

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

PROSECUTION MOTION
FOR JUDICIAL NOTICE

Enclosure 8

24 June 2013

Army Regulation 25-1

Information Management

Army Knowledge Management and Information Technology

**Headquarters
Department of the Army
Washington, DC
4 December 2008**

UNCLASSIFIED

Chapter 1

Introduction

1-1. Purpose

This regulation establishes policies and assigns responsibilities for the management of information resources and information technology (IT). It applies to IT contained in command and control (C2) systems, intelligence systems (except as noted), business systems, and (when identified) national security systems (NSS) developed or purchased by the Department of Army (DA). It implements the provisions of Sections 2223 and 3014, Title 10, United States Code (10 USC 2223 and 3014); 40 USC Subtitle III, Clinger-Cohen Act (CCA); 44 USC Chapters 35 and 36; DODD 8000.01; and other related Federal statutes and directives. It addresses the application of knowledge management (KM) concepts and systems across the Army, the management of information as an Army resource, technology supporting information requirements, and resources supporting IT. This regulation does not apply directly to information systems (ISs) acquired under the National Intelligence Program (NIP) and the Military Intelligence Program (MIP) or for operational support of intelligence and electronic warfare systems.

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. Responsibilities

See chapter 2 for responsibilities.

1-5. Recordkeeping requirements

This regulation requires the creation of records to document and support the business processes of the Army. Records created under the purview of this regulation, regardless of content or format, will be kept in accordance with the retention schedules found at <https://www.arims.army.mil>.

1-6. Managing information resources and information technology

a. The term information resources refers to all resources and activities employed in the acquisition, development, collection, processing, integration, transmission, dissemination, media replication, distribution, use, retention, storage, retrieval, maintenance, access, disposal, security, and management of information. Information resources include doctrine, policy, data, equipment, and software applications and related personnel, services, facilities, and organizations.

b. Information technology refers to any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, image, data, or information by the Federal Government. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

c. Information technology embedded in or integral to weapon systems, machines, medical instrumentation, servomechanisms, training devices, or test and evaluation (TE) systems, except for those systems with no external interface, are included in the provisions of this regulation. This regulation supports the precept that information is a strategic defense asset in peacetime and conflict and that the peacetime information infrastructure must support wartime requirements by providing information services for rapid deployment and sustainment of armed forces around the world.

d. The management of information resources and IT is applicable to all Army organizations.

e. Information used in decision-making and business processes is Army record material, whether stored electronically or as a hard copy, and is scheduled, maintained, and preserved in accordance with Army Regulation (AR) 25-400-2.

1-7. Information as a resource

a. Except where restricted for reasons of national security, privacy, sensitivity, or proprietary rights, personnel will manage information as a shared resource and make it available to all those authorized access to it to accomplish their mission and functions. The cost to the Army of collecting, processing, distributing, and storing information makes it impossible to view information as a free commodity. Army personnel must carefully plan requirements for information and supporting IT. Information technology and related investments will be evaluated in terms of direct support and compatibility with Army Enterprise solutions, mandates, and processes and their corresponding information requirements.

b. Information and the data from which information is derived are broadly categorized as public domain and nonpublic domain. Public domain data or information is Government-owned and is not personally identifiable,

classified, subject to a Freedom of Information Act (FOIA) or Privacy Act exemption, or otherwise considered to be sensitive. The Army will either make this information public in a routine manner or provide the information upon public request with or without charge. Public domain Army data may be made available to the public via the Army Home Page or other authorized Army public Web site. Nonpublic information is identified as one of the following: personally identifiable and subject to the Privacy Act; classified according to the National Security Act; subject to a FOIA exemption; or otherwise sensitive. Unclassified FOIA-exempt information or data is nonpublic and designated For Official Use Only (FOUO). Nonpublic information or data may be shared for official purposes within the DOD and other governmental agencies affiliated with DOD contracts or operations, subject to any stipulated access and release restrictions. Nonpublic Army data in this category may be made available to authorized individuals via the Army Knowledge Online (AKO)/Defense Knowledge Online (DKO) portal or other approved controlled-access (private) Web servers, as required. Requests for nonpublic data from private individuals/organizations should be coordinated with/referred to the local FOIA/Privacy Act official for determination of whether or not the data are releasable. Refer to AR 25-55 for further information on the Army FOIA Program and to AR 340-21 for further information on the Army Privacy Program.

