. Reevaluate and reissue any risk analyses and mitigations plans if there is a successful compromise of an IS or device.

d. Telecommunications systems that do not include the features normally associated with an IS and that handle classified or sensitive information will be implemented and operated in conformance with the risk management process.

7–2. Information operations condition

The IAPM or the command's senior IA person is responsible for coordinating an INFOCON plan. The INFOCON is a Commander's Alert System that establishes a uniform DOD and Army process for posturing and defending against malicious activity targeting DOD ISs and networks. The countermeasures at each level will be available when published or as directed by the combatant command when the command is an ACOM/ASCC. If there is a conflict between Army and combatant command directed measures, those of the combatant command take precedence. Typical countermeasures include preventative actions and actions taken during an attack as well as damage control and mitigation actions.

Appendix A
References

Section I
Required Publications

AR 25–1
Army Knowledge Management and Information Technology Management. (Cited in paras 1–5*g*(13), 2–1*s*, 2–8*l*, 3–3*j*, 3–3*l*, 4–5*a*, 4–20*c*, 4–20*g*, 4–29*a*, 4–30*b*.)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 4–5*a*(7), 4–5*s*(10)(h)3, 4–11*a*, 4–11*d*, 4–16*a*, 4–16*b*, 4–17*c*, 4–32.)

AR 380–53
Information Systems Security Monitoring. (Cited in paras 4–5*m*(6), 4–29*a*.)

DA Pam 25–1–1
Information Technology Support and Services. (Cited in para 4–5*i*.)

Section II
Related Publications
A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 5–12
Army Management of the Electromagnetic Spectrum

AR 15–6
Procedures for Investigating Officers and Boards of Officers

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 36–2
Audit Services in the Department of the Army

AR 70–1
Army Acquisition Policy

AR 190–45
Law Enforcement Reporting

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 195–2
Criminal Investigation Activities

AR 215–1
Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities

AR 340–21
The Army Privacy Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 380–49
Industrial Security Program

AR 380–67
The Department of the Army Personnel Security Program

AR 381–10
U.S. Army Intelligence Activities

AR 381–11
Intelligence Support to Capability Development

AR 381–14
Technical Counterintelligence (TCI)

AR 381–20
The Army Counterintelligence Program

AR 525–13
Antiterrorism

AR 530–1
Operations Security (OPSEC)

AR 608–1
Army Community Service Center

DA Pam 25–1–2
Information Technology Contingency Planning.

Chairman of the Joint Chiefs of Staff Instruction 5221.01B
Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations. (Available at http://www.dtic.mil/cjcs_directives/.)

Chairman of the Joint Chiefs of Staff Manual 6510.01
Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND). (Available at http://www.dtic.mil/cjcs_directives/.)

Common Criteria Evaluation and Validation Scheme (CCEVS)
(http://niap.bahialab.com/cc-scheme/)

Committee on National Security Systems (CNSS) Instruction 4012
Operation of the Defense Acquisition System. (Available at http://www.cnss.gov/instructions.html.)

DOD 5200.2–R
Personnel Security Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 5220.22–M
National Industrial Security Program Operating Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD 5220.22–M–SUP
National Industrial Security Program Operating Manual Supplement. (Available at http://www.dtic.mil/whs/directives.)

DOD 5400.7–R
DOD Freedom of Information Act Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 5500.7–R
Joint Ethics Regulation (JER). (Available at http://www.dtic.mil/whs/directives.)

DOD 8510.1–M
Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5000.1
The Defense Acquisition System. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5220.6
Defense Industrial Personnel Security Clearance Review Program. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5220.22
DOD Industrial Security Program. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5230.9
Clearance of DOD Information for Public Release. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 5230.25
Withholding of Unclassified Technical Data From Public Disclosure. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 8100.2
Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG). (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 8500.01E
Information Assurance. (Available at http://www.dtic.mil/whs/directives.)

DOD Directive 8570.01
Information Assurance (IA) Training, Certification, and Workforce Management. (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 3020.41
Contractor Personnel Authorized to Accompany the U.S. Armed Forces. (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 5000.2
Operation of the Defense Acquisition System. (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP). (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 8100.3
Department of Defense (DOD) Voice Networks. (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 8110.1
Multinational Information Sharing Networks Implementation. (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 8500.2
Information Assurance (IA) Implementation. (Available at http://www.dtic.mik/whs/directives.)

DOD Instruction 8551.1
Ports, Protocols, and Services (PPSM). (Available at http://www.dtic.mil/whs/directives.)

DOD Instruction 1015.10
Programs for Military Morale, Welfare, and Recreation. (Available at http://www.dtic.mil/whs/directives.)

Director, Central Intelligence Agency Directive 1/7
Security Controls on the Dissemination of Intelligence Information. (Available at http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm.)

Director, Central Intelligence Agency Directive 5/6
Intelligence Disclosure Policy. (Available at http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm.)

Defense Intelligence Agency Manual 50–4
Security of Compartmented Computer Operations. (Information may be obtained from the Defense Intelligence Agency, 200 MacDill Blvd, Bldg 6000, Bolling AFB, Washington, DC 20340.)

Director, Central Intelligence Agency Directive 6/3
Protecting Sensitive Compartmented Information within Information Systems. (Available at http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm.)

DOD Memo, July 06, 2006, Subject: Interim Department of Defense (DOD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance
(Available at https://diacap.iaportal.navy.mil.)

Executive Order 12356
National Security Information

Federal Information Security Management Act of 2002
Section 3541 of title 44, United States Code. (Available at http://csrc.nist.gov/policies/HR2458-final.pdf.)

Federal Information Processing Standards Publication 46–2
(http://www.itl.nist.gov/)

Federal Information Processing Standards Publication 140–2
Security Requirements for Cryptographic Modules. (Available at http://www.itl.nist.gov/.)

Field Manual 3–13
Information Operations: Doctrine, Tactics, Techniques, and Procedures

Field Manual 5–19 (100–14)
Composite Risk Management

Joint DODIIS
Cryptologic SCI Information Systems Security Standards. (Available at http://www.nmic.navy.smil.mil/onihome-s/security/sso_navy/policyNpubs/jdcsisss/jdcissi-r2.html.)