c. Data files (both paper and electronic) containing attorney-client privileged information generated by Army attorneys must be protected in accordance with AR 27-26. Attorney-client information is concerned with a client represented by a military or civilian Army attorney or an attorney contracted to perform services for the Army. IT and other personnel providing support services to an Army attorney must support the requirement for attorney-client privileged information to remain confidential and may be required to complete a confidentiality and nondisclosure agreement.

d. The responsible functional proponents will maintain Army data and ensure that the data are readily accessible to whoever requires them. This practice promotes efficient use of resources by eliminating duplication, improving synchronization, and reducing software development costs. It provides system developers with standard Army data to use, relieving them from the requirement to create data for their particular application.

e. Information and related resources will be managed through centralized Chief Information Officer (CIO) management processes and policies. Only approved Army and DOD methods, approaches, models, tools, data, technologies, and information services will be used.

1-8. Army Knowledge Management

Army Knowledge Management (AKM) is the Army's strategy to transform itself into a net-centric, knowledge-based force and an integral part of the Army's transformation to achieve the Future Force. AKM will deliver improved information access and sharing while providing infrastructure capabilities across the Army so that warfighters and business stewards can act quickly and decisively. AKM connects people, knowledge, and technologies.

a. The goals of AKM are—

- (1) Adopt governance and cultural changes to become a knowledge-based organization.
- (2) Integrate KM and best business practices into Army processes to promote the knowledge-based force.
- (3) Manage the infrastructure as an enterprise to enhance efficiencies and capabilities such as collaborative work, decision-making, and innovation.
- (4) Institutionalize AKO/DKO as the enterprise portal to provide universal and secure access for the entire Army.
- (5) Harness human capital for the knowledge-based organization.

b. The result of the AKM strategy is to align Army enterprise knowledge and the information infrastructure with the Global Information Grid (GIG) and the Future Force. See also DA Pam 25-1-1, chapter 3.

c. Army organizations will develop communities of practice (CoPs) or communities of interest (COIs) as an integral part of the transformation to a net-centric, knowledge-based force.

(1) A CoP is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice.

(2) Communities of Practice are supported by collaborative environments such as structured professional forums and knowledge networks.

(3) A COI is a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes. See also paragraph 4-8 of this publication.

(4) All communications within CoPs and COIs are subject to applicable professional, ethical, and security guidelines, including those in this regulation, AR 25-2, and provisions of DOD 5500.7R, the Joint Ethics Regulation.

d. The use of AKO/DKO and Army Knowledge Online-Secret (AKO-S) permits maximum sharing of Army information and knowledge resources across the Army enterprise and reduces the need for investment in duplicative IT resources. Army activities requiring collaborative tools will use those provided on AKO/DKO or as otherwise prescribed by the DA. See also paragraph 6-2g of this publication for policy regarding collaboration tool suite standards.

e. AKO/DKO is the single Army portal for authenticating Army users to gain access to enterprise systems and portals. See also paragraph 6-7d of this publication.

b. All individuals must complete training and certification, as necessary, equal to their assigned duties. (For IA training course information see <https://ia.gordon.army.mil/courses.asp>.)

c. All personnel who require access to ISs processing classified defense information to fulfill their duties will possess a security clearance based on the appropriate personnel security investigation per DOD 5200.2R.

d. Foreign Nationals access and use of IT systems must adhere to the policies prescribed in AR 25-2, para 4-15.

5-8. Communications Security (COMSEC)

Commanders will take the appropriate measures to secure all communications with approved products and devices to the level of security classification of the information to be transmitted over such communications equipment. See also AR 380-40.