JP 1–02
Joint Publication, Department of Defense Dictionary of Military and Associated Terms

JTA–A
Joint Technical Architecture–Army. (Available via AKO at https://www.us.army.mil.)

NSA/CSS Manual 130–1
Operational Information Systems and Networks Security Policy

NSA/CSS Manual 130–2
Media Declassification and Destruction Manual

NIST Special Publication 800–64 REV.1
Security Considerations in the Information Systems Development Life Cycle (http://csrc.nist.gov/publications/nistpubs/800–64/NIST–SP800–64.pdf)

NSTISSI No. 4012
National Training Standard for Designated Approving Authority (DAA). (Available at http://www.cnss.gov/instructions.html.)

NSTISSI No. 4015
National Training Standard for System Certifiers. (Available at http://www.cnss.gov/instructions.html.)

NSTISSI No. 7003
Protective Distribution Systems. (Available at http://www.cnss.gov/instructions.html.)

NSTISSP No. 11
National Information Assurance Acquisition Policy. (Available at http://www.cnss.gov/instructions.html.)

Office of Management and Budget Circular A–130
Management of Federal Information Resources

Public Law 100–235
Computer Security Act of 1987

Public Law 107–314
Bob Stump National Defense Authorization Act for Fiscal Year 2003

Rule for Courts–Martial 303
Preliminary inquiry

UCMJ
Uniform Code of Military Justice

5 USC 552a
The Privacy Act of 1974

22 USC 2551
Congressional statement of purpose

22 USC 2751, et. seq.
Arms Export Control Act

44 USC 3541
Information security; Purposes

RCS CSIM–62
MDEP M54X Report

Section III
Prescribed Forms
This entry has no prescribed forms.

Section IV
Referenced Forms
DA Forms are available on the Army Publishing Directorate Web site (www.apd.army.mil): DD Forms are available from the OSD Web site (http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm). SFs and OFs are available from the GSA Web site (http://www.gsa.gov).

DA Form 11–2–R
Management Control Evaluation Certification Statement

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 254
DOD Contract Security Classification Specification

SF 85P
Questionaire For Public Trust Positions

SF 86
Questionaire For National Security Positions

SF 328
Certificate Pertaining to Foreign Interests

Appendix B
Sample Acceptable Use Policy

B–1. Purpose
This appendix provides a sample AUP that may be used by organizations to obtain explicit acknowledgements from individuals on their responsibilities and limitations in using ISs.

B–2. Explanation of conventions in sample acceptable use policy
Figure B–1, below, illustrates a representative AUP. In this figure, text appearing in italicized font should be replaced with the appropriate information pertinent to the specific AUP being executed. Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate.

Acceptable Use Policy

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in *classified network name (CNN)* and/or *unclassified network name (UNN)* from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. Access. Access to *this/these* network(s) is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. *CNN* is the primary classified IS for (*insert your organization*). *CNN* is a US-only system and approved to process *(insert classification)* collateral information as well as: *(insert additional caveats or handling instructions)*. *CNN* is not authorized to process (*insert classification or additional caveats or special handling instructions*).

a. *CNN* provides communication to *external DoD (or specify other appropriate U.S. Government)* organizations using the *SIPRNET*. Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate)*.

b. The *CNN* is authorized for *SECRET* or lower-level processing in accordance with *accreditation package number, identification, etc.*

c. The classification boundary between *CNN* and *UNN* requires vigilance and attention by all users. *CNN* is also *a US-only system* and not accredited for transmission of *NATO* material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of *TOP SECRET* information through the *CNN* is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. Unclassified Information Processing. *UNN* is the primary unclassified automated administration tool for the (*insert your organization*). *UNN* is a US-only system.

a. *UNN* provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate)*.

b. *UNN* is approved to process *UNCLASSIFIED, SENSITIVE* information in accordance with *(insert local regulation dealing with automated information system security management program)*.

c. The *UNN* and the Internet, as viewed by the (*insert your organization*), are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

Figure B–1. Acceptable use policy

6. Minimum security rules and requirements. As a *CNN* and/or *UNN* system user, the following minimum security rules and requirements apply:

a. Personnel are not permitted access to *CNN* and *UNN* unless in complete compliance with the (insert your organization) personnel security requirement for operating in a TOP SECRET system-high environment.

b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized IS classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the *(insert your organization)* SA and/or IASO and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to *(insert your organization)* SA and/or IASO.

Figure B–1. Acceptable use policy—Continued

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of *(CNN) (UNN)* will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

(insert specific criteria)

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper email use and restrictions (e.g., mass mailing, hoaxes, autoforwarding)
- to explain expected results of policy violations (1st, 2nd, 3rd, etc)

(Note: Activity in any criteria can lead to criminal offenses.)

q. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to (*insert your organization*) information systems.

7. Acknowledgement. I have read the above requirements regarding use of (*insert your organization*) access systems. I understand my responsibilities regarding these systems and the information contained in them.

insert name here Directorate/Division/Branch	*insert date here* Date
insert name here Last Name, First, MI	*insert Rank/Grade and SSN here* Rank/Grade/ SSN
insert name here Signature	*insert phone number here* Phone Number

Figure B–1. Acceptable use policy—Continued

Appendix C
Management Control Evaluation Checklist

C–1. Function
The function covered by this checklist is the administration of the Army Information Assurance Program.

C–2. Purpose
The purpose of this checklist is to assist assessable unit manager and management control administrators in evaluating the key management controls outlined below. It is not intended to cover all controls.

C–3. Instructions
Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, or others). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement). DA Form 11–2–R is available on the APD Web site (http://www.apd.army.mil).

C–4. Test questions
a. Have appropriate security personnel (for example, IAPMs, IAMs, or IASOs) been appointed?

b. Have risk analyses and vulnerability assessments 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 vulnerability assessments?

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

e. Have countermeasures been identified based on the results of risk analyses and vulnerability assessments?

f. Are countermeasures in place commensurate with risks and vulnerabilities?

g. Is there a written security plan to document implementation of countermeasures?

h. Has leadership and management formally accepted the risk to process the information involved (or more precisely stated: "Are the systems accredited?"

i. Are countermeasures routinely tested (for example, user IDs, passwords, audit trails)?

j. Are Command and subordinate organizations implementing and reporting compliance to USSTRATCOM, JTF–GNO, DOD and Army directed solutions or actions such as Command Tasking Orders (CTOs), IAVM, or INFOCON measures?

k. Is Information Assurance training being performed?

l. Are ACOM, ASCC, DRU, installations, or activities identifying their IA requirements under the appropriate MDEP?

m. Are security incidents and violations (for example, viruses, unauthorized access, or attempts) reported?

n. Have plans been developed to ensure continued operation in the event of major disruption (for example, fire, natural disaster, bomb threat, or civil disorder)?

o. Has a configuration control board approved each network?

p. Is there an appropriate security official as a member of each board?

q. Is there a current SSAA on file for each IS?

C–5. Supersession
This checklist replaces the checklist previously published in AR 25–2, dated 14 November 2003.

C–6. Comments
Help to make this a better tool for evaluating management controls. Submit comments to: Chief Information Officer/G–6 (CIO/G–6), 107 Army Pentagon, Washington, DC 20310–0107.

Glossary

Section I
Abbreviations

A&VTR
Asset and Vulnerability Tracking Resource

AASA
Administrative Assistant to the Secretary of the Army

ACA
Agent of the Army Certification Authority (C&A)

ACERT
Army Computer Emergency Response Team

ACL
access control list

ADP (replaced by IT)
automated data processing

AEI
Army Enterprise Infostructure

AES
Advanced Encryption Standard

A–GNOSC
Army - Global Network Operations and Security Center

AIAP
Army Information Assurance Program (replacement for AISSP, Army Information Systems Security Program)

AISSP
Army Information Systems Security Program (replaced by AIAP)

AKO
Army Knowledge Online

AMC
Army Materiel Command

AR
Army Regulation

ARL
Army Research Laboratory

ARNET
Army Reserve Network

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

ASC
Army Signal Command

ATD
Authorization Termination Date

ATS
Automated Tactical System

ATO
approval to operate

AUP
Acceptable Use Policy

AV
Anti Virus

AWRAC
Army Web Risk Assessment Cell

AWS
Automated Weapons System

BBP
Best Business Practices

C4IM
Command, Control, Communications, and Computers for Information Management

CA
Certification Authority

C&A
certification and accreditation

CAR
Certification Authority Representative

CCB
Configuration Control Board

CCI
controlled cryptographic item

CCIU
Computer Crime Investigative Unit

CI
counterintelligence

CID
Criminal Investigation Command

CISS
Center for Information Systems Security

CIT
common information technology

CMB
Configuration Management Board

CND
computer network defense

CNDSP
Computer Network Defense Service Provider

CNO
computer network operations

CNSS
Committee on National Security Systems

COCO
contractor owned, contractor operated

CON
Certificate of Networthiness

CONUS
Continental United States

COR
contracting officer's representative

COS
Chief of Staff

COTS
commercial off-the-shelf

COOP
Continuity of Operations Plan

CPP
Cooperative Program Personnel

CRD
compliance reporting database

CSLA
Communications Security Logistics Agency

CT1S
Common Tier 1 System

CT&E
certification, test and evaluation

CVT
Compliance Verification Team

DAA
designated approving authority

DAPE
Deny all, permit by exception

DATO
Denial of Authorization to Operate

DCE
distributed computing environment

DDL
Delegation of Disclosure Authority Letter

DES
data encryption standard

DIACAP
Department of Defense Information Assurance Certification and Accreditation Process

DiD
Defense in Depth

DISA/CISS
Defense Information Systems Agency/Center for Information System Security

DITYVAP
Do-it-Yourself Vulnerability Assessment Program

DMZ
demilitarized zone

DNS
Domain Name Service

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DOIM
Director of Information Management

DRU
direct reporting unit

EIO&M
engineering, implementation, operation, and maintenance

EKMS
Electronic Key Management System

EOIS
Employee Owned Information System

ESEP
Engineer and Scientist Exchange Program

FISMA
Federal Information Security Management Act

FLO
foreign liaison officer

FN
foreign national

FOCI
Foreign ownership, control, or influence

FOT&E
follow-on test and evaluation

FPAT
Force Protection Assessment Team

I&A
identification and authentication

IA
Information Assurance

IAD
Information Assurance Directorate

IAM
Information Assurance Manager

IANM
Information Assurance Network Manager

IANO
Information Assurance Network Officer

IAPM
Information Assurance Program Manager

IASO
Information Assurance Security Officer

IATC
interim authority to connect

IATO
interim approval to operate

IATT
Information Assurance Technical Tip

IATT
Interim Authorization to Test (C&A)

IAVA
Information Assurance Vulnerability Alert

IAVB
Information Assurance Vulnerability Bulletin

IAVM
Information Assurance Vulnerability Management

ICAN
Installation Campus Area Network (installation backbone)

IDS
Intrusion Detection System

IMA
Installation Management Agency

IO
information operations

IOT&E
initial operational test and evaluation

IOVAD
Information Operations Vulnerability Assessments Division

IP
Internet Protocol

IS
information system

ISS
Information Systems Security (replaced by Information Assurance)