5-9. Risk management

Each commander will establish an effective risk management program. At a minimum, the program will include the four phases of risk management:

a. Risk analysis of resources, controls, vulnerabilities, and threats and the impact of losing the systems' capabilities on the mission objective.

b. Management decision to implement security countermeasures and to mitigate risk.

c. Implementation of countermeasures.

d. Periodic review of the risk management program.

5-10. Army Web Risk Assessment Cell (AWRAC)

The AWRAC is responsible for reviewing the content and security of Army's publicly accessible Web sites to identify and report Web site violations. The AWRAC conducts ongoing operational security and threat assessments of Army Web sites (.mil and all other domains used for communicating official information) to ensure that they are compliant with DOD and Army policies and best practices. See also para 6-7 of this regulation for Web site policy and para 8-7c of DA Pam 25-1-1 for additional information on AWRAC.

Chapter 6

Command, Control, Communications, and Computers/Information Technology Support and Services

6-1. Information technology support principles

This chapter pertains to automation (computer software, hardware, and peripherals), telecommunications (networks, BASECOM, long-haul, and deployable communications), and IT support for military construction.

a. *Information transmission economy and systems discipline.* All Army organizations will implement procedures to promote optimal, responsive, cost-effective use of all types of DOD ISs and services and ensure the application of sound management practices in accomplishing IS services' economy and discipline. (See also DODDs 4640.13 and 8000.01 and DA Pam 25-1-1, paragraph 7-1.) Commanders and activity heads will establish procedures to ensure—

(1) Users of computers and Army telecommunications are familiar with the types and purposes of available communications, services, and systems.

(2) Information managers (or designated telephone control officers (TCOs)) validate monthly bills, which are certified by the users for toll-free service, pager service, cellular phone service, calling card usage, long distance commercial calls, and commercial lines. The use of a personal identification number (PIN) process for telephone control is authorized and recommended.

(3) Information managers must review and revalidate all common-user Army information services, Government and commercial, regardless of user. The information manager will review dedicated information services and facilities at least every two years. Review and revalidation must include voice, video, data, and bandwidth utilization of NIPRNet and SIPRNet.

b. *Continuity of Operations Plan.* Headquarters, Department of the Army, and operational organizations must ensure the uninterrupted execution of their respective essential missions and functions under all conditions. The HQDA COOP, as noted in AR 500-3, is the model upon which organizations will create their COOP which must include procedures for the relocation of key leaders and staff to an alternate site(s), plans for the protection of critical records and files, and provisions for establishing minimum essential operational capabilities at relocation facilities. HQDA staff elements, Army commands, and other separate reporting organizations are required to maintain a COOP consistent with AR 500-3. An IT contingency plan is one essential element of a COOP. Each C4/IT system, including applications, deemed critical to essential Army missions or functions must be supported by its own contingency plan that ensures its continuous operation under all conditions. For guidance and procedures related to IT contingency planning, refer to DA

Pam 25-1-2. All COOPs must be tested at least annually. (See also paragraph 8-5j on the preservation of vital records.)

c. Network-centric (net-centric) applications and support. The net-centric approach promotes applications that are available on the Army's network and support a paperless office environment. Implementation of net-centric concepts to streamline processes will provide capabilities to save manpower, reduce redundancy, increase accuracy, speed transmission, increase information availability, and allow functions that would be impractical or impossible without their use. It is Army policy to employ net-centric concepts to support essential missions and functions. Making data visible, accessible, and understandable while promoting trust are the cornerstones of net-centric information sharing.

(1) Making data visible focuses on creating discovery metadata and deploying discovery capabilities that catalog data assets for users to find. Refer to paragraph 4-9 of this publication for information on Army data standards management.

(2) Making data accessible focuses on offering data assets over the network through commonly supported access methods, such as AKO/DKO, and providing access to the underlying information provided by the data asset so that authorized users can make use of it. Refer to paragraph 6-7 of this publication for policy on Army Web services.

(3) Making data understandable focuses on reaching an agreement on the meaning of information provided by data assets and making that understanding available to consumers through the DOD Metadata Registry. Refer to paragraph 4-9 of this publication for information on Army data standards management, including Army support of the DOD Metadata Registry.

d. Official uses of telecommunications and computing systems.