IT
information technology

ITS
information technology services

JIM
Joint Interagency and Multinational

JDCSISSS
Joint DODIIS Cryptologic SCI Information Systems Security Standards

JKMIWG
Joint Key Management Infrastructure Working Group

KMEC
Key Management Executive Committee

KMI
key management infrastructure

KVM/KMM
keyboard, video, mouse/keyboard, monitor, mouse

LCERT
Local Computer Emergency Response Team

LOC
level of confidentiality

MAC
mission assurance category

MAP
Mitigation Action Plan

MCEB
Military Communications Electronics Board

MDEP
management decision package

MDID
market driven/industry developed

MEVA
mission essential vulnerable area

MOA
Memorandum of Agreement

MPE
miscellaneous processing equipment

MPEP
Military Personnel Exchange Program

MSC
major subordinate command

MWR
morale, welfare, and recreation

NA
network administrator

NAC
National Agency Check

NACIC
National Agency Check with Credit Check and written inquiries

NACLC
National Agency Check with Local Agency and Credit Checks

NCR
National Capital Region

NDI
non-developmental item

NETCOM
Network Enterprise Technology Command

NETOPS
network operations

NGB
National Guard Bureau

NIAP
National Information Assurance Partnership

NIST
National Institute of Standards and Technology

NSA
National Security Agency

NSI
National Security Information

NSS
National Security System

OCA
original classification authority

OPM
Office of Personnel Management

PDA
personal digital assistant

PDS
Protected Distribution System

PED
personal electronic device or portable electronic device

PEG
program evaluation group

PEO
program executive officer

PIN
personal identification number

PL
public law or protection level

PM
program manager or project manager or product manager

POA&M
Plan of Action and Milestones

POLP
principle of least privilege

PPS
ports, protocols, and services

RA
remote access

RADIUS
Remote Authentication Dial-in User System

RAS
remote access server

RCERT
Regional Computer Emergency Response Team

RCIO
regional chief information officer

RDT&E
research, development, test, and evaluation

ROM
read only memory

SA
Systems Administrator

SABI
secret and below interoperability

SBU
Sensitive but Unclassified (obsolete term)

SCI
sensitive compartmented information

SIAO
Senior Information Assurance Officer

SII
Statement of Intelligence Interest or Security/Suitability Investigations Index

SIO
senior intelligence officer

SIOP–ESI
Single Integrated Operational Plan-Extremely Sensitive Information

SIR
serious incident report

SFTP
Secure File Transfer Protocol

SISS
Subcommittee for Information Systems Security

SOP
standard operating procedure

SSAA
System Security Authorization Agreement

SSBI
single-scope background investigation

SSH
secure shell

SSL
secure sockets layer

SSN
social security number

SSP
System Security Policy

STANREP
standardization representative

STEP
standard tactical entry point

STIG
Security Technical Implementation Guide

STS
Subcommittee for Telecommunications Security

SO
System Owner

TA
technical advisory

TAG
technical advisory group

TEMP
Test and Evaluation Master Plan

TLA
Top Layer Architecture

TNOSC
Theater Network Operations and Security Center

TS
Top Secret

TSACS
Terminal Server Access Control System

TSMB
Tier 1 System Management Board

TS/SCI
Top Secret/Sensitive Compartmented Information

TTP
tactics, techniques, and procedures

URL
universal resource locator

USAAA
United States Army Audit Agency

USERID
user identification

VAT
vulnerability assessment technician

VIS
vendor integrity statement

VPN
virtual private network

WLAN
wireless local area network

WWW
World Wide Web

Section II
Terms

Access
(IS) Ability and means to communicate with (that is, provide input to or receive output from), or otherwise make use of any information, resource, or component in an IS. (COMSEC) Capability and opportunity to gain knowledge or to alter information or materiel.

Access control
The process of limiting access to the resources of an IS only to authorized users, programs, processes, or other systems.

Accountability
(IS) Property that enables auditing of activities on an IS to be traced to persons who may then be held responsible for their actions. (COMSEC) Principle that an individual is responsible for safeguarding and controlling of COMSEC equipment, keying materiel, and information entrusted to his or her care and is answerable to proper authority for the loss or misuse of that equipment or information.

Accreditation Decision
An official designation from a DAA, in writing or digitally signed e-mail, made visible to the CIO/G–6, regarding acceptance of the risk associated with operating an IS. Expressed as ATO, IATO, IATT, or DATO.

Adjunct Network
For the purpose of C&A, those networks that depend on the connections to the common transport network and services of the ICAN. These networks rely on the ICAN for NIPRNET and SIPRNET connectivity. These may or may not be under DOIM management and usually connect to the ICAN below the security stack. They may be controlled by a tenant as small as an office or as large as a ACOM/ASCC headquarters.

Approval to operate
Synonymous with accreditation.

Army information
Information originated by or concerning the Army.

Audit
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit trail
Chronological record of system activities to enable the construction and examination of the sequence of events or changes in an event (or both). An audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC materiel.

Authenticate
To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or to establish the validity of a transmitted message.

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity or eligibility to receive specific categories of information or perform specific actions.

Authorization to operate
Authorization granted by the DAA for an information system to process, store, or transmit information. Authorization is based on acceptability of the solution, the system architecture, implementation of assigned IA Controls, the operational IA risk level, and the mission need.

Auto-manual system
Programmable, hand-held COMSEC equipment used to perform encoding and decoding functions.

Automated information system (obsolete term)
(See information system (IS))

Automated Information System Application
For IA purposes, the product or deliverable resulting from an acquisition program. An Automated Information System (AIS) application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (for example, integrated consumable items support); multiple software applications that are related to a single mission (for example, payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (for example, Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and often have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in OMB A–130; however, this term is not used in order to avoid confusion with the DOD acquisition category of major AIS.

Automated Tactical System
Any IS that is used for communications, operations, or as a weapon during mobilization, deployment, or a tactical exercise. An Automated Tactical System (ATS) may include, but is not limited to, data processors, firmware, hardware, peripherals, software or other interconnected components and devices (for example, radar equipment, global positioning devices, sensors, guidance systems for airborne platforms).

Automated weapon systems
Any weapons system that utilizes a combination of computer hardware and software to perform the functions of an information system (such as collecting, processing, transmitting, and displaying information) in its operation.

Availability
The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Category
Restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data. Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization.

Central computer facility
One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. Central computer facilities are those areas where computer(s) (other than personal computer(s)) are housed to provide necessary environmental, physical, or other controls.

Certification
Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification and accreditation
The standard DOD approach for identifying information security requirements, providing security solutions, and managing the security of DOD information systems.

Certification authority
Government civilian or military official with the authority and responsibility for formal evaluation of the IA capabilities and services of an information system and risks associated with operation of the information system. The Army CA is the Army FISMA SIAO, the Director OIA&C, NETC–EST–I.

Certification support
Those activities associated with coordination of certification events such as preparation for certification test activities, conduct of the certification event(s), preparation of the Certification Report, preparation of the certification scorecard, and preparation of the ISs risk assessment. Certification support does not include those functions that are the responsibility of the system owner (for example, Information System Security Engineering, primary SSAA development, SSAA consolidation prior to submission for approval, or POA&M development).

Certification event
An evaluation of an information system to determine compliance with IA Controls. This may be in support of an IATO, IATT, ATO, or DATO.

Classified defense information
Official information regarding national security that has been designated top secret, secret, or confidential in accordance with Executive Order 12958, as amended by Executive Orders 12972, 13142, and 13292.

Clearing
Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity in such a way that the data may not be reconstructed using normal system capabilities (for example, through the keyboard). An IS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused within the same environment at the same classification and confidentiality level. It does not produce a declassified product by itself, but may be the first step in the declassification process (see Purge).

Commercial Communications Security Endorsement Program
Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (that is, standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Compartmented mode
IS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: (1) Valid security clearance for the most restricted information processed in the system; (2) Formal access approval and signed non-disclosure agreements for that information to which a user is to have access; and (3) Valid need-to-know for information to which a user is to have access.

Compromising emanations
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment (see TEMPEST).

Computer
A machine capable of accepting data, performing calculations on, or otherwise manipulating that data, storing it, and producing new data.

Computer facility
Physical resources that include structures or parts of structures that support or house computer resources. The physical area where the equipment is located.

Computer security
Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes.

Configuration control
Process of controlling modifications to a telecommunication or information system hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Configuration management
The management of security features and assurances through control of changes made to hardware, software, firmware,

documentation, test, test fixtures, and test documentation of an IS throughout the development and operational life of the system.

Contingency plan
A plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Controlled access protection
Log-in procedures, audit of security-relevant events, and resource isolation as prescribed for class C2 in DOD 5200. 28–STD.

Controlled cryptographic item
Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked CONTROLLED CRYPTOGRAPHIC ITEM or, where space is limited, controlled cryptographic item.

Countermeasure
An action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Cryptographic
Pertaining to, or concerned with, cryptography.

Cryptographic equipment
Equipment that embodies a cryptographic logic.

Cryptography
Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Data security
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Declassification (of magnetic storage media)
An administrative procedure resulting in a determination that classified information formerly stored on a magnetic medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment.

Defense in Depth
The DiD encompasses a physical and logical structure that requires a layering of security policies, procedures, and technology mechanisms to protect network resources, from the desktop to the enterprise, within and across the enterprise architecture. Layered defenses include, but are not limited to, the installation of IA policy protections complementing the use of proxy services, firewalls, IDSs, implementation of DMZs, redundant filtering policies across devices, and access control and accountability.

Degauss
Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Demilitarized zone
A small network or computer host that serves as a "neutral zone" between an internal network and the public network. A DMZ prevents users from obtaining direct access to an internal server that may have business data on it. A DMZ is another approach to the use of a firewall and can act as a proxy server if desired.

Denial of service
Result of any action or series of actions that prevents any part of a telecommunications or IS from functioning.

Designated approving authority
A general officer (GO), SES or equivalent official appointed by the Army CIO/G–6 with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Authorization Authority and Delegated Accrediting Authority.

DATO
DAA determination that an information system cannot operate because of an inadequate IA design or failure to implement assigned IA controls. If the system is already in use, operation of the system is halted.

Digital signature
An electronic rather than a written signature used by someone to authenticate the identity of a sender of a message or signer of a document. A digital signature ensures that the content of a message or document is unaltered. Digital signatures can be time-stamped, cannot be imitated by another person, cannot be easily repudiated, and are transportable.

Discretionary access control (DAC)
Means of restricting access to objects based on the identity and need-to-know of users or groups to which the object belongs. Controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

Eavesdropping
Method used by an unauthorized individual to obtain sensitive information (for example, passwords, data) from a network. Eavesdropping techniques include wiretapping, eavesdropping by radio, eavesdropping via auxiliary ports on a terminal, and use of software that monitors packets sent over a network. Vulnerable network programs are telnet and ftp.

Embedded cryptography
Cryptography that is engineered into a piece of equipment or system the basic function of which is not cryptographic. Components comprising the cryptographic module are inside the equipment or system and share host-device power and housing. The cryptographic function may be dispersed if identifiable as a separate module within the host.

Embedded (computer) system
Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part.

Emission security
Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment, ISs, and telecommunications systems.

Enclave
The collection of computing environments connected by one or more internal networks, under the control of a single authority and security policy that includes personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Extranet
A private network that uses Internet protocols and the public telecommunications system to securely share information among selected external users. An Extranet requires the use of firewalls, authentication, encryption, and VPNs that tunnel through the public network.

File server
Computer hardware used to provide storage for user data and software applications, processing capabilities for user workstations, and (normally) connection and control of workstations to a LAN.

Firewall
A system or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration.

Firmware
Software that is permanently stored in a hardware device that allows reading and executing the software, but not writing or modifying it.

Fly Away C&A package (tactical deployed)
Tactical C&A package that supports tactical IS deployment and contains the minimum amount of C&A information necessary for secure operations and allow connection to a network in their deployed location.

Foreign exchange personnel
Military members or civilian officials of a foreign defense establishment (that is, a DOD equivalent) who are assigned to a DOD component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DOD component.

Foreign liaison officers
A foreign government military or civilian employee who is authorized by his or her government, and is certified by the DOD Component, to act as an official representative of that government in its dealing with the DOD component in connection with programs, projects, or agreements of interest to the governments. Three types of foreign liaison officers include security cooperation, operational, and national representatives.