(1) The use of DOD and other Government telephone systems, electronic mail (e-mail), and other systems (including the Internet) are limited to the conduct of official business or other authorized uses. Commanders and supervisors at all levels will make all users of Government telecommunications systems aware of permissible and unauthorized uses. Local policies and procedures will be promulgated, as necessary, to avoid disruptions of telecommunications systems. (Authorized use is defined in paragraph 6-1e of this publication.) The Joint Ethics Regulation, Section 2-301, serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and disruptions to Army communications systems.

(2) All communications users must be aware of security issues, their consent to monitoring for all lawful purposes, restrictions on transmitting classified information over unsecured communications systems, prohibitions regarding release of access information such as passwords, and of the need to encrypt transmissions containing unclassified sensitive information. (See paragraph 6-4q of this publication for additional information on communications monitoring.)

(3) Commanders will recover toll charges, as practical, for unauthorized personal telephone calls placed on official telephones by personnel within their organizations. Charges may also apply to misuse of government communications through modem/other connections. See also paragraph 7-2c of DA Pam 25-1-1.

(4) Official business calls and e-mail messages are defined as those necessary in the interest of the Government (for example, calls and e-mail messages directly related to the conduct of DOD business or having an indirect impact on DOD's ability to conduct its business).

(5) Official use includes health, morale, and welfare (HMW) communications by military members and DOD employees who are deployed in remote or isolated locations for extended periods of time on official DOD business. HMW calls will be made on DSN. When authorized by the theater combatant commander, the theater commander will institute local procedures to authorize HMW communications when commercial service is unavailable or so limited that it is considered unavailable. HMW calls may be made only during non-peak, non-duty hours and should not exceed 15 minutes once per week. The commander may authorize calls that exceed this limit and frequency on an exception basis. (See paragraph 6-4u of this publication for guidance on acquiring and using cellular telephones.)

(6) Guidance for telephone calls while at a temporary duty (TDY) location is reflected in the Joint Travel Regulations.

e. Authorized uses of communication systems. Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of transportation or schedule changes. They also include personal communications from the DOD employee's usual workplace that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor, auto, or home repair appointments; brief Internet searches; e-mailing directions to visiting relatives). Such communications may be permitted, provided they—

- (1) Do not adversely affect the performance of official duties by the employee or the employee's organization.
- (2) Are of reasonable duration (normally five minutes or less) and frequency (twice per day), and, whenever possible, are made during the employee's personal time, such as during lunch, break, and other off-duty periods.
- (3) Are not used for activities related to the operation of a private business enterprise.
- (4) In the case of long distance (toll) calls, are—
 - (a) Charged to the employee's home phone number or other non-Government numbers (third party call).
 - (b) Made to a toll-free number.
 - (c) Charged to the called party if a non-Government number (collect call).

(d) Charged to a personal telephone card.

(5) Are of a legitimate public interest (such as keeping employees at their desks rather than requiring the use of commercial systems; educating DOD employees on the use of communications systems; improving the morale of employees stationed for extended periods away from home; enhancing the professional skills of DOD employees; job-searching in response to Federal Government downsizing).

f. Prohibitions in telecommunications usage. Prohibitions in the use of Army communications systems include the following:

(1) Use of communications systems, including Web services, that would adversely reflect on DOD or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images); chain e-mail messages; unofficial advertising, soliciting, or selling via e-mail; or subversive and other uses that are incompatible with public service.

(2) Use of communications systems for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DOD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or laws. This may include, but is not limited to, violation of intellectual property and copyright laws, gambling, support of terrorist or subversive activities, and sexual or other forms of harassment.

(3) Political transmissions to include transmissions that advocate the election of particular candidates for public office.

(4) Actions that result in the theft of resources or abuse of computing facilities. Such prohibitions apply to e-mail services and include, but are not limited to: unauthorized entry, use, transfer, and tampering with the accounts and files of others and interference with the work of others and with other computing facilities.