Foreign national
Non-U.S. citizens who normally reside in the country where employed, though they may not be citizens of that country, and who are employed by the Government or the DA to perform services or duties and are not considered a foreign official or representative of that nation.

Foreign official
Non-U.S. citizens who may or may not reside in the country where employed, who are employed by their respective nation as an official representative of that nation in their official capacity, and assigned to the Government or DA organizations or commands in the role of liaison, representative, engineer, scientist, or a member of the Military Personnel Exchange Program.

Formal access approval
Documented approval by a data owner to allow access to a particular category of information.

Foreign ownership, control, or influence
A company is considered to be under foreign ownership, control, or influence whenever a foreign interest has the direct or indirect power either through the ownership of the company's securities, contractual arrangements, or other means; to direct or decide matters affecting the operations of that company. This influence may result in unauthorized access to classified or sensitive information, information systems, or information systems architectures.

Information assurance product
Product or technology whose primary purpose is to provide security services (for example, confidentiality, authentication, integrity, access control, or non-repudiation of data); correct known vulnerabilities; or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

Information assurance-enabled product
Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

IAA view
See interconnected accredited IS view.

Information owner
Government, civilian or military official with statutory or operational authority for specified information, and responsibility for establishing the controls for its generation, collection, processing, dissemination and disposal. Information owners will ensure that the DA information entrusted to their care is store, processed, or transmitted only on information systems that have obtained IA approval to operate in accordance with Army processes for the confidentiality level of their information. This applies to all systems, to include services on COCO systems as well as GOCO systems.

Interconnected accredited information system view
If a network consists of previously accredited ISs, a MOA is required between the DAA of each DOD component IS and the DAA responsible for the network. The network DAA must ensure that interface restrictions and limitations are observed for connections between DOD Component ISs. In particular, connections between accredited ISs must be consistent with the mode of operation of each IS as well as the specific sensitivity level or range of sensitivity levels for each IS. If a component that requires an external connection to perform a useful function is accredited, it must comply with any additional interface constraints associated with the particular interface device used for the connection as well as any other restrictions required by the MOA.

Information system
Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

Information assurance
The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities. This regulation designates IA as the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST).

Information Assurance Vulnerability Management (IAVM)
IAVM is the DOD program to identify and resolve identified vulnerabilities in operating systems. It requires the completion of four distinct phases to ensure compliance.

Information dissemination management
Activities to support the management of information and data confidentiality, integrity, and availability, including document management, records management, official mail, and work-flow management.

Information technology (IT)
The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Integrity
The degree of protection for data from intentional or unintentional alteration or misuse.

Intelligence information
Information collected and maintained in support of a U.S. intelligence mission.

Interim authority to operate
Temporary authorization granted by the DAA to operate an information system under the conditions or constraints enumerated in the Accreditation Decision.

Interim authority to test (certification and accreditation)
Temporary authorization granted by the DAA to test an information system in a specified operational information environment (usually a live information environment or with live data) within the timeframe and under the conditions or constraints enumerated in the Accreditation Decision.

Incident
Assessed occurrence having actual or potentially adverse effects on an information system.

Internet
A global collaboration of data networks that are connected to each other, using common protocols (for example, TCP/IP) to provide instant access to an almost indescribable wealth of information from computers around the world.

Intranet
Similar to the Internet, but is accessible only by the organization's employees or others with authorization. Usually internal to a specific organization.

Installation Campus Area Network
The common transport network provided by the responsible DOIM on every Army post/camp/station and the associated common network services, including network management and IA services. The ICAN is often commonly referred to as the backbone network.

Information system security incident (security incident)
Any unexplained event that could result in the loss, corruption, or denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of the system. Also, an occurrence involving classified or sensitive information being processed by an IS where there may be: a deviation from the requirements of the governing security regulations; a suspected or confirmed compromise or unauthorized disclosure of the information; questionable data or information integrity (for example, unauthorized modification); unauthorized modification of data; or unavailable information for a period of time. An attempt to exploit any IS such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code. (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.) (NSTISSD 503)

Information system serious incident
Any event that poses grave danger to the Army's ability to conduct established information operations.

Key
Information (usually a sequence of random or pseudo-random binary digits) used initially to set up and periodically to change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-measures patterns (for example, frequency hopping or spread spectrum), or for producing another key.

Key management
Process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed.

Least privilege
Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. This also applies to system privileges that might not be needed to perform their assigned job. NOTE: Application of this principle limits the damage that can result from errors, and accidental and unauthorized use of an IS.

Limited privileged access
Privileged access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

Local area network
A system that allows microcomputers to share information and resources within a limited (local) area.

Machine cryptosystem
Cryptosystem in which the cryptographic processes are performed by crypto-equipment.

Mainframe
A computer system that is characterized by dedicated operators (beyond the system users); high capacity, distinct storage devices; special environmental considerations; and an identifiable computer room or complex.

Malicious code
Software or firmware capable of performing an unauthorized function on an IS.

Malicious software code
Any software code intentionally created or introduced into a computer system for the distinct purpose of causing harm or loss to the computer system, its data, or other resources. Many users equate malicious code with computer viruses, which can lie dormant for long periods of time until the computer system executes the trigger that invokes the virus to

execute. Within the last several years, the Internet has been the conduit of various types of computer viruses. However, there are other types of malicious codes used to cause havoc that are not as well publicized as the virus.

Mission assurance category
Reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity.

Manual cryptosystem
Cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or auto-manual devices.

Military information environment
The environment contained within the global information environment, consisting of information systems and organizations-friendly and adversary, military and non-military-that support, enable, or significantly influence a specific military operation.

Monitoring
Monitoring is the observation of a resource for the purpose of ascertaining its status or operational state. Monitoring includes the automated, real or near-real time interception of information transiting the system or network by a system or network administrator during the normal course of employment while engaged in activities necessary to keep the system or network operational and to protect the rights and property of the system or network owner. For example, automated monitoring or logging of system or network events (such as by IDS, IPS, firewalls, and so on) can provide valuable information related to malicious content of communications; unauthorized access, exceeding access or misuse of systems or networks; policy and criminal violations, etc. as well as the performance of the systems. Because most electronic communications do not involves "parties to the conversation," monitoring by system and network administrators is not "electronic surveillance" as defined in AR 381–10.

Multilevel (security) mode
IS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

a. Some users do not have a valid security clearance for all the information processed in the IS.

b. All users have the proper security clearance and appropriate formal access approval for that information to which they have access.

c. All users have a valid need-to-know only for information to which they have access.

Multilevel security
Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

National Security System (44 USC 3542)
Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency – (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Need-to-know
Approved access to, or knowledge or possession of, specific information required to carry out official duties.

Net-centricity
A robust globally connected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles.

Network
Communications medium and all components attached to that medium whose function is the transfer of information. Components may include ISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Network management
Activities to support the management and support of the network, including the engineering of changes to the network, maintenance of the network and its components, and user support activities.

Network operations
The organizations and procedures required to monitor, manage, and control the global information grid. Network operations incorporate network management, IA, and information dissemination management.

Network security
Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.

Networthiness
The networthiness program manages the specific risks associated with the fielding of ISs and supporting efforts, requires formal certification throughout the life cycle of all ISs that use the infostructure, and sustains the health of the Army enterprise infostructure.

Networthiness certification
The Army's networthiness certification process incorporates and demonstrates the completeness of guidance, formats, and practices such as the Army knowledge enterprise; the Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP); the DIACAP; and existing developmental and operational test requirements.

Non-communications emitter
Any device that radiates electromagnetic energy for purposes other than communicating (for example, radar, navigational aids, and laser range finders). A non-communication emitter may include features normally associated with computers, in which case it must also meet the requirements for an IS.

Non-privileged access
User-level access; normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls and rules to be changed or bypassed by a typical user.

Operations Security
For the DOD components, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to:

a. Identify those actions that may be observed by adversary intelligence systems.

b. Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Outsourced IT-based Process
For DOD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Password
Protected or private character string used to authenticate an identity or to authorize access to data.

Personal computer
See information system.

Personal digital assistant
A hand-held computer that allows an individual to store, access, and organize information. Most PDAs work on either a Windows-based or a Palm operating system. PDAs can be screen-based or keyboard-based, or both.

Personal electronic devices
A generic title used to describe myriad available small electronic portable devices that employ the wireless application protocol and other "open standards".

Personal e-mail account
An e-mail account acquired by an individual for personal use. Also know as a private account.

Platform information technology interconnection
For DOD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

Principle of least privilege
The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a system or domain with those privileges and nothing more.

Private account
See personal e-mail account.

Privileged access
Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access:

a. "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth.

b. Access to change control parameters (for example, routing tables, path priorities, addresses) of routers, multiplexers, and other key information system or network equipment or software.

c. Ability and authority to control and change program files, and other users' access to data.

d. Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed.

e. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operations.

Protected Distribution System
Wire-line or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Proxy server
A server acting on behalf of another server or servers. Such an arrangement allows a single point of entry or exit into a TCP/IP network. A proxy server may also have built-in software that will allow it to be configured to act as a firewall, cache server, or logging server.

Purge
Removal of data from an IS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. An IS must be disconnected from any external network before a purge (see Clearing).

RADIUS
Remote Authentication Dial-In User Service is a protocol by which users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, dial-back, serial line Internet protocol (SLIP), and point-to-point protocol (PPP).

Remote access server
A server that is dedicated to handling users that are not on a LAN, but need remote access to it. The remote access

server allows users to gain access to files and print services on the LAN from a remote location. For example, a user who dials into a network from home using an analog modem or an ISDN connection will dial into a remote access server. Once the user is authenticated he can access shared drives and printers as if he were physically connected to the office LAN.

Remote terminal
A terminal that is not in the immediate vicinity of the IS it accesses. This is usually associated with a mainframe environment and the use of a terminal. Terminals usually cannot operate in a stand-alone mode.

Risk
The probability that a particular threat will exploit a particular vulnerability of an information system or telecommunications system.

Risk assessment
Process of analyzing threats to and vulnerabilities of an information system, and determining potential adverse effects that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective countermeasures.

Security guard/filter
IS trusted subsystem that enforces security policy on the data that passes through it.

Security test and evaluation
Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of the system.

Sensitive but unclassified (obsolete term)
An obsolete term (in DOD) that has been replaced by sensitive information (see below).

Sensitive information
Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 USC 552a (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes information in routine DOD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

a. FOUO, in accordance with DOD 5400.7–R, is information that may be withheld from mandatory public disclosure under the FOIA.

b. Unclassified technical data is data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DOD 5230.25.

c. Department of State (DOS) sensitive but unclassified (SBU) is information originating from the DOS that has been determined to be SBU under appropriate DOS information security polices.

d. Foreign government information is information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DOD 5200.1–R.

e. Privacy data is personal and private information (for example, individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974.

Social engineering
Term used among crackers and security professionals for cracking techniques that rely on weaknesses in process rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a user or helpdesk who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

SPAM
Unsolicited e-mail received on or from a network, usually the Internet, in the form of bulk mail obtained from e-mail distribution lists or discussion group lists.

Stand-alone information system
An IS that is physically, electronically, and electrically isolated from all other IS.

Survivability
The ability of a computer communication system-based application to satisfy and to continue to satisfy certain critical requirements (for example, specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.

Susceptibility
Technical characteristics describing inherent limitations of a system that have potential for exploitation by the enemy.

System
The entire computer system, including input/output devices, the supervisor program or operating system, and other included software.

System administrator
A system administrator (SA), or sysadmin, is a privileged-level individual employed or authorized to maintain and operate a computer system or network. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information assurance policy and procedures. (CNSS Instruction No. 4009)

System audit
The process of auditing and spot checking to verify secure operation of a system and its support software. If irregularities are discovered, the audit process includes analysis and identification of the problem, performing corrective actions necessary to resolve the situation, tracking open items actively, and briefing management on identified security deficiencies.