(5) Use of communications systems that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications. Such uses include, but are not limited to, the use of communications systems to—

(a) Create, download, store, copy, transmit, or broadcast chain letters.

(b) "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(c) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.

(d) Broadcast unsubstantiated virus warnings from sources other than systems administrators.

(e) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting the relevant audience.

(f) Employ applications for personal use using streaming data, audio, and video; malicious logic and virus development software, tools, and files; unlicensed software; games; Web altering tools/software; and other software that may cause harm to Government computers and telecommunications systems.

(g) Disseminating large files over e-mail instead of using shared drives or AKO/DKO.

g. Web access blocking. Per AR 25-2, paragraph 4-5, the use of Web access blocking/filtering tools is authorized for permanently blocking user access to inappropriate Web sites associated with the prohibited areas itemized in para 6-1f above. Exceptions to this policy will be applied to positions which may require unimpeded access to the Internet due to mission requirements, such as public affairs officers, intelligence specialists, staff judge advocates, inspectors general, auditors, and criminal investigation specialists. Other exceptions may be authorized by the organizational DAA. Organizations requiring exceptions to Web access blocking will maintain records to document access requirements for each position. Access to prohibited Web sites for mission support reasons is considered authorized use.

h. Administrative, criminal, and adverse actions. Unauthorized use or abuse of DOD and Army telecommunications and computing systems, to include telephone, e-mail systems, Web services or other systems, may subject users to administrative, criminal, or other adverse action.

i. Use of DOD-owned IT. Connecting or installing non-DOD-issued IT hardware or software to the LWN is prohibited. Exceptions will be approved by the organizational DAA prior to connection to the network. This includes the use of employee-owned assets that connect to the network at the work site. Use of employee-owned assets to process unclassified Army-related work off the Government work site must comply with the provisions of paragraph 4-31 of AR 25-2. See also paragraph 6-1o (telework) and paragraph 9-1g of DA Pam 25-1-1.

j. Product ownership. The products of Army-related work are the property of the U.S. Government, regardless of the ownership of the automation hardware or software.

k. IT support services for Army organizations on Army installations. IT support services consist of four categories: baseline, enhanced, mission-funded, and mission-unique. The current approved C4IM Service List or LWN Catalog is located at <https://www.itmetrics.hua.army.mil/>. See also paragraph 9-2 of DA Pam 25-1-1.

(1) Baseline services - These services are specifically designated as "baseline" in C4IM Services List. Installation DOIMs will provide baseline IT services to Army activities on a non-reimbursable basis.

(2) Enhanced services - These services are "baseline" services with enhanced performance measures that exceed one

automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information, and acquisition and use of automatic data processing, telecommunications, and other IT.

Information Technology (IT) Portfolio

A grouping of IT capabilities, IT systems, IT services, IT systems support services (for example, IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal.

Information system

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS-AITR, the terms "application" and "information system" are used synonymously - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. The application of IT to solve a business or operational (tactical) problem creates an information system.

Information Technology (IT)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment, or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Reference 40 USC Subtitle III (Clinger-Cohen Act of 1996).)

Infrastructure

The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities (to include building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format including audio, video, imagery, or data, whether supporting Information Technology or National Security Systems as defined in the CCA.

Installation

Geographic area subject to the control of the installation commander, including Government-owned housing or supported activities outside the perimeter of the military installation which depend on it for support.

Integration

The process of making or completing by adding or fitting together into an agreed framework (architecture) the information requirements, data, applications, hardware, and systems software required to support the Army in peace, transition, and conflict.

Integrity (of information)

Assurance of protection from unauthorized change.

Internet

An electronic communications network that connects computer networks and organizational computer facilities around the world.

Internet Service Provider (ISP)

An organization that provides other organizations or individuals with access to, or presence on, the Internet. Most ISPs also provide extra services including help with design, creation and administration of WWW sites, training, and administration of intranets.

Interface

A boundary or point common to two or more similar or dissimilar telecommunications systems, subsystems, or other entities at which necessary information flows take place.

IPv4 Interoperable

An IPv6-Capable system or product capable of receiving, transmitting and processing IPv4 packets.

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