System of systems
A total network made up of all the interconnected computer systems, communication systems, and network components within some logical boundary. (Replaced with the term enclave.)

System owner
The Government civilian or military person or organization responsible for introduction or operation of an IS used by or in support of the Army. The SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented and provided as an artifact to the accreditation package. If a contractor provides IA services to a system with the intent of meeting some or all of the SOs IA responsibilities, the IA responsibilities do not shift from the Government SO to the contractor. The Government SO remains responsible for ensuring that the IA services are provided. The Government SO may charge the IAM with authority to perform many of the SO IA duties, if appropriate; however, final responsibility will remain with the SO. The SO could be a product, program or project manager, a staff or command element that purchases or develops IT equipment and systems, a DOIM or anyone else who is responsible for an IS. The SO is responsible for ensuring that all IA requirements are identified and included in the design, acquisition, installation, operation, maintenance, upgrade or replacement of all DA IS in accordance with DODD 8500.1.

Terminal Access Controller Access System
A system developed by the Defense Data Network community to control access to its terminal access controllers.

Technical vulnerability
A hardware, firmware, communication, or software weakness that leaves a computer processing system open for potential exploitation or damage, either externally or internally, resulting in risk for the owner, user, or manager of the system.

Telecommunications
Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and information systems security
Protection afforded to telecommunications and information systems to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure authenticity. Note: Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security materiel and technical security information.

Telecommunications system
Any system that transmits, receives, or otherwise communicates information by electrical, electromagnetic, electro-mechanical, or electro-optical means. A telecommunications system may include features normally associated with computers, in which case it must also meet the requirements for an IS.

Telnet
A terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control Web servers.

Terminal
Any device that is used to access an IS, including "dumb" terminals (which only function to access an IS), as well as personal computers or other sophisticated ISs that may access other ISs as one of their functions.

Threat
Capabilities, intentions, and attack methods of adversaries to exploit, damage, or alter information or an information system. Also, any circumstance or event with the potential to cause harm to information or an information system. Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service (see CNSS Instruction No. 4009).

Threat agent
A means or method used to exploit a vulnerability in a system, operation, or facility.

Threat analyst
Designated member of the intelligence staff of the supported command of the DAA who will provide the interface on behalf of DA with the DOD Intelligence Community, the G2, NETCOM/9th SC (A), and the intelligence component of the 1st Information Operations Command (Land) to document foreign threats regarding computer network attack (CNA) and computer network exploitation (CNE) or other non-technical threats.

Time bomb and logic bomb
Malicious code that can be triggered by a specific event or recur at a given time. A logic bomb is triggered by an event instead of a specific time. One example of a logic bomb would be a set of programmed instructions to search a company's payroll files, checking for the presence of the programmer's name. Once the programmer ceases employment, the logic bomb is triggered to cause damage to data or software.

Trapdoor
A hidden software program (potentially embedded into the hardware or firmware) mechanism that causes system protection mechanisms to be bypassed. The code can be hidden in the logon sequence where users are asked to input their user IDs and then passwords. In normal circumstances, the input passwords are checked against stored values corresponding to the user ID; if the passwords are valid, logon proceeds. The trapdoor software would check for a specific user ID, and whenever that user ID is checked, it bypasses the password checking routine and authorizes immediate logon. Trapdoors are sometimes built into development systems by programmers to avoid the lengthy logon procedure.

Trivial file transfer protocol
A simple form of the File transfer protocol (FTP). TFTP uses the user datagram protocol (UDP), a connection-less protocol that, like TCP, runs on top of IP networks. It is used primarily for broadcasting messages over a network and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trojan horse
A non-replicating program that appears to be legitimate, but is designed to have destructive effects on data residing in the computer onto which the program was loaded. These programs can perform various malicious activities, such as deleting files, changing system settings, allowing unauthorized remote access, and running malicious programs resulting in destruction or manipulation of data. Trojan horses require user intervention to propagate and install such as opening an e-mail attachment.

User
Person or process accessing an IS by direct connections (for example, via terminals) or indirect connections.

User ID
Unique symbol or character string that is used by an IS to uniquely identify a specific user.

Virtual private network
A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Virus
A small program written to alter the way a computer operates without the permission or knowledge of the user. A virus is self replicating with a potentially malicious program segment that attaches or injects itself into an application program or other executable system component and leaves no external signs of its presence, and usually programmed to damage system programs, delete files, create a denial of service, or reformat the hard disk.

Vulnerability
Weakness in an information system, cryptographic system, or components of either (for example, system security procedures, hardware design, internal controls) that could be exploited.

Vulnerability assessment
Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Warning banner
A warning banner is verbiage that a user sees or is referred to at the point of access to a system which sets the right expectations for users regarding acceptable use of a computer system and its resources, data, and network access capabilities. These expectations include notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.

Wide area network
A WAN covers a wider geographic area than a LAN, is an integrated voice or data network, often uses common carrier lines for the interconnection of its LANs, and consists of nodes connected over point-to-point channels. Commercial examples are Internet and public data. Government examples are NIPRNET and SIPRNET.

World Wide Web
The universe of accessible information available on many computers spread through the world and attached to that gigantic computer network called the Internet. The Web encompasses a body of software, a set of protocols, and a set of defined conventions for accessing the information on the Web. The Web uses hypertext and multimedia techniques to make the Web easy for anyone to roam, browse, and contribute to. The Web makes publishing information (that is, making that information public) as easy as creating a "homepage" and posting it on a server somewhere in the Internet. Also called WEB or W3.

Worm
An independent program that replicates itself by copying from one system to another, usually over a network without the use of a host file. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources or even shutting a network down, but, in contrast to viruses, does not require the spreading of an infected host file. Usually the worm will release a document that already has the "worm" macro inside the document.

Section III
Special Abbreviations and Terms
This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 238

PIN:	081066–000
DATE:	10-25-07
TIME:	08:09:16
PAGES SET:	94

DATA FILE:	C:\Wincomp\r25-2.fil
DOCUMENT:	AR 25–2

SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION