Army Regulation 25–1

Information Management

Army Information Technology

Headquarters
Department of the Army
Washington, DC
25 June 2013

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–1
Army Information Technology

This major revision, dated 25 June 2013--

- Changes the title of the publication from "Army Knowledge Management and Information Technology" to "Army Information Technology" (cover).

- Realigns chapters by five principles: Army information technology management; Web site management; information and security management; enterprise architecture standards and certifications; and installation information technology services and support (para 1-5).

- Incorporates the newly formed Army Cyber Command/Second U.S. Army as the principal organization responsible for Army cyber operations and delineates multiple changes to roles and responsibilities as a result of Cyber Command's stand-up (chap 2).

- Updates the responsibilities of higher officials as necessary (chap 2).

- Adds requirements for Army organizations to use the Computer Hardware, Enterprise Software and Solutions procurement system (paras 2-16*h*, 3-4*a*, and 3-4*l*).

- Incorporates information management organizations below Headquarters, Department of the Army as a new paragraph (para 2-31).

- Removes knowledge management roles and responsibilities in response to functional roles and missions being realigned in the Army (throughout).

- Deletes Records management, Printing and publishing, Information Assurance, and Visual information chapters and incorporates relevant policy through and into the appropriate chapters (throughout).

- Restructures content in this publication; removes procedural, historical, and background information; and updates paragraphs with authoritative documents and Web sites in order to create a more lean, relevant, and user-friendly document (throughout).

- Removes telecommunications policy for inclusion in a new Army Regulation (throughout).

- Cancels DA Form 3938, Local Service Request (throughout).

- Cancels DA Form 5697, Visual Information (VI) Activity Authorization Responsibility Record (throughout).

- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
25 June 2013

*Army Regulation 25–1

Effective 25 July 2013

Information Management

Army Information Technology

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Acting Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation establishes policies and assigns responsibilities for information management and information technology. It applies to information technology contained in both business systems and national security systems (except as noted) developed for or purchased by the Department of Army. It addresses the management of information as an Army resource, the technology supporting information requirements, and the resources supporting information technology. This regulation implements 40 United States Code, Subtitle III; 44 United States Code, Chapters 35 and 36; 10 United States Code, Sections 2223 and 3014; and DODD 8000.01. It establishes the Army's Chief Information Officer. The full scope of the Chief Information Officer's responsibilities and management processes are delineated throughout this regulation. These management processes involve strategic planning, capital planning, business process analysis and improvement, assessment of proposed systems, information resource management (to include investment strategy), performance measurements, acquisition, and training.

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. Portions of this regulation prescribe specific prohibitions that are punitive, and violations of these provisions may subject offenders to non-judicial or judicial action under the Uniform Code of Military Justice. During mobilization, procedures in this publication can be modified to support policy changes as necessary.

Proponent and exception authority. The proponent of this regulation is 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 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 internal control process. This regulation contains internal control provisions and provides an Internal Control Evaluation for use in evaluating key internal controls (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–PRG), 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 Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (cio-g6.policy.inbox@mail.mil).

Committee management. AR 15–1 requires the proponent to justify establishing or continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060-5527. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15–1, then the proponent will follow all AR 15-1 requirements for establishing and continuing the group as a committee.

Distribution. 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.

*This regulation supersedes AR 25–1, dated 4 December 2008.

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Appendixes

Table List

Glossary

Chapter 1
Introduction

1–1. Purpose

This regulation establishes policies and assigns responsibilities for information management and information technology (IT). This regulation applies to IT contained in mission command systems; intelligence systems (except as noted); weapon systems (except as noted); business systems; and, when identified, national security systems (NSSs) developed or purchased by the Department of Army (DA). This regulation does not apply directly to information systems (ISs) acquired under the National Intelligence Program (NIP), the Military Intelligence Program (MIP), or to the operational support of intelligence and electronic warfare systems operating in a stand-alone configuration where inclusion of integrated support would not be efficient or effective.

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. Overview

a. This regulation is structured according to five disciplines. Army information technology management; Web site management; information and security management; enterprise architecture (EA) standards and certifications; and installation information technology services and support. Organizing IT policy under these five disciplines will assist end users in finding information within the regulation.

b. Regulation structure.

(1) *Responsibilities, chapter 2.* This chapter outlines the roles and responsibilities for Army organizations to manage and implement IT in the Army.

(2) *Army information technology management, chapter 3.* The information technology management (ITM) chapter outlines the life cycle of an IT investment. This chapter addresses Army IT governance and requirements for reporting, accountability, and compliance through the life cycle. Compliance with Army policies is supported through the Army's governance boards, reporting structures, and oversight procedures. The Strategic Management System tracks essential priorities and strategic initiatives in support of Army IT policy and strategic direction.

(3) *Web site management, chapter 4.* The Web site management chapter provides information on the appropriate and authorized use of Army Web sites, including Army Knowledge Online (AKO), SharePoint, and social media sites.

(4) *Information and security management, chapter 5.* This chapter includes information on data management (DM), visual information (VI) management, records management, publishing and printing, and information security. Information management (IM) includes the collection and management of information from one or more sources and the distribution of that information to one or more audiences. All ISs and IT described within this publication are subject to Army and Department of Defense (DOD) information assurance (IA) and security requirements. The IA and security policies are specifically addressed in AR 25–2 and the AR 380 series (for example, AR 380–5 and AR 380–53).

(5) *Enterprise architecture standards and certifications, chapter 6.* This chapter provides policy and guidance governing the composition and use of architecture documentation in the Army. It includes discussion on architecture governance, compliance with DOD and Army policies, and Internet protocol (IP) management.

(6) *Installation information technology services and support, chapter 7.* This chapter covers services and support on Army installations. Additional information about installation IT services and support can be found on the Installation Management Command's portal at http://www.acsim.army.mil/index.htm.

c. Global enterprise network. Land Warrior Network (LandWarNet) is the Army's contribution to the global information grid (GIG), which consists of the globally interconnected, end-to-end set of Army information capabilities; associated processes; and personnel for collecting, processing, storing, disseminating, and managing information on demand to support Warfighters, policy makers, and support personnel. LandWarNet includes all Army-owned, leased, and leveraged DOD, Joint communications and computing systems and services; software (including applications); data-security services; and other associated services.

(1) The Army's network, LandWarNet, is one of the Army's top modernization efforts. It is an essential enabler to a 21st-century expeditionary Army. Every facet of the expeditionary Army, from garrison to the tactical edge, leverages the network. Network functionality, agility, reliability, and security enable operationally effective business and warfighting operations. LandWarNet is continually changing and modernizing and requires Army users to update operational business processes to keep Soldiers, commanders, civilians, and mission partners connected, informed, and empowered.

(2) As LandWarNet is a global enterprise network, it is critical that regulations regarding the network and its proper use are understood and enforced. A vulnerability created by a single individual or organization not following Army regulations regarding the network's proper use will be a vulnerability shared by all users and organizations across this enterprise network.

1–6. Information accountability and transparency

a. Record-keeping requirements. Records created under the purview of this regulation, regardless of content or format, will be kept, at a minimum, in accordance with the retention schedules found at https://www.arims.army.mil. The Army Records Information Management System (ARIMS) is a role-based system managed and operated by the U.S. Army Records Management and Declassification Agency (RMDA). The primary purpose of ARIMS is to provide authorized personnel with Web-based tools and technology to manage both hardcopy and electronic Army records. Additional requirements at the State level, including statutory, legal, financial, or administrative by the authority of the State's governor and adjutant general, will be governed by Title 32 of the United States Code and managed in accordance with State policy. Note that 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 AR 25–400–2.

b. Information as a resource.

(1) 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 authorized to access the information 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. The management of information resources and IT is applicable to all Army organizations.

(2) The IT and related investments will be evaluated in terms of direct support and compatibility with Army enterprise (AE) solutions, mandates, and processes and their corresponding information requirements.

(3) The IT 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 during peacetime and wartime, and the peacetime information infrastructure must support wartime requirements by providing information services for rapid deployment and sustainment of U.S. Armed Forces around the world.

(4) The Army information architecture (AIA) was developed based on DOD's information enterprise architecture (IEA) in order to enable better understanding and interoperability of shared information by providing guidance and compliance requirements to Army stakeholders. The AIA enables the design, development, deployment, and use of information systems that are consistent, comprehensive, compatible, and integrated across the Army enterprise. This multiplies the impact of agile, adaptive IT by leading to more efficient and effective computing environments; which as part of the common operating environment are less costly to develop, design, field, and support. In addition, the AIA aligns to the Army and DOD data strategy to make data visible, accessible, understandable, trusted (to include protection, assurance, and security), and interoperable throughout their life cycle to any authorized Army consumer or mission partner possessing the appropriate security clearance and need to know. The end state of the LandWarNet, enabled by integrating the AIA into overall Army Enterprise Architecture (AEA) activities, will consist of data-enriched applications with an increased ability to access, interact with, and use diverse data stores. This is done via a layer of standard data services, informed as needed by information exchange standards specifications (IESS) within or among communities of interest (COIs).

1–7. Force generation through information sharing

When IT capabilities are focused to meet the information needs of the Warfighter, information can be employed as a force multiplier.

a. Force-multiplier benefits of information. Information becomes a force multiplier when it provides a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and enhances the probability of successful mission accomplishment. Information technology and DM provide tools that enable the Army to achieve force multiplication through information sharing and network-centric operations. Command and control has been a recognized force multiplier, and improvements in information technologies offer opportunities to improve existing information sharing and explore new approaches.

b. Customer-focused information technology management. The IT community professionals will maintain customer focus in their support of system users and the Warfighter.

(1) The Army IT community provides information capabilities and services for the benefit of Army, DOD, non-Defense Federal agencies, coalition partners, and the general public. The IT capabilities and services are not ends in themselves. Ultimately, they have value only when they support the Warfighter and the Army's mission. Because of the strategic and tactical roles of IT in support of the Army's missions, the IT community must maintain focus on the needs of its customers.

(2) This customer focus should include awareness of current user requirements, the quantity and quality of the

support provided, future customer requirements, and emerging IT capabilities. The Army's use of IT requires a strong relationship between the IT community and its customer, where both the customer and the service provider take responsibility for communicating with one another. Each organization's ITM process must have that same communication strength. Although primary responsibility must be assigned to the various aspects of this process, both IT providers and their customers must remain actively engaged for the process to succeed.

c. Customer participation in information technology management.

(1) Army customers must be sensitive to the IT community's need for customer involvement in seemingly unrelated management issues because of the potential IT impacts to Army organizations. Customers must also be willing to participate actively in the support process, especially in defining their requirements. Customers must identify their IT requirements and communicate these clearly to IT personnel (that is, information management officers (IMOs), S–6, G–6, or network enterprise centers (NECs)) throughout the procurement process to ensure the customers' needs are fulfilled.

(2) The IT community must embrace accountability to the customer. Ensuring that customer requirements are identified and met are essential elements of the ITM process. The IT community's acceptance of an agreed-upon customer support level must be fully backed with adequate IT staff and resources in order to meet the commitment at the supported installation site. Service and accountability to the customer will be incorporated into the analysis to outsource or consolidate, and included in agreements and contracts for IT support capabilities.

Chapter 2
Responsibilities

2–1. The Army Chief Information Officer/Deputy Chief of Staff, G–6

a. The Army has consolidated the Army Chief Information Officer (CIO) and the DCS, G–6 positions as the Army CIO/G–6. This allows the Army to better synchronize the Army's global network activities; to achieve secure, seamless interdependent global network processes and services; and, to better synchronize Warfighter requirements with global network capabilities and services. The Office of the Army CIO/G–6 serves as the principal focal point in Headquarters, DA (HQDA) for IM matters with Congress; the Government Accountability Office; the Office of Management and Budget (OMB); other Federal agencies; DOD; Joint Staff (JS); Army organizations and commands; and, other military departments, academia, and industry. The Army CIO/G–6 provides policy and guidance on IT systems and networks in accordance with General Order 2012–01. This includes reviewing and evaluating existing Army IM and IT policies to determine their adequacy and overseeing the implementation of DOD IT or IM-related policies or guidance. The CIO/G–6 provides oversight and coordination for the implementation of policies in—

(1) 44 USC 29, 44 USC 31, and 44 USC 33 (Public Law 94575, Federal Records Management); and 44 USC 35 (Federal Information Security Management Act (FISMA)), and 44 USC 36 (E-Gov Act).

(2) 5 USC 552 (Freedom of Information Act).

(3) 5 USC 552a (Privacy Act of 1974).

(4) 10 USC 3014 and 10 USC 2223(b).

(5) 40 USC Subtitle III (Clinger-Cohen Act).

(6) DODD 8000.01.

b. The CIO/G–6, as the Army CIO, is the principal staff assistant and advisor to the Secretary of the Army on Army IM, pursuant to 10 USC 3014(c)(1)(D), including but not limited to information enterprise (IE) networks and network-centric policies and concepts; command, control, communications, and computers (C4); non-intelligence space matters; and enterprise-wide integration of Army information matters. The CIO sets the strategic direction for and supervises the execution of Army IM policies and programs, including the global network, network architecture, and information-sharing policy. The CIO directs information resources management, including the allocation and obligation of IT capital assets in accordance with 40 USC Subtitle III; 44 USC 35; and, 44 USC 36. The CIO is the principal official within HQDA with oversight responsibilities for all IT resources under the provisions of the Clinger-Cohen Act. The CIO/G–6 coordinates with the Under Secretary of the Army, in his role as Chief Management Officer, to develop Army enterprise-wide business system architecture that supports Army business operations management.

c. The Army CIO/G–6, as the Army CIO, will—

(1) Serve as the Army's lead agent for LandWarNet to enhance the ability to reconcile current to future force LandWarNet capabilities, improve business agility, and achieve Warfighter decision superiority. The CIO is the single authority responsible and accountable to—

(a) Deliver structured, controlled, repeatable, and measurable processes that drive accountability and compliance for the management of the Army's information technology enterprise.

(b) Ensure secure LandWarNet capabilities and services to Army leadership and Warfighters.

(c) Enable agile responses to rapidly changing operational requirements for Army and Joint missions.

(2) Direct IM function within the DA, including to—

(a) Develop the DA's IM strategy, policies, and guidance that are in compliance with laws, regulations, and standards.

(b) Oversee IM and IT resources planning, programming, budgeting, and execution;

(c) Develop and implement the IM and IT capital planning and investment-control strategy, including the design and operation of all major information resources management processes.

(d) Develop, coordinate, and implement an assessment process for Army IM programs; including compliance with IM policies, guidance, standards, and monitoring.

(3) Support the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA (ALT)) through the development of policy on the acquisition of IM, IT, and information resources. Ensure that acquisitions are managed in a manner that implements CIO/G–6 policies and procedures to maximize value while assessing and managing the risks for acquiring IT.

(4) Serve as the appeal authority to receive and resolve appeal requests for ensuring the quality, objectivity, and integrity of Army information disseminated to the public in accordance with FOIA and Privacy Act programs.

(5) Establish, maintain, facilitate, and guide the implementation of the Armywide EA.

(6) Prescribe Army strategy, policy, and portfolio management for Army bandwidth capabilities and activities.

(7) Serve as member of the Federal CIO Council and the DOD CIO Executive Board (EB).

(8) Chair the Army CIO EB.

(9) Develop, promulgate, and direct compliance with information security and IA policy (see AR 25–2).

(10) Review, coordinate, and co-certify the IT Budget in conjunction with the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)).

(11) Represent the Army on the Committee on National Security Systems.

(12) Oversee the Armywide implementation and modernization of LandWarNet.

(13) Prescribe Army IE strategy, policy, portfolio management, architecture, and strategic communications that result in effective IT investments Armywide.

(14) Participate as a core member of the Business Systems Information Technology–Executive Steering Group (BSIT–ESG) in the role of standards provider.

(15) Serve as the Army designated approval authority (DAA) for the certification and accreditation (C&A) of collateral top secret and below Army information systems (see AR 25–2).

(16) Monitor the operations and structure of the military and civilian personnel management systems to ensure that the Army's requirements for qualified IT and communications personnel are addressed and that IT career development plans, programs, and objectives are established. Duties include serving as the functional chief for the ITM career program 34 (CP–34) and as the principal coordination point for designated military specialties. The CIO is responsible for the policy, oversight, and management of the Army civilian ITM CP–34. (See also DA Pam 25–1–1, AR 690–950, and AR 350–1.)

(17) Prescribe IT portfolio management (PfM) policy and oversee implementation of mission area (MA) IT portfolios to ensure they are aligned with Army enterprise solutions.

(18) Serve as the Army's lead for the Enterprise Information Environment Mission Area (EIEMA) to support the DOD EIEMA lead and ensure enterprise information environment efforts are traceable to, and fully enable, the required capabilities for the Warfighting and business MAs.

(19) In coordination with Army Cyber Command, direct research of new IT technologies and training venues that deliver value across the enterprise.

(20) Reduce the introduction of vulnerabilities and system interoperability performance problems by controlling and approving changes to the Army's authorized software baseline that constitutes its operational network. For additional information, see the Configuration Management Plan at https://ctsf.army.mil/cmweb/librarian.htm and scroll down to click on the "SOPs" tab.

(21) Serve as functional proponent for the Army enterprise portals (that is, AKO, enterprise collaboration services, and so forth).

(22) Serve as the functional proponent of AEA, to include establishing, implementing, leading, and managing the AEA.

(23) Establish and oversee the Army Data Management Program (ADMP) to include the appointment of the Army Chief Data Officer (see also chapter 5 of this publication).

(24) Provide oversight and direction for network-centric concepts and management, including the Army Networthiness Program.

(25) Serve as the functional proponent and primary interface with the Defense Information Systems Agency (DISA) on existing and emerging DOD enterprise services such as email, data center consolidation, collaboration, and unified communications.

d. The Army CIO/G–6, as the Army Staff G–6, is the principal advisor to the Chief of Staff of the Army, the Army Staff, Army service component commands (ASCCs), Army Cyber Command/Second U.S. Army, and combatant commands of unified and specified commands for IM, IT, and their impact on current and future Warfighting

capabilities. This includes advice on all matters concerning enterprise information activities required to ensure the standardization, compatibility, security, interoperability, and fiscal discipline of enterprise information services supporting the Warfighter.

e. The CIO/G6, as the Army Staff G–6, is responsible for information management and signal operations, network and communications security, force structure, equipping, and employing signal forces. The CIO/G–6, as the Army Staff G–6, will—

(1) Develop and execute the Army's IM and IT strategy, policy, plans and programs; and oversee the execution of IM and IT policies and plans by other Army organizations.

(2) Monitor and advise on information and signal operations, network and communications security, force structure, and the equipping and employment of signal forces. Assess the impacts to the Warfighter of IM-related strategy, policies, plans, services, and programs. Advocate for and monitor the implementation of IM requirements on behalf of the Warfighter.

(3) Oversee the implementation and enforcement of Army global network requirements and operations to achieve standardization, compatibility, security, interoperability, and fiscal discipline of IM and IT services supporting the Warfighter.

(4) Provide policy, guidance, and resourcing for the Army's communication needs for all network layers, including top secret and higher levels of security, as well as access to coalition networks.

(5) Serve as senior authority for telecommunications programs and committees. See AR 25–13 for more information.

(6) Serve as senior authority for Army VI and multimedia products as defined in chapter 5 of this regulation and in DA Pam 25–91. The Army CIO/G–6 Visual Information Management office is responsible for managing the Army's VI activities.

(7) Serve as the proponent for the information systems supporting C4 and IT programs, including, but not limited to—

(a) Serve as the Army focal point for IT system issues (to include NSS). Receive, coordinate, and integrate these issues, ensuring the integration of systems-development efforts with cross functional or technical lines.

(b) Participate in and provide representation for the planning, programming, budgeting, and execution (PPBE) process decision group; and exercise centralized oversight of IT expenditures for all appropriations, including formulating and defending the resources necessary to provide C4/IT to the Warfighter.

(c) Develop, coordinate, and manage the IT capital planning and investment management program.

(d) Recommend and coordinate new standards and ensure IT system conformance to the approved DOD IT Standards Registry (DISR); coordinate and support the priorities within IT for information system development-related activities; and secure adequate resource support.

(e) Coordinate resource requirements for IT support activities.

(f) Coordinate IT requirements relevant to Army continuity of operations (COOP) plans and systems that support survival, recovery, and reconstitution; and ensure essential information services in support of DA COOP are available to alternate sites of HQDA agencies, Army commands (ACOMs), and installations.

(g) Prescribe, in conjunction with the Office of the Administrative Assistant to the Secretary of the Army, records management requirements in the life cycle of ISs, beginning at the initial milestone.

(h) Collaborate with the Deputy Chief of Staff, G–8 in the development of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) positions presented at Functional Capabilities Boards, the Joint Capability Board, and the Joint Requirements Oversight Council.

(8) Lead and manage the Army Net-Centric Data Management Program and serve as the Army component data administrator under the DOD Data Administration Program (see chap 5).

(9) Manage, plan, and program for the Army Spectrum Management Program (AR 5–12).

(10) Ensure Army interoperability processes are structured to allow seamless transition for obtaining Joint Interoperability Certification and synchronize the Army Portfolio Management Solution (APMS) with the DOD IT Portfolio Repository (DITPR). This includes, but is not limited to—

(a) Represent Army interests in Joint, DOD, and Army technical interoperability forums.

(b) Expand interoperability certification process to cover all capability areas. Incrementally establish memorandums of agreement (MOAs) with functional proponents laying out portfolio Army Interoperability Certification (AIC) requirements and strategies.

(c) Ensure appropriate Joint certification documentation has been developed to allow for continued fielding of Army systems while also satisfying Joint Interoperability Certification requirements.

(d) Establish Federated Net-centric Sites (FaNS) criteria for accreditation by the Office of the Army CIO/G6.

(e) Coordinate with the U.S. Army Training and Doctrine Command (TRADOC) and ASA (ALT) in the development and review of all mission threads.

(f) Prescribe guidance for the Army's use of the Defense Research and Engineering Network (DREN). (See https://www.us.army.mil/suite/files/13410760 for additional DREN guidance.)

(g) Prescribe Army IP address policy, and direct plans for IP address management and usage.

(h) Validate IT and NSS requirements through the review of data on the capabilities and Army Requirements Oversight Council Management System.

(i) Ensure that IT infrastructure requirements to sustain interoperability requirements are identified in the Army's budget submissions.

(j) Ensure the compatibility and interoperability of IT and NSS with Joint, unified, combined, Federal Government, and other Army systems as required.

(11) Establish annually, in coordination with Army Cyber Command and U.S. Army Network Enterprise Technology Command (NETCOM), the vision, direction, and architecture of Installation-Information Infrastructure Modernization Program (I3MP) for use by NECs in their requirements development efforts.

2–2. Army Cyber Command/Second U.S. Army

Army Cyber Command/Second U.S. Army will conduct cyber operations, including to—

a. Exercise a single command and control authority for all collateral top secret and below Army network operations in accordance with Army, Joint, and DOD regulations.

b. Serve as the single authority for the operation, management, and defense of the LandWarNet global enterprise network, including as follows—

(1) Prescribe all common-user IT services and capabilities.

(2) With exception to Joint Worldwide Intelligence Communications System (JWICS), serve as the single authority to implement Army IP policy, conduct Army IP registration, and manage Army IP address space.

(3) Prescribe "army.mil" and "army.smil.mil" Internet domains and the assignment of sub-domains requested by other Army organizations.

(4) Manage Army IT network and system capabilities to achieve survival, recovery, and reconstitution for COOP support requirements in accordance with AR 525–27.

(5) Execute Army Computer Network Defense-Service Provider (CND-SP) responsibilities to include incident, event, and problem management, in accordance with DODD 0–8530.1. Serve as the Army's primary general service CND-SP, which includes responsibility for executing, monitoring, and managing CND services for Army-controlled networks. In addition, also be responsible for coordinating Army CND-SP support for networks supported by Army Forces but not under direct Army control.

c. Oversee and report threats to the Army global enterprise network and, as required, other DOD agencies and their enabling technologies.

d. Prescribe the operational activities, policies, processes, procedures, and protocols for reportable intelligence and information; in addition to incident management, event management, problem management, and database and Internet/Web management.

e. Prepare and rehearse a network operations COOP plan, to include resolving actual or potential interruptions in service or reductions in quality of service in mutually agreed upon response times; identifying and prioritizing infrastructure, service, and security events; establishing appropriate responses to those events; defining and eliminating problems that have detrimental impact on quality and cost of services; mitigating probability of problem occurrence; and ensuring optimal performance, security and functionality of enterprise databases and hosted applications.

f. In coordination with CIO/G–6, support information security and information assurance compliance for collateral top secret and below networks and systems—

(1) Prescribe the operational aspects of information protection and data security, including processes that enforce Armywide compliance with the Federal Information Security Management Act of 2002 and OMB Circular A–130. Identify and analyze threats to the Army global enterprise network and its enabling technologies.

(2) Measure Army compliance with IA requirements and prescribe IA program operational execution activities, processes, and practices (see AR 25–2).

g. Enable external engagement—

(1) Formulate Army military telecommunications exchange agreements between the United States and regional defense organizations or friendly foreign nations, and coordinate each agreement's procedural details with the commander of the relevant theater of operations.

(2) In support of Joint staff information requirements—

(a) Develop and maintain plans.

(b) Provide reports on JS-controlled communications assets, as required.

(3) Fund (as appropriate), operate, maintain, and defend equipment, facilities, systems, and required services supporting the United States, the North Atlantic Treaty Organization (NATO), and NATO-member communications objectives, as assigned; and provide subject-matter expertise in negotiations for communications agreements.

h. Oversee operational review and coordination of information infrastructure or architectures. Advise the CIO/G–6 on AEA, in support of implementation, management, and security of the global enterprise network.

i. Operate Army communications facilities and circuitry as part of the Defense Information Systems Network (DISN), including to—

(1) Approve and validate telecommunication requests for service, to include special-access requirements.

(2) Operate, maintain, and defend the Defense Red Switch Network, as well as the Army's portion of military satellite communications for Defense satellite communications systems; Defense Information Infrastructure (microwave and fiber optic cable systems); and routers on the non-secure Internet protocol router network (NIPRNET), secret Internet protocol router network (SIPRNET), and defense switched network (DSN).

j. Develop, validate, and execute approved Army telecommunications requirements to DISA and overseeing implementation of Army telecommunication requirements.

2–3. The U.S. Army Network Enterprise Technology Command

NETCOM will provide enterprise management and services, including to—

a. Serve as the DAA for the Army enterprise, as directed by the CIO/G6.

b. Serve as the Army IT integrator to achieve a single, virtual, Enterprise Network by advising the end-to-end management of the Army's enterprise service area (service delivery, service operations, and infrastructure management) using the AEA and IEA. Provide Army network enterprise services and capabilities, including the mandated core enterprise services of the DOD Information Enterprise Architecture, installation IT services, and network connectivity. Prescribe the Army's IT Service Management Program—

(1) Prescribe all service delivery activities, policies, processes, procedures, and protocols for configuration management, availability management, capacity management, change management, and release management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority for any system architecture design or device that impacts the Army global-enterprise network and enabling technologies.

(2) Prescribe all service operations activities, policies, processes, procedures, and protocols for incident management, event management, problem management, spectrum management, and database and Internet Web management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority over capabilities that impact the Army global-enterprise network and enabling technologies.

(3) Prescribe all infrastructure management activities, policies, processes, procedures, and protocols for network and telecommunications management, facilities management, data storage management, IT services continuity management, and mid- and mainframe management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority over capabilities that impact the global-enterprise network and enabling technologies.

c. Prescribe security of assigned fixed-station communications facilities and Army contractor telecommunications.

d. Prescribe requirements for mobile or transportable communications assets to support assigned missions and functions.

e. Organize and chair the LandWarNet technical configuration control board, and direct the Army enterprise configuration control and release management.

f. Advocate for transformation, and engineer the enterprise network to efficiently and effectively serve the needs of the Army.

g. Oversee Army leases of telecommunications services, and ensure that such services conform to DOD and National Communications Systems guidance.

h. Oversee the Army Military Affiliate Radio System program, including amateur radio operators licensed to operate as a Military Affiliate Radio System member (see AR 25–6).

i. Support CIO/G6 to prescribe resources (people, projects, technology, and infrastructure) for service delivery, service operations, infrastructure management, IA, and network defense.

j. Prescribe communication services in support of the news media during field exercises, contingencies, and combat operations when commercial capabilities are not available.

k. Prescribe the Army's Networthiness Program; and the operational assessment of systems, applications, or devices to determine security, interoperability, supportability, sustainability, usability (SISSU), and compliance with Federal, DOD, combatant commanders, Services, and agency regulations, policies, and guidelines.

l. Require mission application owners and maintainers to provide evidence of a rigorous source code validation and remediation program for Government-developed or -maintained software and applications components submitted for certificates of networthiness. This ensures adherence to secure coding practices and provides evidence of due diligence with respect to software assurance considerations in the selection of commercial off-the-shelf (COTS) products integrated into systems or submitted for certificates of networthiness.

m. Prescribe the Army's IT Service Management Program.

n. Provide combat camera (COMCAM) documentation support for theater Army, Joint military operations, and operations other than war, including to develop and maintain appropriate plans.

o. Oversee the formulation, operation, maintenance, and defense of the Defense Telecommunication Service-Washington, in accordance with DODI 4640.07.

p. Provide an IT-operational engineering force with worldwide deployment capability to provide quick-reaction support to plan, integrate, install, operate, and maintain IT systems from the power projection platform to the tactical theater of operations.

q. Prescribe server and application consolidation, collaboration tools, best-business practices, and Web services supporting the global-network enterprise. Also, prescribe the configuration of Web applications across the Army.

r. Provide technical guidance for connectivity between Army DREN users and Army installations for Army enterprise services.

2–4. Principal officials, Headquarters, Department of the Army

Within their respective areas of functional and process proponency, principal officials, HQDA will—

a. Serve as the HQDA proponent for information requirements and associated capabilities within assigned functional areas of responsibility.

b. Oversee functional processes within respective functional portfolio areas to maximize end-to-end enterprise processes and reduce redundancy in systems and local processes.

c. Analyze their missions and revise their mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes.

d. Request and defend the capabilities and supporting resources needed for the development, deployment, operation, security, logistics support, and modification of ISs through the PPBE process.

e. In coordination with their mission area architect, develop rules-based architectures for their respective functional segments; act as the integrator for any "system of systems" under their purview; and coordinate with CIO/G–6, as needed, on AEA documentation.

f. Use E-Gov technologies to the maximum extent practicable to promote the goal of a paper-free (or nearly paper-free) business environment within the Army.

g. Manage and oversee the records of respective functional areas to appropriately secure, maintain, and preserve them throughout their life cycle (see DA Pam 25–1–1, AR 25–400–2, DA Memo 25–51, and DA Pam 25–403 for additional responsibilities and information on the life cycle of records).

h. Identify functional requirements for Army enterprise ISs and, as required, participate in related governance and advisory board activities.

i. Establish IT PfM processes for assigned mission areas in order to define and justify planned IT expenditures that are consistent with DOD and Army guidance.

j. Administer a telework program for their respective organizations and subordinate elements as prescribed in DOD and HQDA policy and guidance (see DA Memo 690–8 for more information).

k. Provide a subject matter expert who will serve as a data steward under the direction of the Chief Data Officer; and who will also be responsible to develop, implement, and enforce Federal, Army, and organizational data standards, processes, and procedures.

2–5. Under Secretary of the Army

In addition to the duties listed in paragraph 2–4, the Under Secretary of the Army, or a designated representative, will—

a. Serve as the Army's lead for generating force enterprise activities (GFEAs).

b. Serve as the Chief Management Officer (CMO) for the management, coordination, oversight, and synchronization of the generating force's business operations, processes, and decisionmaking procedures. This includes assisting with the integration and management of IT capabilities and services within the Generating Force through the Office of Business Transformation's (OBT) Directorate of Business Operations.

c. Preside over the BSIT-ESG.

d. Ensure that a single, integrated architecture for GFEA exists to support the Business Enterprise Architecture (BEA) and provide architecture products for integration into the AEA.

2–6. Assistant Secretary of the Army (Financial Management and Comptroller)

In addition to the duties listed in paragraph 2–4, the ASA (FM&C) is responsible for the review and co-certification of the IT budget prepared by the CIO/G–6. This includes Exhibit 300s, IT1 spreadsheets (IT budget summaries), and Exhibit 53s. The ASA (FM&C), in collaboration with the CIO/G–6, will co-certify the Army IT budget submission and assist the GFEA lead in financial management of IT.

2–7. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

In addition to the duties listed in paragraph 2–4, the Army CIO/G–6 and the ASA (ALT) are strategic partners in transforming Warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced DM and PfM solutions. Responsibilities for the ASA (ALT) are defined in AR 70–1. The ASA (ALT) responsibilities unique to IT are to—

a. Serve as the source selection authority (or delegate the source selection authority responsibility) for acquiring IT

systems, working together with the Army CIO/G–6. This includes assisting the GFEA lead in the Acquisition IT Program implementation.

b. Direct and review command, control, communications, and intelligence systems; target acquisition systems; and direct tactical IT requiring research, development, test, and evaluation (RDT&E) efforts.

c. Execute the planning, programming, budgeting, and life cycle management necessary for the research, development, and acquisition of ISs required for strategic and tactical programs.

d. Execute the RDT&E and procurement portions of IT programs and budgets, in collaboration with the Army CIO/G–6.

e. Oversee the IT base relative to its impact on the Army industrial base.

f. Review IT system readiness for testing during full-scale development.

g. Participate as a core member of the BSIT-ESG in the role of materiel provider.

h. Ensure that project managers (PMs) and program executive officers (PEOs) successfully complete developmental interoperability assessments prior to AIC.

i. Ensure that PMs and PEOs design, build, test, and field IP-enabled IT and NSSs to efficiently use IP address space. Coordinate materiel solution, and IP address space requirements with TRADOC and Army Cyber Command/Second U.S. Army as required.

j. Review and approve the Army position for acquisition category (ACAT) ID and ACAT IAM programs at each decision milestone, before the Defense Acquisition Board or IT Acquisition Board review. This includes the review and approval of acquisition program baselines (see DODI 5000.2 for further clarification on ACAT programs).

k. Serve as the milestone decision authority for Army ACAT IC, ACAT IAC, and ACAT II programs.

l. Serve as the Army executive architect for mission command system architectures. In the mission command segment, validate Army system views and ensure managed programs develop system views that are integrated with approved operational views (OVs), as prescribed by TRADOC and approved standards views as prescribed by the Army CIO/G–6.

m. Approve and assign software reuse domains and domain management responsibility, based on recommendations from the CIO/G–6.

n. Ensure that materiel developers comply with software assurance, technical architecture (TA), AIC, and baseline configuration management policies and procedures.

o. Ensure that PEOs and PMs comply with AIC policy (chap 6) and configuration-management procedures, and that they resource adequately for systems to undergo AIC testing (see DA Pam 25–1–1).

p. Serve as the Army's domain lead for the acquisition sub-segment within the GFEA segment.

q. Serve as the Army's system engineer responsible for planning, developing, acquiring, fielding, sustaining, and properly disposing of equipment and services; and leveraging technologies and capabilities to meet current and future Army needs. Apply approved system-engineering methods to ensure the integration and interoperability of all Army C4ISR programs of record.

2–8. Office of General Counsel

In addition to the duties listed in paragraph 2–4, the Office of General Counsel will—

a. Advise on legal issues that arise during IS acquisitions.

b. Advise on legal issues that arise within programs and activities managed by the Army CIO/G–6.

c. Advise on legal issues associated with information technology and cyber operations.

2–9. Administrative Assistant to the Secretary of the Army

In addition to the duties listed in paragraph 2–4, the AASA will—

a. Serve as Archivist of the Army.

b. As the Archivist of the Army, the AASA will designate a Senior Agency Official (SAO) to oversee and review the Army records management program. Ensure that records related to matters involved in administrative or legal proceedings are retained until the staff judge advocate or legal advisor authorizes resumption of normal disposition.

c. Oversee the ARIMS, including to—

(1) Serve as the proponent for AR 25–400–2.

(2) Advise the Secretary of the Army (SECARMY) concerning the destruction of records in legal custody in an Army repository outside the continental United States (OCONUS) during a state of war between the United States and another nation or when hostile action (by a foreign power, terrorist agents, or public demonstrators) seems imminent in accordance with 44 USC 3311.

(3) Establish life-cycle management instructions for the systematic identification, maintenance, storage, retrieval, retirement, and destruction of Army information recorded on any medium (for example, paper, microforms, and electronic records).

(4) Ensure that mission-essential records are available in a usable format; and created, maintained, used, and disposed of at the least possible cost.

(5) Preserve records needed to protect the rights and interests of the Army and its current and former members, and records that are of permanent value (see AR 25–55 and AR 340–21).

d. Develop and maintain the Army Information Collection Budget required by 44 USC 35.

e. Establish records declassification requirements in accordance with Executive Order (EO) 12958.

f. Advise the SECARMY concerning the destruction of records that are in legal custody in an Army repository OCONUS during a state of war between the United States and another nation; or when hostile action (by a foreign power, terrorist agents, or public demonstrators) seems imminent.

g. Oversee the Army Privacy Program.

h. Serve as the records official for HQDA as an ACOM.

i. Serve as the Army's representative to receive and resolve claims that allege Army information disseminated to the public does not comply with information quality standards issued by the OMB. (See also chap 5 of this publication.)

j. Oversee the Army Publishing Program (APP), including to—

(1) Be the proponent for AR 25–30.

(2) Establish policy and exercise program management for Army publications and printing, except areas defined in AR 115–11, which governs Army topography.

(3) Establish policy, procedures, and standards for control, production, issue, storage, and distribution of Army publications and forms.

(4) Serve as the HQDA point of contact (POC) on publishing policy issues with the chairman of the Joint Committee on Printing, the Public Printer, the Government Printing Office, the Director of Bureau of Engraving and Printing, and the Administrator of the General Services Administration (GSA).

(5) Oversee modernized processes for the paperless development, storage, and distribution of Army publications.

k. Manage Army Multimedia and Visual Information Directorate (AMVID) operations.

l. Serve as the authenticating official for all departmental publications, except Army General Orders that the SECARMY authenticates.

m. Serve as the sole Army organization authorized to execute contracts for productions in their entirety for the Army, Defense agencies, and as required, other components and Federal agencies.

n. Monitor IT for HQDA internal use. The IM function within HQDA is prescribed by the Army CIO and Army Cyber Command/Second U.S. Army, and executed by the HQDA Information Technology Agency. The Information Technology Agency will—

(1) Integrate and act as the functional and process proponent of internal HQDA information requirements common to more than one HQDA element or agency.

(2) Accomplish all the IM and IT responsibilities for HQDA as those assigned to ACOM commanders (see 2–16 for more information).

(3) Provide IM common services and operational information support to HQDA.

(4) Provide an HQDA perspective to the Army IM and IT strategic planning.

(5) Provide information management officer (IMO) support for the Office of the Secretary of the Army; the Office of the Chief of Staff, Army; and supported activities.

o. Manage and oversee the HQDA Telework Program as prescribed in DA Memo 690–8.

p. Formulate, operate, maintain, and defend the Defense Telecommunication Service-Washington, in accordance with DODI 4640.07.

2–10. Chief of Public Affairs

In addition to the duties listed in paragraph 2–4, the Chief of Public Affairs will—

a. Establish public affairs policy and regulatory guidance for release of Army VI products to the public.

b. Establish public affairs policy for oversight and management of content on Army public Web sites.

2–11. Director of the Army Staff

The Director of the Army Staff will accomplish all the IT responsibilities assigned to the principal HQDA officials for the Office of the Chief of Staff, Army (see para 2–4 for more information).

2–12. Deputy Chief of Staff, G–2

The Army CIO/G–6 and the DCS, G–2 are strategic partners in transforming Warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced solutions. In addition to the duties listed in paragraph 2–4, the DCS, G–2 will—

a. Inform the CIO/G–6 of investments in the intelligence community for purposes of developing Armywide investment strategies.

b. Manage and oversee NIP- and MIP-funded efforts and other intelligence programs.

c. Provide staff supervision for counterintelligence, IS security monitoring, and counter human-intelligence activities.

d. Provide functional oversight and management for Army-managed DOD intelligence IT purchases, systems, and leases.

e. Serve as Army lead for the sensitive compartmented information (SCI) IA program, IP policy, and procedures pertaining to ISs processing intelligence information.

f. Serve as the single DAA and certification authority for the C&A of Army JWICS and noncryptologic SCI systems.

g. Serve as the Army's representative to the intelligence segment led by the Under Secretary of Defense for National Intelligence and National Intelligence Technology Infrastructure. Coordinate with Army segment and sub-segment leads as appropriate to ensure alignment with the Army's IT PfM efforts.

h. Ensure and manage Armywide compliance with FISMA for JWICS and noncryptologic SCI systems.

i. Establish connection requirements and manage connection approval processes for JWICS. The JWICS connection approval process will address DOD information systems, coalition partner information systems, and contractor support or commercial partner information systems.

j. Oversee the Ground Intelligence Support Activity, which serves as the Army service provider for SCI systems, the single Army JWICS IP registration authority, and the responsible organization for implementing Army JWICS IP policy.

k. Oversee the Commanding General (CG), U.S. Army Intelligence and Security Command (INSCOM), as a direct reporting unit (DRU) to DCS, G–2, in his or her responsibilities, in addition to paragraph 2–16, to—

(1) Provide support to Army Cyber Command/Second U.S. Army for full-spectrum cyberspace operations.

(2) Provide C4-related and IT-related combat and materiel development requirements, and update data input for supporting intelligence, electronic warfare, and security operations to TRADOC, the U.S. Army Materiel Command (AMC) and the U.S. Army Forces Command (FORSCOM).

(3) Operate the U.S. Army Cryptologic Records Center, the repository for all permanent cryptologic records.

(4) Operate the U.S. Army Investigative Records Repository to support intelligence and counterintelligence activities or other Army intelligence programs.

(5) Oversee NIP and MIP systems maintained by the command.

(6) Provide functional support to the C4/IT PEOs and PMs as designated by the Army acquisition executive.

(7) Coordinate the C4 and IT system design of proponent systems with TRADOC.

(8) Represent the Army CIO and Army Cyber Command/Second U.S. Army to the national intelligence community for intelligence matters related to computer network operations.

(9) Collaborate with and support the CG, Army Cyber Command/Second U.S. Army and the CG, NETCOM in their missions to operate, maintain, and defend the LandWarNet and conduct cyberspace operations.

2–13. Deputy Chief of Staff, G–3/5/7

The Army CIO/G–6 and the DCS, G–3/5/7 are strategic partners in transforming Warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced solutions. In addition to the duties listed in paragraph 2–4, the DCS, G–3/5/7 will—

a. Validate, synchronize, and prioritize Army network requirements for delivering an interoperable, affordable, and versatile set of mission command and network solutions that meet current, emerging, and future needs of operational commanders. Approve IT requirements in accordance with DA General Order 2012–01.

b. Develop, validate, and establish priorities for strategic, theater, and tactical information requirements for strategic command and control (C2) programs, and assist the GFEA lead in LandWarNet IT implementation.

c. Validate and revalidate requirements for all network-related, operational -needs statements or Joint urgent operational needs statement actions and new procurements, to ensure that they fit within the Army's enterprise network as a part of the LandWarNet and base communications governance construct.

d. Validate and establish priorities for operational information requirements at HQDA.

e. Validate tactical VI COMCAM documentation support for Army operational planning documents for contingencies, emergencies, training exercises, and other peacetime engagements.

f. Lead development of a comprehensive Army network modernization strategy, employing the network architecture prescribed by the Army CIO/G–6, which synchronizes activities and incorporates an identification and reconciliation process for innovative or emerging capabilities.

g. Provide a full-time C2 facility for HQDA.

h. Serve as the Army's MA lead for the warfighting mission area (WMA). Validate, approve, prioritize, and synchronize all LandWarNet capabilities, experimentation, concepts, and operational architecture (OA) development efforts for the WMA.

i. Oversee changes to the certified and approved software baselines in the AIC process.

j. Ensure the formal release of the CIO/G–6 interoperability baseline to the field.

k. Participate as a core member of the BSIT-ESG.

l. Oversee Army architecture policy and publication of the annual architecture development priorities.

2–14. Assistant Chief of Staff for Installation Management

In addition to the duties listed in paragraph 2–4, the ACSIM will—

a. Provide installation-support capabilities to meet installation IT service and support requirements as prescribed by the Army CIO, the Army Cyber Command/Second U.S. Army, and NETCOM. Assist the GFEA lead with installations and environment IT implementation.

b. Integrate the command, control, communication, and computers for information management (C4IM) services list and measurements contained in the Army's IT Metrics Program into the common levels of support (CLS) process.

c. Plan and program IT resources to support the installation's common use IT requirements, as required by the Army CIO, Army Cyber Command/Second U.S. Army, and NETCOM.

d. Oversee Army Family and Morale, Welfare, and Recreation Command ISs.

e. Establish a senior VI official responsible for implementing the VI program in accordance with this regulation as prescribed by the Army CIO/G–6. The senior VI officials will directly oversee, coordinate, and represent ACSIM and the Installation Management Command (IMCOM) on all VI-related programs and activities.

2–15. The Judge Advocate General

In addition to the duties listed in paragraph 2–4, The Judge Advocate General will—

a. Provide IT-related combat and materiel development plans and data supporting military legal operations to Army organizations.

b. Oversee legal technology support provided by the Army CIO, Army Cyber Command/Second U.S. Army, and NETCOM for rapid, responsive, and continuous provision of military justice, claims, legal assistance, international and operational law, and other legal support to the Warfighter, commander, and staff across the full spectrum of military engagement.

2–16. Commanders of Army components, Army commands, Army service component commands, and direct reporting units (as authorized by their respective Headquarters, Department of the Army elements)

The Army CIO/G–6, Army Cyber Command/Second U.S. Army, and ACOM, ASCC, and DRU (as authorized by their respective HQDA elements) commanders are strategic partners. Together, they achieve the standardization, compatibility, interoperability, security, and resourcing of the LandWarNet global network enterprise to ensure Warfighter decision superiority. For the internal IM and IT responsibilities of their commands, commanders will—

a. Establish a senior IM official who is responsible for implementing the command's IM and IT program in accordance with IM and IT policies, as prescribed by the Army CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities as prescribed by the Army Cyber Command/Second U.S. Army, including to—

(1) Provide, as required, representation to the Army CIO EB and associated working groups and committees.

(2) Identify the command's IT requirements and ensure that mission requirements are validated, coordinated, and integrated in accordance with AR 71–9. Collaborate with NECs to obtain command-unique IT requirements beyond common-use services and when acquiring any mission-unique IT products.

(3) Monitor command mission-related IM requirements throughout their life cycle, including those requirements for subordinate organizations located on other installations for IT requirements not included as part of established, common use IT.

(4) Submit requests and requirements for mission-driven, installation-level IT infrastructure implementations (outside cable plant connectivity, campus area switching upgrades, and so forth) to the local installation NEC for processing through NETCOM to the Army CIO/G–6 for ultimate approval or disapproval (see DA Pam 25–1–1 for complete process).

(5) Fund command-unique IT requirements in support of mission and business, including long-haul communications, IA, and other IT requirements not identified as part of common-use IT or LandWarNet global network enterprise capability.

(6) Coordinate IT plans, programs, and requirements with appropriate information assurance managers in accordance with AR 25–2.

(7) Develop, manage, and maintain IT contingency plans, as prescribed by NETCOM, to ensure the uninterrupted execution of essential missions and functions under all conditions (see DA Pam 25–1–2).

(8) Obtain certificates of networthiness supported by the application Security Technical Implementation Guide (STIG), authority to operate, and AIC.

(9) Validate IP address requests from subordinates and ensure that only IP addresses registered by the Army through the procedures published by Army Cyber Command/Second U.S. Army are employed on networks within their purview.

(10) Develop AEA artifacts for respective command-unique functions and act as the integrator for any "system of systems" under their purview, as prescribed by the Army CIO (see DA Pam 25–1–1).

(11) Enforce DISR compliance for designated systems.

(12) Analyze and revise mission-related and administrative work processes necessary to complement pending, significant IT investments.

b. Enforce compliance with AR 25–400–2 to oversee and manage command records, in order to appropriately secure, maintain, and preserve such records throughout their life cycle.

c. Ensure that written contingency plans providing for effective withdrawal or destruction of records and equipment in hostile or unstable conditions are prepared by all commands and other elements in overseas areas not under the jurisdiction of a major overseas commander.

d. Conduct command-wide evaluations of records management programs relating to the adequacy of documentation, maintenance, use, and disposition of records at least once every 3 years.

e. Identify ISs and communication systems' functional requirements for Army military construction (MILCON) projects involving respective command missions.

f. Promote a paper-free business environment in the Army through optimum use of electronic business and electronic Government technologies.

g. Administer command-level IT performance measurements as prescribed by the Army CIO and CMO (see DA Pam 25–1–1 for more information).

h. Regardless of dollar value, Army organizations must use Computer Hardware, Enterprise Software and Solutions (CHESS) to purchase COTS products, including software, desktops, notebook computers, video teleconferencing equipment, and IT peripherals, unless CHESS grants a waiver to procure from an alternate source.

i. Develop and distribute command policy on the issuance of IT devices to employees in accordance with chapter 3 of this regulation.

2–17. Army service component command commanders

In addition to the duties listed in paragraph 2–16, ASCC commanders will—

a. Identify the command's IT requirements and ensure that mission requirements are validated, coordinated, integrated, and prioritized in accordance with AR 71–9. Collaborate with NETCOM, TRADOC, AMC, and FORSCOM to obtain command-unique IT requirements beyond common-use services.

b. Provide IT functional specifications, requirements, and relevant materiel-development systems and programs to ASA (ALT), DCS G–3/5/7, AMC, TRADOC, FORSCOM, Army Cyber Command/Second U.S. Army, and Army CIO/G–6.

c. Establish and maintain staff liaison capabilities with TRADOC, AMC, FORSCOM, INSCOM, and the U.S. Army Medical Command (MEDCOM), which recommend new or improved IT-related doctrine, force structure, training, and materiel.

d. Develop requirement documents and OV input, as needed, to support the respective organization's C2 plans and forward them to TRADOC.

e. Manage satellite communications (SATCOM) assets assigned to support ground mobile forces.

f. Integrate records management support into operational plans for the collection and transfer of records created by deployed units in contingency operations, in accordance with AR 25–400–2.

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

In addition to the duties listed in paragraph 2–16, the CG, TRADOC will—

a. In coordination with Army Cyber Command/Second U.S. Army, formulate IM and IT doctrine for the Army.

b. Serve as the Army Operational Executive Architect for the mission command segment. (See also chapter 6 of this publication.)

c. Ensure that IT solutions for warfighting requirements include an integrated user-training program, simulator, or simulations development plan as appropriate.

d. Provide electromagnetic spectrum impact consideration in the formulation of Army countermeasures, concepts, and doctrine.

e. Establish doctrine for IP addressing and use of IP-enabled systems and equipment for all levels of deployment and usage. Develop programs of instruction and conduct training on tactics, techniques, and procedures (TTP) associated with using IP-enabled systems in coordination with Army Cyber Command/Second U.S. Army and NETCOM.

f. Incorporate records management training in functional and major operating system-producing courses.

g. Ensure that the IT support for accession and recruiting missions reflects an enterprise approach.

h. Support the Army's configuration-control process for the Joint messaging standards implemented in the systems for which they are responsible. Provide support, as required, to the Army's representative to Joint configuration-control boards that configuration manage those same Joint messaging standards (see DA Pam 25–1–1 for more information).

i. Support Network Integration Evaluation (NIE) efforts as part of the agile process and decision-making on issues of network development and sustainment.

j. Provide a model- and simulation-supported analysis on priority network questions of the LandWarNet General Officer Steering Committee (GOSC). Analysis will be coordinated between all Army organizations performing formal modeling and simulation of components that comprise the Army's LandWarNet network enterprise.

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

In addition to the duties listed in paragraph 2–16, the CG, AMC will—

a. Provide functional support to the PEOs and PMs as designated by the Army acquisition executive.

b. Assist in the preparation, maintenance, and promulgation of the AEA.

c. Support the CIO/G–6 in executing the AIC test process and subsequent configuration management of the Army baseline.

d. Validate IS technical requirements and associated cost estimates for all Army MILCON projects, except for those projects specifically designated to U.S. Army FORSCOM.

e. Perform system engineering for the sustainment battlefield functional area of the command, control, and subordinate systems.

f. Resource and execute the AIC test activities as directed by and on behalf of the CIO/G–6.

g. Resource and execute configuration-management processes, as directed by the CIO/G–6, to maintain configuration control and data integrity of Army systems during the AIC test certification process; and to maintain interoperability over the Army fielded baselines.

h. Support the CIO/G–6 in the execution of the AIC test process by providing testers and configuration management personnel to execute AIC test events in compliance with CIO/G–6 policy and procedures.

i. Ensure that the Central Technical Support Facility staff assists with the synchronization of the FaNS AIC distributed environment, including to—

(1) Control and replicate the fielded and certified baseline for distribution.

(2) Provide system of systems engineering integration support.

(3) Provide and integrate Information Assurance Vulnerability Alert (IAVA) products.

j. Ensure the Army Contracting Command executes IT contracts in accordance with HQDA CIO/G–6 guidance, including to—

(1) Ensure that all software development contracts contain records management requirements. For examples of records management contract language, see http://www.archives.gov/.

(2) Ensure that all contracts are compliant with Section 508 of the Rehabilitation Act Amendments of 1998 (29 USC 794d).

(3) Ensure that all software development contracts are approved by the Army CIO/G–6.

(4) Ensure that all IT hardware acquisitions are Electronic Product Environmental Assessment Tool (EPEAT) registered and Energy Star qualified, in accordance with EO 13514; and that they meet the Environmental Protection Agency Energy Star and green requirements for energy efficiency per EO 12845.

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

In addition to the duties listed in paragraph 2–16, the CG, FORSCOM will—

a. Exercise operational control over NETCOM theater-level tactical signal brigades for global commitments.

b. Coordinate with the appropriate COMCAM organizations for current operations and training exercises.

2–21. Commanding General, U.S. Army Special Operations Command

In addition to the duties listed in paragraph 2–16, the CG, United States Army Special Operations Command will—

a. Comply with the United States Special Operations Command (USSOCOM) direction for management of information resources within the special operations forces information enterprise, as an Army component command under the operational control of USSOCOM.

b. Comply with USSOCOM direction for operational, administrative, and technical control of IT resources funded, developed, or procured through Major Force Program 11 funds.

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

In addition to the duties listed in paragraph 2–16, The Surgeon General/CG, MEDCOM will—

a. Provide IT-related combat and materiel development requirements, and data supporting military medical operations, to TRADOC, AMC, FORSCOM, and Army CIO/G–6.

b. Enforce compliance with 2 USC Subtitle F (The Health Insurance Portability and Accountability Act (HIPAA) of 1996) for the protection of health information, to include specific security measures required to support HIPAA standards.

2–23. Commanding General, U.S. Army Corps of Engineers

In addition to the duties listed in paragraph 2–16, the CG, USACE will—

a. Manage the "usace.army.mil" Internet domain and the assignment of sub-domains on CorpsNet.

b. Oversee organizations that operate and maintain portions of the CorpsNet (that is, the systems and networks that constitute the CorpsNet), which is a separate network on the DISA GIG. Although a separate network, CorpsNet IM capabilities are prescribed by the Army CIO/G–6 and Army Cyber Command/Second U.S. Army, and are executed by the USACE. This includes exercising technical authority and configuration management authority for CorpsNet systems and functional processing centers. Provide guidelines and direction for CorpsNet IT configuration management.

c. Implement an IT architecture incorporating all engineering functions that require interface between the Civil Works Program, the Army MILCON program and implementation, and management of common assets.

d. Coordinate the documentation of data standards for MILCON and Corps of Engineers' Civil Works Program data elements.

e. Coordinate planning, designs, and contract negotiations of the technical and functional requirements of ISs and communications systems for all Army MILCON projects.

2–24. Chief, Army Reserve

The Chief, Army Reserve will have the same responsibilities as specified in paragraphs 2–14*a*, 2–14*c*, and 2–16. In addition to these responsibilities, the Chief, Army Reserve will—

a. Manage the "USAR.army.mil" Internet domain and the assignment of sub-domains requested by other USAR organizations on ARNet II.

b. Oversee organizations that operate and maintain portions of the ARNet II (that is, the systems and networks that constitute the ARNet II).

2–25. Chief, National Guard Bureau

The CNGB serves as the channel of communications and collaborations between the Department of the Army and the several States on all matters pertaining to the National Guard and the Army National Guard (ARNG) of the United States. The CNGB will have the same responsibilities as specified in paragraphs 2–14*a*, 2–14*c*, and 2–16 and will perform these duties as required by the Army CIO/G–6; CG, Army Cyber Command; CG, NETCOM; adjutants general of the several States and territories; and the CG of the District of Columbia. The CNGB will—

a. Designate the Director, ARNG as the lead agent for GuardNet.

b. Oversee organizations that operate and maintain GuardNet, a separate network providing LandWarNet services from the States, territories, and the District of Columbia (collectively referred to as States) that comprise the ARNG to the DISA GIG. This includes, but is not limited to—

(1) Plan, program, and provide support capabilities and resources to NGB and Joint Forces Headquarters (JFHQ)-State IT and IM service and support requirements.

(2) Execute technical authority and configuration-management authority for GuardNet, systems, and functional processing centers, providing guidelines and direction for GuardNet IT configuration management as prescribed by Army Cyber Command and NETCOM.

(3) Execute all infrastructure-management activities, policies, processes, procedures, and protocols for the management of networks, telecommunications, facilities, data storage, IT and IM services continuity, and distributed computing operating within GuardNet as prescribed by Army Cyber Command and NETCOM.

(4) Provide technical and administrative guidance, direction, and resources to the JFHQ–States who assume direct responsibility for communications and IT and IM services operating within their State boundaries.

(5) Execute Army National Guard leases of communications, capabilities, and services and ensure that such services conform to NGB, Army CIO/G–6, Army Cyber Command, and NETCOM guidance in collaboration with the JFHQ–States where applicable.

(6) Formulate, manage, support, and approve ARNG military communications as well as IT and IM exchange agreements between the United States Army, other Joint Services, JFHQ–States, and State government and first-response agencies in collaboration with the JFHQ–States, where applicable.

(7) Manage GuardNet-specific, system-to-system interfaces between the States and the Department of the Army in collaboration with the JFHQ–States, where applicable, and as prescribed by Army Cyber Command and NETCOM.

(8) Collaborate with the JFHQ–States or the National Capital Region directors of information management (DOIMs) who are responsible for NEC-like responsibilities, as outlined in this regulation, for their respective States or the National Capital Region.

(9) Manage NGB-specific Internet domains and the assignment of sub-domains requested through ARNG on behalf of NGB and supported organizations as prescribed by Army Cyber Command and NETCOM.

2–26. Commanding General, U.S. Army Test and Evaluation Command

The CG, USATEC will support system acquisition, force development and experimentation processes through overall

management of the Army's T&E programs. USATEC is the Army's independent operational test activity and reports directly to the Vice Chief of Staff, U.S. Army through the Director of the Army Staff. The CG, USATEC, will perform responsibilities and duties as assigned in AR 73–1.

a. Serve as the principal developmental and operational test agency for Army enterprise systems and lead for evaluation of Army enterprise and information systems.

b. Support the CIO/G–6 in the assessment of network interoperability certification. Provide accredited test performance data for Army enterprise and information systems under consideration for Army acquisition.

2–27. Commanders or directors of major subordinate commands; field-operating agencies; and separately authorized activities, tenant, and satellite organizations

Based upon guidance from their parent organization, commanders or directors of major subordinate commands (MSCs); field-operating agencies (FOAs); and separately authorized activities, tenant, and satellite organizations will accomplish the same IM responsibilities as their parent organization, commensurate with their respective mission, size, responsibility, and location. In addition to the duties listed in paragraph 2–16, these commanders will—

a. Establish a senior IM official responsible for implementing the command's IM and IT program, in accordance with IM and IT policies as prescribed by the Army CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute LandWarNet global network enterprise activities as prescribed by Army Cyber Command/Second U.S. Army.

b. At a minimum, FOAs and other organizations will—

(1) Establish or appoint an IM office or officer to plan or supervise the execution of IM.

(2) Coordinate with the relevant NEC for common-use IT services.

(3) Designate in writing a subordinate organization records manager (RM), who will perform duties as described in AR 25–400–2, DA Pam 25–403, and DA Memo 25–51.

2–28. Joint Force Headquarters-State, U.S. Army Reserve Command, or comparable-level community commanders

In addition to the duties listed in paragraph 2–16, Joint Force Headquarters-State, U.S. Army Reserve Command (USARC), or comparable-level community commanders will—

a. Establish a senior IM official responsible for implementing the command's IM and IT program, in accordance with IM and IT policies as prescribed by the Army CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute LandWarNet global network enterprise activities as prescribed by NETCOM. The senior IM official NEC will—

(1) Perform voice and data network-management functions for the installation or assigned geographical boundary, to include installation, operations and maintenance, and configuration management of common user component devices.

(2) Determine procedures for enforcing standards view architecture compliance on a single installation or assigned geographical area.

(3) Design or acquire systems within the constraints of the AEA.

(4) Appoint a frequency manager to coordinate, plan, program, manage, and supervise frequency management responsibilities.

(5) Provide oversight and management of the installation's participation in the Army's IT Metrics Program.

(6) Perform IA functions in accordance with AR 25–2.

(7) Perform functions as the single authority to validate the purchase of IT items on the installation, in accordance with IM and IT policies as prescribed by the Army CIO.

b. Coordinate with NETCOM for common use IT common services. JFHQ–States will coordinate with the ARNG Network Operations and Security Center.

c. Provide non-tactical VI documentation (VIDOC) support within VI activity capabilities and request additional support through the NEC VI manager when local capabilities cannot meet requirements.

d. Coordinate with the NEC when moving to an active Army installation.

e. Ensure that fielded systems are networthy and AEA compliant.

2–29. Program executive officers and direct-reporting product managers

PEOs and direct-reporting product managers will—

a. Develop AEA architectures for assigned systems in coordination with CIO/G–6 and consistent with DOD guidance.

b. Develop and coordinate architecture data as input to architectures under their purview.

c. Develop and submit information support plans in accordance with DOD guidance at http://jitc.fhu.disa.mil/jitc_dri/jitc.html/. (See DA Pam 25–1–1.)

d. Ensure that all fielded systems are logistically supportable during the life cycle of the system and follow integrated logistics support (ILS) responsibilities in accordance with AR 700–127.

e. Prepare the Exhibit 300 business case(s) for systems as applicable for submission with the IT budget in accordance with OMB Circular A–11.

f. Submit all defense business systems with a total cost in excess of $1 million (over the period of the current future-years defense program submitted to Congress) for review by the appropriate Investment Review Board and certification approval by the Defense Business System Management Committee (DBSMC) (see 10 USC 2222).

g. Ensure records management requirements are included in office operations and systems throughout their life cycle.

h. Design, build, test, and field IP-enabled IT and NSSs to efficiently use IP address space. Coordinate materiel solution IP address space requirements with TRADOC and NETCOM as required. Request IP addresses to support materiel solutions in accordance with procedures published by NETCOM.

i. Ensure compliance with IA C&A requirements, the Army Networthiness Program, and AEA for all PM-developed IT systems.

j. Ensure that compliance with DOD policy regarding accelerated use of COTS IT and NSS by establishing a baseline and documenting progress in this effort.

k. Comply with AIC policy (chap 6), configuration-management procedures, and resource adequately for systems to undergo AIC testing (see DA Pam 25–1–1).

l. Support the Army's configuration control process for the Joint messaging standards that are implemented in the systems for which they are responsible. Provide support, as required, to the Army's representative to the Joint-configuration control boards that manage the configurations for these same Joint-messaging standards.

m. Ensure that all installation-level IT infrastructure requirements (outside cable plant connectivity, campus area switching upgrades, and so forth) needed to support a specific product, program, or system fielding on Army posts, camps, and stations are validated and prioritized by NETCOM and approved by Army CIO/G–6 prior to implementation (SAIS–AOI). (See DA Pam 25–1–1 for complete process.)

n. Provide IT functional specifications, requirements, and relevant development systems and programs with ATEC to establish & maintain RDT&E capabilities.

o. Adhere to the platform requirements as specified in the COE architecture and information sharing requirements specified in the AIA.

2–30. Program, project, and product managers and information technology materiel developers

Program, project, and product managers and IT materiel developers (MATDEVs) will—

a. Implement applicable AEA guidance as related to their assigned program. The PM will—

(1) Develop architecture views and products for the systems being acquired to comply with CJCSI 6212.01.

(2) Develop and acquire technical support solutions and ensure that they are within the constraints of the AEA.

(3) Coordinate AEA architectures for their systems with the program executive office (PEO) and the management official of gaining commands and installations (not applicable to weapons platforms).

(4) Use the DISR online tool at https://disronline.csd.disa.mil/ to build standards views.

(5) Coordinate their systems architecture with Army Architecture Integration Center prior to fielding systems. For more information, see DA Pam 25–1–1.

(6) Program for resources required to develop architectures and architecture products for assigned systems.

(7) Program for resources required to perform accreditation and interoperability testing for integration with existing systems.

(8) Identify bandwidth requirements to support program and collaborate with NETCOM for bandwidth support.

b. Coordinate fielding plans for their systems with senior IM officials of gaining commands and installation NECs to ensure compatibility with existing systems and IT support structure.

c. Develop and submit information support plans in accordance with DOD guidance at http://jitc.fhu.disa.mil/jitc_dri/jitc.html/. For more information, see DA Pam 25–1–1.

d. Ensure that all fielded systems are logistically supportable during the life cycle of the system and follow ILS responsibilities in accordance with AR 700–127.

e. Ensure that records management requirements are included in systems throughout their life cycle in accordance with AR 25–400–2.

f. Develop and prepare Exhibit 300 business case(s) for systems as applicable for submission with the IT budget in accordance with OMB Circular A–11 (not applicable to weapons platforms).

g. Submit all defense business systems with a total cost in excess of $1 million (over the period of the current future year defense program submitted to Congress) for review by the appropriate Investment Review Board and certification approval by the DBSMC (see 10 USC 2222). This requirement does not apply to tactical systems.

h. Design, build, test, and field IP-enabled IT and NSSs to efficiently use IP address space. Coordinate materiel solution IP address space requirements with TRADOC and NETCOM as required. Request IP addresses to support materiel solution in accordance with procedures published by NETCOM.

i. Ensure compliance with IA C&A requirements, the Army's Networthiness Program, and AEA for all PM-developed IT systems.

j. Comply with AIC policy (chap 6), configuration-management procedures, and resource adequately for systems to undergo AIC testing (see DA Pam 25–1–1).

k. Act as the systems engineer, technical integrator, and materiel developer for assigned ISs.

l. Ensure that IT materiel testing, acquisition, and support comply with Joint, NATO, and the American, British, Canadian, Australian (Quadripartite) armies' operations, standardization, and interoperability agreements; and Federal and international standards.

m. Plan, program, and conduct new equipment training for assigned systems and recommend required training for inclusion in their Army schools programs.

n. Provide input and trade-off analysis to TRADOC as required for developing the warfighting OV.

o. Ensure software testing is compliant with the requirements found in AR 70–1.

p. Adhere to the platform requirements as specified in the COE architecture and information sharing requirements specified in the AIA.

2–31. Information management organizations below Headquarters, Department of the Army level

a. Subordinate organizations below HQDA, except as indicated below, may at their discretion designate a senior IM official and establish supporting offices within their organization. Regardless of designation, all IM organizations will comply with governing legislation; Federal, DOD, and Secretary of the Army guidance; and the appropriate responsibilities delineated in chapter 2 and elsewhere in this regulation (see also DA Pam 25–1–1). The ARNG will comply with Defense Appropriations Bill 1997, Senate Report 104–286. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute LandWarNet global enterprise network activities as prescribed by NETCOM. Every ACOM and ASCC will appoint a senior IM official as a principal staff officer. DRUs may appoint a senior IM official as a principal staff officer if required and designated in writing by the respective HQDA official. MSCs may appoint an equivalent IM official with similar staff responsibilities as an ACOM's or ASCC's senior IM official. Senior IM officials will—

(1) Perform voice and data network-management functions for the installation or assigned geographical boundary, including installation, operations and maintenance, and configuration management of common user component devices.

(2) Determine procedures for enforcing standards view architecture compliance on a single installation or assigned geographical area.

(3) Design or acquire systems within constraints of the AEA.

(4) Appoint a frequency manager, if required, to coordinate, plan, program, manage, and supervise frequency management responsibilities.

(5) Provide oversight and management for the installation's participation in the Army's IT Metrics Program.

(6) Perform IA functions in accordance with AR 25–2.

(7) Perform functions as the single authority to validate the purchase of IT items on the installation, in accordance with IM and IT policies as prescribed by the Army CIO.

b. The Army Cyber Command operates, maintains, and secures Army global network operations via their theater signal commands. Subordinate brigades, battalions, and NECs comprise the IM and IT command, control, and operational structure across all theaters and on all Army installations. Their responsibilities include the following:

(1) Provide quality common-user IM and IT baseline services to Army organizations at the highest possible level, commensurate with resourcing as defined in the approved-services list.

(2) Provide quality mission level and enhanced IM and IT services to installation customers on a reimbursable basis as documented in the approved service level agreements (SLAs).

(3) Oversee shared and common-user IT systems within their assigned area of responsibility and provide technical oversight for the IT services provided.

(4) Develop MOAs and SLAs to document the above-baseline, customer-and-service-provider expectations, and to ensure successful conduct of the full spectrum of the theater IM and IT mission.

(5) Implement and enforce Army-level IM and IT policies, standards, architectures, programs, plans, and portfolio management and budgets for common-user concerns within their assigned regions.

(6) Prescribe to Signal Command (Theater) NECs implementing processes and procedures for reviewing and issuing technical validation certification for IT non-service requirements that will be connected to the LandWarNet.

(7) Implement the tenets of the LandWarNet strategy, transitioning service delivery, management, and oversight from local-level provisioning to enterprise operations as capabilities evolve.

(8) Identify and consolidate theater IM and IT requirements; ensure that these requirements are validated, coordinated, and integrated in accordance with AR 70–1.

(9) Maintain network security C&A documentation for the common-user network and systems under their purview, and exercise visibility of C&A documentation for mission systems and services operating in or on respective areas of responsibility. (See AR 25–2 and associated IA Best Business Practices.)

(10) Ensure that current contingency plans providing for effective withdrawal or destruction of records in hostile or unstable conditions are prepared by all installations, including any element in an overseas area not under the jurisdiction of a major overseas commander. (See AR 25–2 and associated IA Best Business Practices.)

(11) Collaborate with the appropriate theater network operations and security centers (TNOSCs) to achieve situational awareness for all supported units to include deploying force units. ARNG Title 10 and Title 32 personnel will collaborate with the ARNG NOSC.

(12) Implement an inspection program to verify the service provider's compliance with requisite policies, MOAs, and SLAs, and to assess customer satisfaction with the services provided.

(13) Maintain a uniform set of IT performance metrics and report to the Army IT Metrics Program as required.

(14) Review and validate all NEC management decision evaluation package funding and re-programming actions in the theater to ensure equitable distribution and resourcing of C4/IT.

(15) Develop and publish service costing model for service delivery at local levels.

(16) Manage all coordination and connections to long-haul IT services.

(17) Serve as the on-installation entry point for all installation-level IT infrastructure requirements (outside cable plant connectivity, campus area switching upgrades, and so forth).

c. The NEC is designated as the IM and IT manager on Army posts, camps, and stations, and is the single authority for providing common-user IT services in accordance with the C4IM Services List. There is only one NEC (operation) at an installation and a single NEC at USARC. The NEC is the initial focal point for tenant organizations and activities to obtain support for unique IT services that are listed as "mission resourced," enhanced level of common-user services, or required services that simply are not listed in the C4IM Services List and customer-facing catalog.

(1) NECs are assigned or designated by the theater signal command in coordination with garrison commanders on IMCOM installations.

(2) The National Guard Joint Force Headquarters-State is equivalent to an installation for purposes of providing IT support (see para 2–25).

(3) Conduct the necessary site-centric analysis to ensure the new system or capability will not adversely impact their respective installation networks.

(4) Ensure that all systems have received a certificate of networthiness prior to allowing them to field or connect within their respective networks.

(5) Support NETCOM in the networthiness certification process by identifying specific issues and recommendations for overcoming the obstacles to achieving a certificate of networthiness.

(6) Ensure that a thorough code review is performed as part of the development process for all NEC or locally developed software and applications.

(7) Ensure that IT requests and requirements are—

(a) Accompanied by requisite documentation (see DA Pam 25–1–1).

(b) Valid from an installation perspective.

(c) Submitted to NETCOM for validation through their theater signal command to the Army CIO/G–6 for ultimate approval or disapproval.

(8) The USAR secures particular services via the C4IM Services List from installation NECs; however, due to their mission, the USAR provides all data-related and IA-related services to USAR locations via the Army Reserve Network.

d. Tenant commands, satellite organizations, separately authorized activities, Government-owned and contractor-operated facilities, regional support activities, U.S. Army Reserve (USAR) regional support commands, FOAs, and major staff entities will not establish a NEC but will have an IMO appointed on official orders to coordinate internal IT services with the appropriate NEC. The IMO will identify their organization's information requirements to the designated NEC, as directed by the appropriate theater signal command to identify a NEC to provide the IT support. The IMO is the primary interface between the NEC and the supported organization(s). Where no post, camp, or station installation configuration exists, the host command or activity will coordinate IT services with the respective theater signal command. See DA Pam 25–1–1 for a detailed list of responsibilities. For the USAR, only the USAR NEC may negotiate with or coordinate with the theater signal command.

Chapter 3
Army Information Technology Management

3–1. General

The Army's ITM approach is one that follows a recurring life cycle of planning, investment, and execution. The cycle begins once capability gaps or requirements are identified. These gaps are based on emerging guidance or legislation. This approach applies to all IT.

3–2. Planning phase

The planning phase is where the problem statement, IT transformational plans, and hardware and software authorization architectures are developed and gaps are identified.

a. Transformation plan. All commands, DRUs, and functional proponents for generating force enterprise activities will develop and publish an annual IT transformation plan that is submitted to OBT and the CIO/G–6 in January of each year. The transformation plan will include—

(1) Organizational vision, core missions, and alignment with Army strategic plans.

(2) Goals and objectives.

(3) IT baseline and the current situation.

(4) Evaluation of needs.

(5) Resource summary.

(6) Key metrics, timelines, and milestones to track IT transformation.

(7) Mitigation strategy for redundancies, gaps, risks, and performance issues.

b. Commercial off-the-shelf information technology authorization architecture. COTS IT refers to commercially developed hardware or software that provides the common-user infrastructure used to generate force activities in the continental United States (CONUS) or in a forward-deployed environment. TRADOC develops the minimum mission-essential COTS IT capabilities to develop a sustainable life-cycle strategy and to achieve assigned, full-spectrum operations. COTS IT will be included in an appropriate modified table of organization and equipment, a table of organization and equipment (TOE), and a table of distribution and allowances (TDA) documentation. Network equipment, including routers, hubs, and switches—and enterprise services, servers, and server software—will not be a part of the COTS IT authorization architecture. However, these items are included in LandWarNet architecture and will be included in concept plans.

c. Managing the planning phase. Command senior IM officials will manage the organization's implementation of the Army's IT investment strategy, IT infrastructure changes, acquisition strategy, and IA prerequisites. This responsibility should not be delegated to subordinate command, senior IM officials.

3–3. Investment phase

The investment phase is where the resource requirements are identified, business cases are developed, and solution analysis is completed.

a. Local IT approval authorities will be designated by all Army components, ACOMs, ASCCs, DRUs, and functional proponents.

b. There is no standard life cycle replacement. Hardware or software that is a part of the COTS IT authorization architecture can be replaced when equipment is broken or otherwise unusable. A 5-year life cycle will be used for planning and budgeting purposes.

c. Command senior IM officials will conduct a portfolio review before approving new technical solutions to avoid redundancy and promote standardization. To retain IT that duplicates a service provided by the enterprise, organizations must provide a complete business case and submit it to the DA for approval. This responsibility should not to be delegated to subordinate command, senior IM officials. Guidance on implementation is available on AKO at https://www.us.army.mil/suite/page/603932/.

d. All Army organizations must analyze their missions and revise their mission-related and administrative work processes, as appropriate, before making significant IT investments in support of these processes. A governance process will be instituted locally; however, IT investments will not be approved at local levels unless they can show the investment will provide measurable improvements in mission performance. Any investment that provides a new capability, significant modernization, or duplicates an enterprise solution will have a well-documented business case to support the investment. The submitted business case must include—

(1) Doctrine, organization, training, materiel, leadership and education, personnel, facilities, and cost.

(2) Business process reengineering assessment.

(3) Analysis of alternatives.

e. Business case templates are located on AKO at https://www.us.army.mil/suite/page/603932.

3–4. Execution phase

During the execution phase, the solution is acquired and implemented in accordance with the business case, and ongoing reviews are completed via established governance to ensure both milestones and expected results are realized.

a. Centralized information technology contracts. CHESS is the primary source for establishing commercial IT contracts for hardware, software, and services (not applicable to IT hardware or software embedded in weapons platforms). The use of CHESS contract offerings will make purchasing more efficient and reduce costs through volume buying. CHESS simplifies and centralizes IT life-cycle management throughout the Army enterprise. More information on CHESS can be obtained at https://chess.army.mil.

(1) Regardless of dollar value or financial appropriation, Army organizations must procure COTS IT software and

hardware from CHESS, including desktop and notebook computers, video teleconferencing equipment, routers, servers, printers, and so forth. The purchase of IT hardware and software from a non-CHESS vendor requires a waiver from CHESS. All waiver requests must include a rationale explaining the extenuating circumstances or unique configurations required by the mission and not available through CHESS. The CHESS contract vehicles and electronic market (e-mart), are available at https://chess.army.mil/ascp/commerce/index.jsp/. Requests for waivers may be submitted through the CHESS Web site at https://chess.army.mil/. JFHQ–States are permitted to use cooperative agreements in lieu of CHESS.

(2) Regardless of the dollar value or financial appropriation, when no small business capability exists, CHESS contract vehicles are the preferred source for acquisition of IT services.

(3) CHESS, in conjunction with the Army Contracting Command's designated offices, will conduct semiannual consolidated buys (CBs) for desktop and notebook computers. Organizations shall use the CB to satisfy their desktop and notebook requirements to the maximum extent possible. Exceptions for mission-critical requirements, non-CB configurations, and mandatory OCONUS host-country agreements may be requested in accordance with the procedures on the CHESS Web site.

(4) In the event CHESS cannot support an organization's requirement, the office will notify the acquiring organization that other DOD and Federal activity contracts will be considered to satisfy their documented requirements.

b. Non-information technology programmed funds. Submit a request for CIO (Goal 1) waivers for all IT expenditures using non-IT programmed funds when said expenditures exceed the dollar thresholds of $25,000 operations and maintenance; Army funds; and $100,000 research, development, test, and evaluation funds, as published in the annual resource guidance. Non-IT programmed dollars will not be spent on IT requirements without a CIO waiver. For more information, see DA Pam 25–1–1.

c. Governance. The Army IT enterprise governance framework establishes a decision-enabling framework that directs and controls enterprise IT and assigns accountability to support the Army mission. The Army IT enterprise governance forums support transformation efforts by providing the mechanism that ensures the Army CIO/G–6 has visibility and oversight throughout the entire life cycle to govern the IT enterprise. Forums are in place to quickly adjudicate any issues that arise and elevate only as needed. The current governance framework can be found on the Army CIO/G–6 Governance Wiki page at https://www.kc.army.mil/.

d. Information technology capital asset management.

(1) All IT investments will be managed as part of the Army's IT portfolio. All IT will be accounted for in APMS, the Army's authoritative data source for IT. Information on registration criteria can be found at appendix B. Commands are responsible for ensuring system owners validate and update their data in APMS as required, on a daily, weekly, monthly, or quarterly basis. The review and validations of specific functional areas will be performed on a quarterly basis. FISMA data is entered as required and is not tied to a quarterly update.

(2) Defense Business System (DBS) (as defined in 10 USC 2222(j)) certifications are required for any business-system program that will have a total expected cost, regardless of fund source for acquisition, modernization, or sustainment, in excess of $1 million over the period of the current future-years defense program submitted to Congress under 10 USC 2221, and is independent of MA alignment. This process is started using APMS. An obligation of DOD funds (appropriated or non-appropriated) for a business-system program of more than $1 million, which has not been certified and approved by the DBSMC, is a violation of 31 USC 1341 (The Anti-Deficiency Act). IT that supports generating force functions as outlined in field manual (FM) 1–01, or performs functions that can be mapped to the BEA, is considered DBS (even if used in the operational environment). Information on DBS certifications can be found under the Investment Review Boards Products at http://www.bta.mil/.

(3) The capital planning and investment management (CPIM) process includes selecting the IT investments and establishing their priorities throughout the PPBE and acquisition processes. CPIM addresses capability gaps, investment risks, and IT interdependencies across multiple areas of IT investments. The CPIM process and resulting C4/IT investment strategy are approved by the CIO/G–6; briefed to respective program evaluation groups; and used to determine the selection of C4/IT investments and whether to continue, modify, or terminate a C4/IT program or project in accordance with the CCA.

(4) The CIO will issue an annual guidance memorandum in order to identify key investment IT capabilities that the Army will strategically invest in with their next fiscal year (FY) dollars. Those selective issues that cannot be funded within the resources of a single program evaluation group may be taken to the next level of the PPBE process.

(5) Army components, ACOMs, ASCCs, DRUs, and functional proponents (domains) will—

(a) Ensure that IT investment items, including all networks, are registered in APMS by the system owner.

(b) Review their portfolios for redundancies and gaps, risk, environmental impact, and strategic alignment annually. Mitigation strategies will be included in transformation plans. IT investment reviews will focus on capabilities and include the full life-cycle costs of IT expenditures.

(c) Appoint leads to perform portfolio-management responsibilities.

(d) Ensure system owners comply with required data calls and maintain accurate system records. Progress will be reviewed and reported bi-annually through the governance structure.

(6) HQDA proponents, ACOMs, ASCCs, PEOs, and other organizations will ensure that all businesses or nontactical or platform systems that support generating force activities IT systems are Web-enabled and linked to the enterprise portal. If not, they will receive a waiver from the CIO/G–6.

e. Information technology performance measurements. Measuring IT performance is the process of assessing transformational change, as well as the effectiveness and efficiency of IT in support of achieving an organization's missions, goals, and quantitative objectives through the application of outcome-based, measurable, and quantifiable criteria compared to an established baseline. Performance measures will be developed for each organizational C4/IT initiative and investment before execution or fielding.

(1) The performance measures will determine the value-added contribution of the IT initiative or IT investment to missions, goals, and objectives; and provide a clear basis for assessing accomplishments, aiding decisionmaking, and assigning accountability at each management level. These measures will directly support the metrics used in the Strategic Management System, the Army's IT Metrics Program, or other defined programs.

(2) The Army's IT Metrics Program establishes the use of metrics to assess the status of the IT infrastructure and to evaluate its support to mission accomplishment. Installation information managers are required to collect, compile, and report IT data on a quarterly basis via the IT metrics database at https://www.itmetrics.hua.army.mil. For additional information, see DA Pam 25–1–1.

f. Element of resource codes. When obligating funds for IT resources, the element-of-resource codes must be specified in the obligation documentation from the list of approved elements of resource (see DA Pam 25–1–1).

g. Minimize employee information technology devices. Issuing employee IT devices (for example, desktops, laptops, cellular phones, smart phones, or tablet computers) is a command responsibility. Issuance will be based on the mission and assigned position, rather than grade or rank of the individual. The number of devices should be minimized per employee and be the least amount required for the assigned mission, in accordance with EO 13589.

h. Information system security documentation. FISMA (44 USC Chapter 35) mandates that the security status of Army ISs be documented, updated, and verified at least annually. APMS will be used to implement this requirement.

i. Accelerated use of commercial off-the-shelf products and services. The CCA and other Federal policies, laws, and directives require the maximum use of COTS and non-developmental item products and services. DODD 5000.1 identifies the DOD order of preference in capability acquisition. The first order of preference is the procurement or modification of commercially available products, services, and technologies from domestic or international sources, or the development of dual-use technologies.

(1) To ensure compliance with the above policies, each system PEO or acquiring organization will establish and report a baseline of its commercial IT and NSS software assets, non-commercial IT and NSS software assets, commercial IT and NSS services, and noncommercial IT and NSS services in APMS. The baseline will be developed and maintained at the system or program level, and at a component summary level. The baseline will be reported to the MA domain owner, and it will enable Army leaders and managers to determine the current status of commercial IT and NSS software and services, plan for increasing their use, and measure progress toward achieving the DOD goal.

(2) To ensure accountability for accelerating the use of commercial solutions in DOD, and to obtain senior leadership visibility into the progress towards achieving this goal, each PEO or acquiring organization must annually confirm that its system is in compliance with the above and report the results achieved toward meeting the goal of increasing the use of commercial IT and NSS in the Army.

(3) Acquisition program dollars will not be used to fund IT services that are defined as baseline in the most current version of the Army-approved C4IM Services List.

j. Department of Defense-provided processing services. DOD-provided centralized information processing services (for example, DISA's Defense Enterprise Computing Centers) are available to all military departments and services on a fee-for-service basis.

(1) Fee-for-service rates will be coordinated among the requesting organization, NETCOM, and the DOD service providers. NETCOM will help Army activities resolve issues that involve the provisioning of, and funding for, services from DOD providers.

(2) Coordination is required with the supporting NEC in determining requirements for centralized processing services. Installation requirements will be integrated and coordinated with the DOD service provider on behalf of all activities within their supported area. (See DODI 4000.19 for procedures on service parameters and estimating annual fees.)

(3) All software, firmware, system, or Web services using the LandWarNet must obtain networthiness certification (see para 6–8 of this regulation, and DA Pam 25–1–1).

k. Consolidating Army data centers. The purpose of the Army Data Center Consolidation Plan (ADCCP) is to enhance performance, improve information security, and increase fiscal and operational efficiencies. The Army will close data centers by buying enterprise hosting as a managed service, with a long-term goal of decreasing the Army's IT infrastructure and application inventory. The Army will maintain a limited number of data centers to support local installation services only as required; these data centers will be the exception. The ADCCP will leverage the Army CIO governance boards and the LandWarNet Mission Command GOSC for governance. The Enterprise Guidance Board will address IT enterprise, service-related decisions as stipulated in its charter.

(1) ADCCP applies to all ACOMs; ASCCs; DRUs; Army staff, including FOAs; data center owners; application owners; and IT portfolio and domain leads, whether or not they own or operate a data center. For additional information, go to the ADCCP homepage at https://www.us.army.mil/suite/page/643748/.

(2) Consistent with the ADCCP, the Secretary of the Army issued a directive expanding the scope of the moratorium on IT spending. Voice switches and IT equipment, including servers, racks, storage area network storage, matrix switches, optical storage systems, tape drive and storage devices, high-speed printers, mainframe computers, and mini computers will not be procured. Hosting facilities will not be constructed or renovated without a waiver granted in advance by the CIO/G–6. Details on obtaining a waiver and the requirements for waiver submission can be obtained from the DA Pam 25–1–1.

l. Enterprise software licenses.

(1) The Defense Federal Acquisition Regulation Supplement (DFARs), subpart 208.74, which details the enterprise software agreement, requires DOD components to fulfill requirements for commercial software and related services such as software maintenance in accordance with the DOD Enterprise Software Initiative (ESI). This includes purchasing from the DOD inventory before using any other source. DOD enterprise software agreements (ESAs), negotiated with specific software publishers or their agents, provide the best available prices, terms, and conditions. Organizations should consult with CHESS, the Army representative to the DOD ESI, before re-negotiating any of the terms or conditions of an ESA. The DOD ESI is the DOD implementation of the Federal-wide Software Managed and Acquired on the Right Terms (SmartBUY) program. ESAs that have been designated as SmartBUY agreements are mandatory for use when requirements evaluation has led to the designated brand name software product or service. SmartBUY and other ESI policies are available on the CHESS Web site at https://www.chess.army.mil.

(2) An enterprise license agreement (ELA) is an IT license or an ESA that has been required and validated by two or more ACOMs or Army staff elements, and whose designation as an enterprise asset would lead to economies of procurement at sufficient levels to warrant consolidation of the license or service with the CIO in conjunction with contract support provided by the Army Contracting Command-designated offices and programmatic support from CHESS. The CIO is the decision authority for enterprise license agreements. The evaluation authority for enterprise designation processes resides within the CIO/G–6 Chief Integration Office and supported by CIO/G–6 Architecture, Operations, Networks and Space directorate, Army Contracting Command-designated offices, the Project Director CHESS, and the Program Executive Office for Enterprise Information Systems. An ELA is a license that applies to the entire Army. The license is acquired and the software distributed through a centrally managed process. An ELA is the single source for Army organizations to obtain specified products. CHESS is the Army's designated software product manager and the exclusive source for all software through the ELAs, as well as for CBs for licenses that do not apply to the entire Army enterprise but to groups of customers consolidating their requirements to obtain more favorable prices, terms, and conditions.

(3) Before entering into an agreement with any COTS vendor, Army organizations (including contractors purchasing IT intended for use by Army organizations) will coordinate acquisition plans with the NEC. The NEC will coordinate with the CHESS office regarding planned acquisition of specific products. If the existing ESA does not contain the desired terms and conditions or prices, the NEC must notify CHESS, the Army's ESA manager. CHESS may determine the most cost-effective method for obtaining the licensing for the NEC, such as improving the existing ESA or establishing a new agreement. CHESS is responsible for authorizing new ESA agreements and granting waivers for organizations to acquire any COTS software from other sources, regardless of whether a product is in an ESI agreement. The CHESS Web site is https://chess.army.mil. The DOD ESI Web site, which lists all ESI-managed software, is located at http://www.esi.mil.

(4) Users will not install software, including new software packages, software upgrades, free software, freeware, shareware, and unlicensed open source software without the approval of the applicable DAA as captured in the DAA repository. Only open-source software that is copyrighted and distributed under a license may be used to support Army mission requirements. Army organizations acquiring, using, or developing open-source systems must comply with all lawful licensing requirements and ensure that the application complies with the same Army and DOD policies that govern COTS and Government off-the-shelf software.

m. Leasing information technology assets. Requirements for leasing hardware and software will be handled using the same approval and validation procedures as other acquisition strategies. Activities will use the total life-cycle leasing cost estimates to determine the required level of approval. Requests for leases will be validated in the same manner as the NEC validation of other acquisitions. For more information, see DA Pam 25–1–1.

n. Purchase of energy-efficient computer equipment. All purchases of microcomputers, including the personal computer (PC), monitors, printers, and other peripheral equipment, will meet the requirements of the Environmental Protection Agency Energy Star and EPEAT, and the green requirements for energy efficiency within EO 12845 and EO 13514. EO 13423 requires Federal agencies to ensure that at least 95 percent of their annual acquisitions of electronic products are EPEAT-registered electronic products, unless there is no EPEAT standard for such products. See paragraph 7–10 of this publication for IT equipment energy-conservation guidelines and AR 420–1 for Army facility energy-management requirements.

o. Modifications. Software applications, whether combined with hardware or as separate end items, are subject to the same procedures regarding modifications as other IT. Software applications that are approved for standardized use

across multiple commands will have one configuration manager assigned by AMC. The configuration manager will establish and publish procedures that identify which organizations are using the application, track when an organization discontinues use, and let users recommend required, post-production software support (PPSS) changes and enhancements. The Army Systems Architect (ASA (ALT)) must approve the cancellation of PPSS for any software application approved for standardized use.

p. Information technology and national security systems acquisition process. The acquisition process begins when an organization's C4 and IT needs have been established and approved in the appropriate capability documentation. The appropriate capability documentation is published by DCS, G–3/5/7 and is the LandWarNet Mission Command, GOSC-approved, potential solutions list that includes material and nonmaterial solutions. The acquisition process involves validating requirements to satisfy the mission and user's needs; understanding how the business-process analysis is accomplished by evaluating outcome- and output-oriented performance measurements; monitoring the solicitation and selection of sources; awarding contracts; financing contracts; evaluating contract performance; monitoring contract administration; and performing those technical and management functions directly related to the acquisition process in accordance with AR 70–1.

(1) The Army CIO/G–6 will perform a compliance assessment on all ACAT I, II, and special-interest programs for 40 USC Subtitle III (Clinger-Cohen Act (CCA)) compliance, prior to a milestone and a full-rate production (FRP) decision. To assess CCA compliance, the program is required to provide a self-assessment based on the CIO/G–6 assessment criteria, which serves as the basis for the required evaluation. In support of the milestone decision for ACAT I, II, and special-interest programs, a CIO/G–6 compliance determination will be assessed and prepared. The CIO/G–6 will recommend a determination to the Office of the Secretary of Defense for ACAT I and special-interest programs. The CIO/G–6 determines CCA compliance for ACAT II programs.

(2) The CIO/G–6 has delegated the CIO compliance for ACAT III programs to the Army-delegated milestone decision authority (MDA) for the Joint program executive office, PEO, direct-reporting PMs, Army commands, and agencies of the program. The responsible organization will perform the compliance assessment and determination prior to a milestone or FRP decision. When the compliance determination for ACAT III programs is complete, the determination will be forwarded to the CIO/G–6, who retains Title 10, United States Code, C4, and IT acquisition oversight.

(3) The CCA determination applies to both ACAT and non-ACAT programs. The CIO performs compliance assessments and determinations on non-ACAT programs prior to a milestone and FRP decision. The non-ACAT program is required to provide a streamlined assessment to serve as the basis for the required CIO/G–6 compliance assessment and determination.

q. Collaboration tools standards.

(1) Collaboration capabilities are defined as the wide range of structures, processes, procedures, and services or tools necessary to enable two or more individuals who are not co-located to use an electronic synchronous or asynchronous environment to communicate, plan, coordinate, and make decisions to achieve an objective.

(2) All Army activities (operational, tactical, and institutional) investing in or implementing collaborative tools will use enterprise collaboration services and tools to the greatest extent possible. The Networthiness Division maintains a list of enterprise collaboration tools and services on the approved product list (APL) Networthiness home page at https://www.us.army.mil/suite/page/137030/. Army organizations may use tools on the APL, if deployed in accordance with the approved configuration and implementation processes. If Army organizations have collaboration requirements that are not met by current capabilities, they are required to submit these requirements through CHESS for approval prior to implementing a collaboration solution (see DA Pam 25–1–1).

(3) The Communications-Electronics Command is the Army focal point for technical matters and the Army interface with the DISA Configuration Management Office to address interoperability within Army systems. The Army CIO/G–6 will support only the new tools or the sustainment of existing collaborative tools that meet the DOD standards.

(4) When using collaboration services and tools, Army commands will adhere to all usage policies and guidelines established for IT and communications systems. This includes the requirement of commanders and supervisors to—

(a) Develop acceptable use policies for all users under their control.

(b) Develop local policies and procedures on access control and management of information used in collaborative efforts.

(c) Comply with configuration management and IA vulnerability management policies to maintain security of the collaborative environment over its entire life cycle.

(5) All individual users are responsible for any communication or exchange, and the creation of information using collaboration capabilities are subject to applicable professional, ethical, and security guidelines.

r. Property book accountability. Hardware will be accounted for using the appropriate supply regulations that address property book accountability. Software is treated as a durable item. Although software does not require property book accountability, it will be controlled by the using organization's IMO (see DA Pam 25–1–1).

s. Redistribution and disposal of information technology assets.

(1) The screening, redistribution, and disposal of IT equipment are completed through the Defense Reutilization and Marketing Service (DRMS). For further guidance and clarification on the processes and communications flow for the

disposal of excess IT equipment, the installation NEC should contact its installation property book officer for guidance on the reuse, transfer, and donation programs for excess IT equipment, or visit the DRMS Web site at http://www.dispositionservices.dla.mil. See also DRMS Instruction 4160.14; DOD 4160.21–M; and DA Pam 25–1–1.

(2) DRMS supports EO 12999 through the DOD Computers for Learning Program. Refer to https://www.dispositionservices.dla.mil/cfl for more information on this program.

Chapter 4
Web Site Management

4–1. Army enterprise portals, Web sites and email

The transition to enterprise services will reduce the number of servers, the cost of hardware and software, and will improve the user experience. This section addresses how technology can be used to: support standardized, collaborative tool sets; share information to the maximum extent possible; and, provide portals with single sign-on capability.

a. Enterprise portal. The Army enterprise portal improves information sharing and saves resources currently expended on traditional means of Web and email communication. The Enterprise Collaboration Services Program will replace the current AKO enterprise portal for collaboration and coordination of Army's nonpublic information.

(1) *Enterprise Web portals.* AKO (at https://www.us.army.mil), and Army Knowledge Online SIPRNET (AKO-S) are the current enterprise Web portals supporting unclassified and classified Army Web sites that activities will use to develop knowledge networks and portals.

(2) *Identity and access management.* All Army email and Web servers that host sensitive information will be configured to use certificate-based client authentication using only DOD public key infrastructure (PKI)-approved certificates. The Enterprise Identity Management Service will populate the Global Address List, and will provision and maintain user account data and access management to enterprise applications. Issuance of the common access card (CAC) will serve as the authoritative source for account provisioning. Once a CAC is provisioned from the Defense Manpower Data Center, the user will have access to Army and DOD enterprise services from any Army system.

(3) *Logon.* In accordance with AR 530–1, all account users are responsible for the security of their credentials and the content they create on the enterprise portal. Users who fail to properly secure their credentials and content via any Army IT resource may be subject to punitive and/or adverse administrative action.

(4) *Posting.* Users will conform to posting procedures and policy on the use of official and authorized telecommunications. See AR 25–13 for the unified capabilities (UC) policy.

(5) *Enterprise portal records.* Email and other files on the enterprise portal that are determined to be records will be managed in accordance with AR 25–400–2.

b. Web sites and services.

(1) *Management of Web domains.* NETCOM will manage the "army.mil" Web site assignment of subdomains and the Web domain registration process. The Web domain registry will include all of the Web domain information for "army.mil" Web sites at the third-level domain, as well as any commercial Web sites being used.

(2) *Web domain registration.* Army organizations that desire subdomains must register their domain through the registration processes and guidelines found at https://www.us.army.mil/suite/page/600053/. All Army social-networking sites and social-media sites must register at http://www.army.mil/.

(3) *Social-networking sites.* The policy for Internet-based capabilities and social networking sites is prescribed in DODI 8550.01. Current policies, implementation plans, and best practices can be found at http://www.defense.gov/socialmedia and http://www.army.mil/media/socialmedia. For more information, see paragraph 4–2 of this publication.

(4) *Use of the army.mil Web domain.* All Army public and nonpublic Web sites must be located on an "army.mil" or "disa.mil" domain, unless the CIO/G–6 waives that requirement. In accordance with DODI 8410.01, organizations must use the ".mil" domain as their second-level domain name for the unclassified-but-sensitive NIPRNET and ".smil.mil" for the SIPRNET, unless a waiver has been granted by the CIO/G–6 and, in turn, the DOD CIO. See https://www.milsuite.mil/wiki/Non-.Mil_Domain_Waivers for more information on non-.mil domain waivers and exceptions.

(5) *Web domain authorizations.* Only specified organizations or functions are authorized to have Web sites at the third-tier level of the Web domain (for example, netcom.army.mil) as primary Army Web sites. HQDA principals, the USAR and ARNG, ACOMs, ASCCs, DRUs, PEOs, PMs, Service schools or centers, installations, division-level units, and special-Service organizations will establish third-level Web sites and will consolidate subordinate organizations into these sites in order to minimize the total number of Army Web sites. All other organizations may have a Web presence (for example, Web pages) on the Web sites of their respective parent organizations.

(6) *Use of Internet protocol restrictions.* Public Web sites are considered unrestricted or restricted. A Web site that is intended to be accessible from the Internet to anyone and authentication is not required for access, is considered a public unrestricted Web site. A Web site that is intended to be accessible from the Internet, but access is restricted to authorized users and authentication is required, is considered a public restricted Web site.

(7) *Web management policy.* Army Web site managers and maintainers must comply with the Web management

policy in this regulation, the DOD Web site administration policy located at http://www.defense.gov/webmasters/, and subsequent DOD guidance and direction. Information contained on publicly accessible Web sites is subject to the policies and clearance procedures prescribed in AR 360–1 for the release of information to the public. Web site managers and maintainers will—

(a) Ensure that only official Army information that is releasable and of value to the public is posted on the Army's public Web sites.

(b) Ensure that official information of interest to Army employees is posted on the enterprise portal.

(c) Ensure that Web servers are compliant with the Information Assurance Vulnerability Management program and placed behind a reverse proxy server, or implement an alternative security procedure (see AR 25–2). Reverse proxy servers must be configured in a way that does not cache secure socket layer (SSL) traffic.

(d) Ensure that Web site content is accurate, current, and provides reliable data in compliance with information quality guidelines in paragraph 5–8.

(e) Make immediate corrections or block the Web site or link until corrections can be made when notified of Web site violations by the Army Web Risk Assessment Cell. (See AR 25–2 for additional information.)

(f) Apply appropriate privacy and security policies to respect all visitors' privacy.

(g) Display a privacy and security notice in a prominent location on at least the first page of all major sections of each Web site. Each privacy and security notice must clearly and concisely inform visitors to the site regarding what information the activity collects about individuals, why it is collected, and how it will be used.

(h) Ensure surveys, questionnaires, and forms collecting information from members of the public or Federal personnel and contractors comply with AR 335–15.

(8) *Web site reviews.* Army commanders and organizational heads will ensure that the public affairs officer, operations security officer, and other appropriate designee(s) (for example, command counsel, force protection, intelligence, and so forth) complete required training. The public affairs officer and operations security officer will review and clear Web content and format prior to posting to the Internet, in accordance with AR 530–1. The designated reviewer(s) will conduct routine reviews of Web sites on a quarterly basis to ensure that each Web site is in compliance with the policies in this regulation and that the content remains relevant and appropriate. The use of Web analysis software for reviews is encouraged but not required. The minimum review will include all of the Web site internal control checklist items at appendix C, paragraph C–4. For more information about the types of information exempt from this requirement, see DA Pam 25–1–1.

(9) *File transfer protocol.* File transfer protocol sites in the public domain are not authorized and will not be used in the place of authorized public Web sites.

(10) *Privacy.* Army organizations must observe Federal, DOD, and Army policies for protecting personal privacy on official Army Web sites and must establish a documented process for Webmasters and maintainers to screen their Web sites quarterly, to ensure compliance.

(11) *Security and access.* Army organizations must establish a security and access-control process based upon the sensitivity of the information and the target audience for which it is intended.

(12) *Assignment of Webmaster and maintainer.* Army organizations will assign a Webmaster and maintainer for each of their Web sites and pages. Army organizations will provide their Webmasters and maintainers sufficient resources and training on both technical and content matters. Resources are available at https://informationassurance.us.army.mil/. Online training is available at https://iatraining.us.army.mil/.

(13) *Section 508.* Web sites are required to comply with the provisions of Section 508 of the Rehabilitation Act Amendments of 1998 (29 USC 794d). Web sites must be equally accessible to disabled and non-disabled Federal employees and members of the public. Guidance on Section 508 standards concerning Web-based information and applications is located at http://www.access-board.gov/. Exceptions should be referred to the staff judge advocate for legal review.

(14) *Private Web sites.* Private Web sites are an official area on AKO or on internal organizational Web servers for DOD organizations to publicize projects and goals, and to share valuable information with the community for collaboration and coordination purposes. Activities will only establish organizational private Web sites in AKO or on internal organizational Web servers. Organizational Web site managers will install access-control mechanisms, see AR 25–2. All Internet-facing applications must be hosted within a STIG-compliant NIPRNET DOD demilitarized zones (DMZ). Internet-facing applications must be registered with the Army IP registration authority.

(15) *Use of cookies.* Use of cookies follows the requirements found in OMB M–10–22. Persistent "cookies" that track users over time and across different Web sites to collect personal information are prohibited on public Web sites. The use of any other automated means to collect personally identifiable information (PII) on public Web sites without the express permission of the user is prohibited. Third-party cookie generation will be disabled.

c. Web access blocking. In accordance with AR 25–2, the use of Web access blocking or filtering tools is authorized for permanently blocking user access to inappropriate Web sites. Exceptions to this policy are described in DA Pam 25–1–1. Access to prohibited Web sites for mission support reasons is considered authorized use.

d. Other private Web sites (Intranets and Extranets).

(1) *Hosting.* Army organizations are authorized to host private Web sites when enterprise resources cannot support the functional requirement.

(2) *Authentication.* All NIPRNET and SIPRNET Intranets (private Web sites used for processing information limited to DOD users) will be enabled to use DOD PKI certificates for server authentication, and client/server authentication. Owners of authorized Intranets must ensure that the SSL is enabled and that PKI SSL encryption certificates are loaded on the servers. Use of IP restriction by itself is insufficient; such sites will be considered publicly accessible rather than private. PKI Web server certificates may be obtained from the NETCOM TNOSC.

(3) *Web application authentication.* All Intranet Web applications will be enabled to use DOD PKI certificates with CACs for user access, unless waived by the CIO/G–6. Legacy applications currently using the AKO lightweight directory access protocol to authenticate clients must use PKI-capable platforms.

(4) *Use of Public Key Infrastructure.* Web applications must be PKI-enabled. For more information on PKI requirements, standards, and implementation, see AR 25–2 and on AKO at https://www.us.army.mil/suite/folder/10144308/.

(5) *Exceptions.* Any unclassified Army Web server that is categorized as a private Web server but provides nonsensitive and publicly releasable information resources is exempt from using CAC or any other form of PKI credential for authentication. An unclassified Web server providing nonsensitive and publicly releasable information is considered a private Web server when it limits access to a particular audience and/or provides access restrictions for purposes other than safeguarding sensitive Army mission base for official use only (FOUO) data. Although considered a private Web server, this type of private Web server provides nonsensitive and publicly releasable information and is exempt from CAC and PKI requirements.

(6) *Extranet authentication.* Unclassified extranets (private Web sites used for exchanging nonpublic domain information with members of the public and other individuals not authorized to use DOD PKI resources) may be operated to facilitate Army missions and functions. To ensure ease of access, organizations that collect sensitive but unclassified information from the general public as part of their assigned mission are authorized to purchase and use approved, commercially available certificates to provide SSL services. Extranet owners must select from the trusted and validated products lists on DISA's Web site at https://aplits.disa.mil/. All Internet-facing applications must be hosted within a STIG-compliant NIPRNET DOD DMZ. Internet-facing applications must be registered with the Army IP registration authority, NETCOM.

e. Internet service providers. The only authorized access from Army computers, systems, and networks to the Internet is through a DISN-controlled and DISN-monitored connection. Exceptional situations may exist where Army organizations connected to the NIPRNET may also require direct connection to the Internet, for example, through an Internet service provider. For more information, see https://www.milsuite.mil/wiki/Non-.Mil_Domain_Waivers; and for GIG Waivers, see the GIG Waiver Panel Army page at https://intellipedia.intelink.gov/wiki/GIG_Waiver_Panel_Army/.

f. Email services.

(1) *Use of encryption.* Emails transmitting sensitive data from an Army-owned, Army-operated, or Army-controlled system or account will be encrypted to maintain confidentiality; and digitally signed for data integrity, message authenticity, and non-repudiation using an approved DOD PKI certificate. The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates. In addition, sensitive information transmitted in email messages must be clearly labeled to show any sensitivity, such as "Sensitive-Privacy Act Information." Signature or encryption will be used to send information that is—

(a) Protected by 5 USC 552a (The Privacy Act). The Privacy Act includes protection of PII.

(b) Identified as FOUO.

(c) Protected under HIPAA. (See also para 2–22*b* and references.)

(d) Otherwise sensitive (as defined in the glossary).

(2) *Bandwidth usage.* NECs are required to develop local procedures on bandwidth usage and to encourage processes to manage bandwidth demand.

(a) Only mission-essential attachments will be transmitted.

(b) When internally staffing documents within an organization, place the documents in internally accessible areas, shared drives, or approved organizational Intranets instead of sending documents via email.

(c) When sharing documents external to an organization, place documents in the aggregate on the enterprise portal or on an approved organizational Web server, and provide the link or uniform resource locator (URL) where the documents are located. Activities will use the enterprise portal as the primary tools for collaboration.

(3) *Use of official Government email service.* Only Government-provided email services are authorized for use as primary simple mail transfer protocol addresses and for use on CACs. Email services provided by a commercial service provider are prohibited for Army business communications. Automatically forwarding from an official Government account to an unofficial (commercial service) is prohibited. "Auto-forward" default settings on email will restrict individuals from automatically forwarding their email messages to commercial (private) addresses. There is no prohibition for manually forwarding email messages, one at a time, after opening and reading the content to ensure that the information is not sensitive or classified.

(4) *Email administration.* Local email procedures will provide for implementation of sound email account management consistent with guidance in this regulation and other Army security guidance. NECs will establish local procedures to ensure that—

(a) System administrators are assigned and trained.

(b) System administrators establish office accounts to receive organizational correspondence. All shared organizational accounts will use DOD-approved PKI certificates to ensure that email requiring data integrity, message authenticity, or nonrepudiation, is correctly identified and protected. Data owners must classify their data as public, public restricted, or private. If data is classified as public restricted or private, then the data owner must restrict access to the information by using an approved, two-factor authentication access-control method such as CAC and PKI.

(c) Accounts are assigned only to individuals authorized to use Army-operated IT systems.

(d) Passwords are protected and stored at the same level of protection as the most sensitive data in the system.

(e) Inactive accounts are terminated after a specified period of time (for example, 30 days), if no longer needed.

(f) Addresses are correctly formatted and registered with central directories as required for efficient operations (and that the Global Address List reflects DSN numbers as well as commercial numbers).

(5) *Email records.* Army policies for records management apply to email traffic. Designated RMs, records coordinators, and records custodians will monitor the application of records management procedures to email records. Email backup storage is not considered records archiving. Refer to AR 25–400–2 and chapter 5 of this publication for more information on preserving email communications as records.

(6) *Email backup and storage.* Systems administrators will ensure that email and Web file servers are backed up for a period of time (no less than 90 days) in an off-site, secure storage facility. Backups will be conducted on a daily, weekly, and monthly basis in accordance with local procedures.

4–2. Social media sites

a. The NIPRNET will be configured to provide access to Internet-based capabilities across all DOD components. For more information, see DODI 8582.01 and DOD DTM 08–037. Commanders at all levels must continue to defend against malicious activity affecting Army networks. Commanders may therefore take actions to limit access to Internet-based capabilities on a temporary basis, to ensure that a mission is safeguarded or to preserve operational security.

b. Commanders must continue to deny access to sites with prohibited content (for example, pornography, gambling, hate sites).

c. All dealings with external official presences (EOPs) must comply with DODI 8550.01, which details the responsible and effective use of Internet-based capabilities.

d. All information contained on publicly accessible Web sites is subject to the policies and clearance procedures described in AR 360–1 for the release of information to the public. Furthermore, all organizations engaging in social media or EOPs must comply with records management requirements as detailed in AR 25–400–2.

e. Agency personnel using or accessing social-media technologies must comply with DOD 5500.07–R, and Part 2635, Title 5, Code of Federal Regulations (5 CFR 2635). These rules include prohibiting the release of nonpublic information, requiring appropriate disclaimers of opinions being expressed, and restricting the use of Government computers in order to access and manage personal sites during official duty time.

f. The Office of the Chief of Public Affairs provides best practices and guidance on how to implement an EOP. This can be found in The United States Army Social Media Handbook and other documents found at http://www.slideshare.net/USArmySocialMedia/.

Chapter 5
Information and Security Management

Section I
Data management

Data is a strategic asset. The Army CIO is responsible for and prescribes the Army's information management policy at the strategic level. Consistent with this responsibility, the Army CIO establishes and oversees DM transformation through the ADMP. The Army's Chief Data Officer is appointed by the Army CIO and is responsible for developing, implementing, and enforcing Army and Federal data standards and strategy for the Army. Each mission area and Joint capability area will identify a data steward empowered by the Army CIO to perform the same duties as the Chief Data Officer within their functional areas. As a team they will lead the DM transformation, which is fundamental to net-centricity. The ADMP allows the Army to achieve a single authoritative source for all data, while reducing the number of data centers and computer rooms to more effectively manage IT operations. DM will move the Army to a single, standard set of technology and will facilitate the retirement of legacy systems and applications. A more efficient DM environment will maximize opportunities for greater information- and knowledge-sharing. The need for centralized DM

arose from the realization that the Army's predominantly decentralized computing environment had reached unsustainable levels from operational, financial, technological, and security perspectives. Implementing enterprise DM and warehousing increases operational performance and reliability, introduces standardization, provides the agility to respond efficiently and effectively to change, enhances security, and allows for economies of scale in terms of operations and maintenance costs.

5–1. Army Data Board

The Army Data Board (ADB) provides an enterprise data-sharing environment that allows decision-makers access to information in a timely and secure manner. More information regarding ADB structure, positions, responsibilities, and other information is located on the Army Data Board Web page located at https://www.milsuite.mil/wiki/Army_Data_Board/.

5–2. Army Data Management Program

a. General. The ADMP is prescribed in Army Directive 2009–03. For more information on the ADMP, see DA Pam 25–1–1.

b. Army data standards management.

(1) *Data standards.* Data standards (specified in the DISR and other guidance documents and their associated authoritative data sources (ADSs), IESS, unique identifiers (UIDs), eXtensible markup language (XML), resource description framework (RDF), RDF vocabulary description language, RDF schema, and RDF schema derivatives) will be used to guide all data exchanges, including those needed to support legacy systems. DM requirements will be included in IT planning documents.

(2) *Army organizations.* All Army organizations producing or using data standards (such as ADS, IESS, UID, and XML) will ensure that—

(a) Only Army-approved data standards are used in systems.

(b) New data standards are registered in the appropriate part of the Data Performance Plan System (DPPS) as needed.

(c) Input is provided to Army data standards reviews.

(d) Data standards used for information exchanges are identified during Army and Joint interoperability certification processes.

(e) Only organizations identified by the data stewards as data standards producers will create or update DPPS content exchanged with or disseminated to any other organization.

(f) Valid implementation of data standards Armywide. Functional data managers will manage ADSs, IESS, UIDs, and XML.

(g) Their data is categorized as public, public restricted, or private. DOD requires protection requirements and accessibility requirements based upon the type of data. Public data that must be accessible from outside the .mil domain must reside in a DOD-approved shared space. Public data cannot be mixed or stored with public restricted or private data. Public restricted data must use some access-control method to restrict access to the data. Examples are CAC or user ID and password. Private data cannot be accessed outside the .mil domain. Private data must be separate from public and public restricted data in accordance with DOD policy, directives, and Chief Technology Offices.

(3) *Army data quality management.* All Army organizations producing or maintaining enterprise data must incorporate a comprehensive data quality management process (DQMP) as part of their data production and maintenance activities. For more information on DQMP, see https://www.milsuite.mil/wiki/Data_Product_Catalog. The DQMP comprises the policies and procedures for selecting and implementing data-quality standards. These ensure that Army information products achieve and maintain the necessary level of data quality necessary to support all Army enterprise-wide operations and processes. All organizations producing or maintaining enterprise data will—

(a) Create an environment and support the infrastructure needs to facilitate the exchange of lessons learned and best practices, so that all information products are brought to specified data-quality levels, regardless of operational environment.

(b) Ensure that data-quality management procedures are adopted and applied to the Army data assets under their control.

(c) Ensure that information products are objectively assessed by the DQMP for conformance to the necessary quality levels.

(4) *Army producers and maintainers of information products will—*

(a) Treat their information resources as "products" and ensure their fitness for purpose by implementing a data quality management system (DQMS).

(b) To the maximum extent possible, adopt well-established industry standards for their DQMS implementations, such as International Standards Organization (ISO) 9001:2008.

(c) Seek to obtain certification for their DQMS, for example, "ISO 9001 certified" status.

(d) Evaluate additional industry standards applicable to data quality, such as "ISO 8000–Data Quality", and develop strategic plans for their adoption.

(e) Adopt for their information products, industry standards that enable both platform-independent machine processing and automated quality verifiability; by standing up, for example, an open technical dictionary (as defined by ISO 22745–1:2009) to manage the metadata for their information products.

(f) Seek to achieve maximum visibility, accessibility, and understandability of their information products through the adoption of Web services that expose their information products, via XML, and register the XML schemas in the DOD Metadata Registry (MDR) as applicable.

(g) Document and make available their "lessons learned" pertaining to their implemented DQMS.

(5) *Applicable Army data-quality metrics.* The quality of a product is the degree to which a set of inherent product characteristics fulfills specified user requirements derived from ISO 9000. Therefore, Army producers and maintainers of information products will—

(a) Document and validate their specific information product user requirements.

(b) To the extent possible, select quantifiably measurable data-quality metrics intended to support the goals and objectives stated by OMB in "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies," which is in Volume 67, Federal Register, p. 36; and in the charter of OMB's Federal Data Architecture Subcommittee, May 2006.

(c) Assess the relevance of applicable data-quality characteristics, with respect to the specified information product user requirements, and develop quantitative measures for them as the basis for their data quality evaluation methodology. Typical data-quality characteristics to be used include, but are not limited to, the following: relevance, provenance, completeness, clarity, timeliness and latency, interpretability, accuracy, consistency of values, consistency of representation, precision, objectiveness, believability, reliability, understandability, security, accessibility, and syntactical correctness.

(d) Establish appropriate values to be achieved for each of the quality metrics selected as part of their data-quality evaluation methodology (as well as timelines for reaching them), with particular emphasis on the cost-benefit ratio associated with the impact on the information product user requirements.

(6) *Army data-quality institutionalization.* In order to achieve and maintain information superiority, all Army-information-products producers and maintainers will—

(a) Ensure that Army architects incorporate DQMS components in their architectures.

(b) Allocate resources for data quality-management training of all pertinent personnel.

(c) Seek to maintain liaisons with industry standardization bodies whose focus relates to product quality management and data quality specifications.

c. Authoritative data sources.

(1) "Authoritativeness" is not a global attribute for all conceivable uses, but rather for a given set of consumers to use within a particular context. This distinction is critical to understanding the role of ADSs within DOD because there are differences of opinion about what source is "best" (that is, the most accurate or the most up-to-date). The answer depends upon how the data consumer is using the data. Hence, authoritative bodies must carefully review candidate ADSs to ensure their particular information needs are fulfilled for that specific use prior to designating a data source as an approved ADS.

(2) A data source becomes an ADS when an authoritative body designates it as an approved ADS. The authoritative body needs to provide the information necessary for the appropriate data consumers to understand which data objects available from the ADS are authoritative, and under what circumstances and for what purpose are they authoritative.

(3) The owner of Army reference data (a type of data object) will make the coded data values available as an ADS to ensure maximum reuse and interoperability. These value sets will be made accessible to authorized data consumers.

(4) Data synchronization requirements will be identified and documented as part of the ADS documentation.

(5) Data synchronization requirements will consider information flows and reference table value domains (including data transfers, system run cycles, management decision cycles, timeliness, and accuracy).

(6) Functional data managers (FDMs) are considered authoritative bodies and subject-matter experts within their domain, and identify and propose candidate ADSs. Each FDM will enter ADS metadata into the Enterprise ADS (EADS) registry to initiate the ADS process. Completion of the registration process within the EADS registry will result in formally recognized Army ADSs. A schema describing an ADS should be defined by the respective FDM.

(7) Data stewards will sponsor proposed ADS for EADS certification. Upon approval, the EADS registry will maintain information about the ADS. Approved ADSs will be reviewed periodically by the ADS owners to ensure accuracy and harmonization with Joint and DOD-designated authoritative sources.

(8) Army IS PMs and managers will implement enterprise-level ADSs in their ISs.

(9) Data producers will—

(a) Create and maintain ADSs whose values are shared among Army ISs, such as reference table value domains, force structure decompositions, and so on.

(b) Synchronize ADS implementations with the standardized versions managed and published by those organizations with the ADS management authority.

d. Unique identifiers.

(1) All Army data collected and maintained in relational databases designated to support Army enterprise capabilities will use globally unique UIDs to ensure full data integration, referential integrity, and data interoperability (see DODD 8320.03).

(2) Data standards producers will—

(a) Use UIDs in new systems. All new systems will add UIDs to their physical schemas in a manner that best fits their fiscal constraints and user needs.

(b) Use UIDs in specified legacy systems. Specified legacy systems that are not scheduled for termination will add UIDs to their physical schemas in a manner that best fits their fiscal constraints and user needs.

(c) Use UIDs in commercial enterprise resource planning (ERP) applications. As part of the contractual agreement with ERP application developers, provisions must be made in their physical schemas for the use of UIDs.

(d) Support and ensure that all pertinent data resources identified via unique UIDs will be maintained and registered to permit discovery and reuse within functional areas and at the enterprise level. Specifically, all reference data sets identified with UIDs will be documented and published in the DPPS to facilitate exchanges by other users.

(e) Maintain a registry in the DPPS of all the UID seed users to provide optimal implementation oversight of the UID-based key management process.

(f) Use UIDs as an additional means of information resource identification expressed via emerging Web technologies, such as raw data file triples, which normally use URIs for that purpose. This will facilitate the insertion of these types of information resources in relational databases.

e. Information exchange standards specifications.

(1) To control the production and applicability of information standards required to ensure interoperability for information exchanges among Army ISs, the participating systems must conform to information exchange specifications. An information system will be deemed "conformant" with an approved IESS if the model of the particular information system—

(a) Is based either on the entire IESS or on a subset of the IESS. Not all attributes of selected entities need to be implemented.

(b) Has extensions of that subset that are not redundant with elements of the IESS itself. Emerging extensions that could apply to a specific IESS will be proposed for general use in succeeding versions.

(c) Uses approved data types and coded domains.

(d) Identifies POCs for generating instances of UID keys (to avoid redundancy and non-uniqueness).

(e) Has identifiers that are identical with or directly derivable from those specified in the IESS. In the case of relational database schemas, the IESS-conformant information system uses alternate keys, but the original IESS keys are preserved. To ensure fully faithful information transfer among databases, the IESS-defined primary keys of one database for any entity comprised within the IESS specification must be identical either to the primary or alternate keys of the same entity in any other IESS-conformant database. The primary or alternate key, in this case, will be based on the UID from the ADS.

(2) All Army ISs will exchange data by specifying their exchanges within the DPPS in a format that conforms to IESS developed and agreed to by the COI that support the respective information system. Whenever database implementations identify data requirements not yet in a pertinent IESS, these will be shared with members of the COI that own the IESS so that the requirement will include all the core requirements.

(3) Program manager and materiel developer responsibilities:

(a) Each PM and MATDEV will develop and maintain architecture models, data models, business rules, and other artifacts within the DPPS.

(b) Respective COI(s) will review and approve submissions to the DPPS.

(c) The MATDEV is responsible for integrating COTS software and ensuring interoperability with the existing metadata contained in the DPPS.

(4) Data standards producers will—

(a) Use, as required by the DPPS to specify all IESS, appropriate open-source and industry standards for information modeling and specification as their base set of data-model artifacts, and create necessary processes and supporting business rules. Create in machine-processable form using an appropriate rule language, such as the object constraint language (OCL) or the semantic of business vocabulary and business rules. To ensure maximum interoperability, the IESS must be implemented through software that reliably conforms to the DPPS.

(b) Add to the list of relevant tools and techniques, if sufficient Governmental and commercial support develops for them, any evolving structured languages and frameworks for creating IESS. In the context of IESS written in Unified Modeling Language, this includes the application of, for example, the model-driven architecture framework and the query/view/transformation language.

(c) Use only tools with nonproprietary extensions. IESS will not be created with tools that use proprietary extensions for which there is no translation mechanism into and out of the DPPS.

(d) Use ISO 11179 data elements already tested within COIs whenever practical vice newly created ISO 11179 data

elements. When selecting existing data elements for exchange, Army activities will adhere to the following order of precedence (highest to lowest) for selection:

1. ISO 11179 data elements from Joint COIs.

2. ISO 11179 data elements from Army COIs mapped to those elements from Joint COIs.

3. ISO 11179 data elements from other Federal department COIs mapped to those from Joint COIs.

f. Extensible markup language.

(1) All XML tags for use in data exchanges shall be derived from the pertinent IESS adopted by the COI engaged in such data sharing and reuse activities. The logical names of entities (or classes) from the DPPS should be used for the generation of XML tags to enhance readability unless other factors make this choice impractical (for example, insufficient bandwidth). In those cases, shorter names akin to the physical table and column names used in relational database management system implementations should be used for the XML tags. When the names of the XML tags differ from the names of the tables and columns used in IESS-conformant databases, Extensible Stylesheet Language Transformations files will be provided and maintained by the COI to transform the tags into a form that facilitates the automated import.

(2) All data exchanges among ISs executed via Web-based solutions will use XML as their transfer mechanism. The producers of the data will register their XML metadata and non-XML metadata (that is, data models, message formats, and database schemas) with the DOD MDR. (Not applicable to weapons platforms).

(3) Data standards producers will—

(a) Use World Wide Web Consortium (W3C) technical specifications with a "recommended" status to ensure maximum interoperability. A W3C recommendation is a technical report that is the end result of extensive consensus-building about a particular technology or policy (see http://www.w3c.org for further definition).

(b) Adhere to XML-related standards promulgated by other nationally or internationally accredited standards bodies when developing applications within the domain that the standard addresses.

1. When a standard produced by one of these bodies competes with a similar product of the W3C, the W3C standard will take precedence.

2. XML implementations must not use proprietary extensions to XML-based specifications.

(c) Actively participate in the work of appropriate XML and XML-related technical and business standards bodies. The Army CDO will act as coordinator of such participation.

(d) Whenever practical, use existing XML components rather than developing new XML components. When selecting existing XML tags, Army activities will adhere to the following order of precedence (highest to lowest) for selection:

1. Joint COI IESS-based tags.

2. Army COI IESS-based tags.

3. Federal department COI IESS-based tags.

(e) The order of precedence recommended above does not preclude selection of a component with lower priority when other considerations, such as cost, implementation schedules, and so on, would make the use of a component of higher ranking less defensible. All Army XML business standards will be at the enterprise level of the entire Army.

(f) Leverage commercial practices, standards, and products before creating Army-unique ones.

g. Data Services Layer-Army service interface specifications. The Data Services Layer-Army (DSL–A) is a set of standards and guidelines for implementing data services within the Army enterprise in a manner that will facilitate achieving the Army's goal of interoperable data sharing in a net-centric Army enterprise. The DSL–A service interface specifications (SISs) establishes the standard operations, behaviors, error handling, and protocols for systems that will be used to expose data as a service and to exchange data.

(1) All data exchanges among information systems executed via Web-based solutions will adopt or extend services or service patterns defined in the DSL–A SIS.

(2) Data services producers (COI leads, system owners, PEOs, program and project managers, system architects, and system developers) will—

(a) Create new systems or applications only when existing services in the service-oriented architecture do not provide the needed functionality, and existing services cannot be orchestrated into a service that provides the needed functionality.

(b) Ensure that their data services meet Army enterprise standards by designing and developing data services using and complying with the DSL–A SIS.

(c) Register their service artifacts (Web Services Description Language and schemas) with the MDR.

(d) Register their services with the Net-Centric Enterprise Services Service Registry.

(3) Data stewards will take the lead implementing a plan to reach the goal of common data service interfaces across the Army enterprise (as defined in the AIA). Data stewards will—

(a) Identify and prioritize data sources to expose data through data services.

(b) Develop the implementation plan for implementing data services using the DSL–A SIS.

(c) Oversee development and validate the DSL–A compliant data services.

h. Data initialization.

(1) Systems providing communications and information exchange for the mobile Warfighter must be synchronized or initialized for operation using agreed to network settings. All systems using or enabling IP routing must be correctly set. The initialization process will put in place correct addressing, open and close router ports and switch channels, establish paths over communications media, ensure the correct versions of operational data are exchanged, and ensure the correct information is rendered on common operational picture displays.

(2) Commonly, initialization is executed for all systems of a tactical unit, such as a brigade combat team, at the same time. The initialization process requires the development and application of a complex integrated software utility or package of setup instructions, commonly called "data products." The initialization effort must account for interoperability with systems of other units with which information must be exchanged for mission accomplishment. Reinitialization is required each time there is a tactical unit or task-force reorganization.

Section II
Information Management

5–3. Visual information management

VI is the element of IT that addresses the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery; and linear or nonlinear multimedia, with or without sound, for the purpose of conveying information. VI includes the exchange of ideas, data, and information, regardless of formats and technologies used (see DODI 5040.02). VI shall be viewed and used as an essential information resource and a supporting capability for strategic communication. Army activities shall make, acquire, or create VI, appropriately distribute VI gathered, and preserve VI obtained following procedures detailed in DODI 5040.02.

a. Defense Imagery Management Operations Center. All Army VI activities will participate in the Army Documentation Program by making daily submissions of record VIDOC to the Defense Imagery Management Operations Center (DIMOC) for accessioning. The capture and submission of record VIDOC will be considered high priority by all VI activities.

(1) *Historically significant visual information documentation products.* DRUs, COMCAM teams, and local VI activities will submit historically significant VIDOC products directly to DIMOC. Provide noncurrent VI records having historical or long-term value to DIMOC for accessioning into the DOD VI records holdings or the National Archives and Records Administration.

(2) *Tactical documentation.* Record VIDOC is obtained by COMCAM teams during theater-level Army and Joint wartime operations, contingencies, exercises, or humanitarian operations. COMCAM teams will electronically forward imagery, with embedded captions, to DIMOC for distribution to operational decision-makers and other customers. COMCAM teams will provide original source material to DIMOC for accessioning.

b. Visual information activities responsibilities.

(1) All multimedia and visual information (M/VI) activities will use DD Form 2858 (Visual Information Activity Profile) to review, update, and certify compliance with their Defense visual information activity number (DVIAN) and the C4IM Services List annually, no later than 30 September of each odd-numbered fiscal year (FYs 13, 15, and so forth). Certification, changes to an authorization, or waiver requests will be endorsed by the commander of the activity and forwarded through the major command to CIO/G–6. In the event of deficiencies or noncompliance, the M/VI activity should address steps being taken to mitigate and correct identified issues. Regardless of cost and without exception, all Army productions will be documented using the online DD Form 1995 (Visual Information (VI) Production Request and Report). Approval will be obtained prior to commencing production. If no suitable production exists in the Content Discovery and Access Catalog (CDAC), complete section 1 of DD Form 1995 in coordination with the supporting VI activity to establish the production requirement. DD Form 1995 initiates the production process and remains with the production through its life cycle.

(2) AMVID supports the requirements in DODI 5040.02 by operating and maintaining a VI activity to support the OSD, the office of the CJCS, major commanders, and other DOD organizations in the NCR, as required. AMVID provides a specialized VI activity to procure productions and other VI end products from commercial sources to support the Army, other DOD Component requirements established in resourcing agreements. AMVID is the Army's component coordinating point, which is a central designated point in the Army for the coordination of imagery for transmission to the DIMOC records holdings in accordance with DODI 5040.02.

(3) The Enterprise Multimedia Center (EMC) supports the realignment of VI resources, functions, and facilities for the transforming institutional Army. The EMC will be designed to support mission products and services as defined on the C4IM Services List and connected to an Armywide network. The EMC will provide products and services classified as "above-baseline" or mission in accordance with the CIO/G–6 SLA and operational-level agreement on C4IM services. All M/VI personnel will comply with the C4IM Services List. Above-baseline mission services and products will be provided on a fee-for-service basis. All requests received on an installation for above-baseline mission services and products will be forwarded to the EMC for production or approval for local installation production. The EMC will provide in-house production of multimedia and VI in support of Army, DOD, other military departments,

and other Government agency requirements. Each installation M/VI activity will be connected to an EMC for support from a single location. For more information on the Fort Lewis EMC, please see http://www.lewis-mcchord.army.mil/vi/index.htm; for information on Fort Eustis EMC, please see http://www.eustis.army.mil/emc.

(4) The VI activity performs or provides any product or service listed in DA Pam 25–91 and the C4IM Services List. No organization or individual will perform, provide, or contract these products or services without authorization unless specifically excluded.

(5) VI activity profile changes and updates will be requested through the DOD Web site at http://dodimagery.afis.osd.mil/ using DD Form 2858. The CIO/G–6 (SAIS–AOI) will assign the DVIAN. For more information, see DODI 5040.07. Each installation will consolidate VI functions into a single VI activity within an installation, community, or local support area, with all functions assigned to a single VI manager. VI activities will support all DOD and Federal agencies. Dedicated VI capabilities within the authorized DVIAN may be maintained to support medical, safety, criminal investigation, or intelligence requirements.

(6) All installation directorates of plans, training, mobilization, and security, in coordination with VI managers, will plan, program, and budget for all authorized VI requirements. See DA Pams 25–91 or 25–1–1 for more information.

(7) Unless an exception or waiver is granted, training support centers will provide all baseline services contained in the C4IM Services List. Waiver requests must include justification that includes a full analysis of the expected benefits and a formal review by the activity's senior legal officer. All waiver requests must be endorsed by the commander of the requesting activity and forwarded through the major command to the CIO/G–6. Refer to AR 25–30 for guidance.

(8) The designated EMC for each region will provide mission services or above-baseline services from the C4IM Services List. No other M/VI activities are authorized to provide above-baseline services. All requests for above-baseline services must be referred to the EMC at Fort Eustis; Fort Lewis; or US Army Europe, VI Service Europe using the Visual Information Ordering Site (VIOS). Enterprise locations are identified in the DVIAN document and may only be approved by the CIO/G–6.

(a) If an M/VI activity cannot provide a baseline service that would normally be approved, the request will be forwarded through the chain of command for further coordination and possible execution.

(b) VIOS will not be used as a formal tasking mechanism. A customer request submitted in VIOS does not guarantee approval or support.

(c) When a valid tasking order is issued for an event that requires visual information support, all VIOS requests for that event, regardless of source, will be forwarded to the formally tasked supporting M/VI unit for coordination, approval or disapproval, and execution.

(9) Installation VI managers will maintain and actively use the VIOS to manage and collect metrics for the quarterly top-loading of data into the Army's IT Metrics Program. The EMC VI Manager will coordinate with the IT metrics POC to ensure the metrics submission occurs during the specified time frame, usually the last day of the reporting cycle. VIOS is the central IT metrics data-collection point for both CONUS and OCONUS VI activities. All VI installations will use the VIOS as the official asset management work order program to centralize and provide solution for providing common user IT M/VI services. All M/VI organizations will use VIOS as the mechanism to collect data and metrics.

(10) Army productions will be acquired in accordance with the relevant FARs and DFARS. Without exception, Army productions will be created or acquired at the lowest possible cost that achieves communications objectives. All productions must be mission-essential.

(11) AMVID Production Acquisition Division (AMVID/PAD) provides a central capability to rent, lease, procure, or produce M/VI productions in support of Army, DOD, other military departments, and other Government agency requirements, as established in resourcing agreements. The AMVID/PAD is the only multimedia/visual information activity authorized to contract for total productions. Contact AMVID/PAD at the AMVID Customer Service Desk (703) 697-1699 for assistance with production cost estimates. The EMC is an authorized Army activity to facilitate production procurement contracts exceeding the $5,000 limit (including man-hours, equipment rental, administrative expenses, and any other operating cost). Local VI procurements exceeding the $5,000 threshold must be vetted according to procedures identified in DA PAM 25-91.

(12) IMCOM will conduct an annual data call to the garrisons and provide requirements to the CIO/G–6 for IMCOM installations. For non-IMCOM installations, data will be collected by the appropriate command. See DA Pam 25–91 for more information.

c. Visual information procedures. For more information on the Visual Information Systems Program, certifications of VI assets, and the VIDOC program, see DA Pam 25–91.

Table 5–1
Required visual information forms

Form	Purpose
DA Form 4103, Visual Information (VI) Product Loan Order	To record media loans.
DA Form 3903, Multi-media/Visual Information (M/VI) Work Order	To identify and capture all work associated with a customer request for products and services.
DA Form 5695, Information Management Requirement/Project Document	To document all requirements for VI items (excluding expendables and consumables) with an end item cost over $25,000.
DD Form 1367, Commercial Communication Work Order	To submit a commercial communication work order against an existing consolidated contract when acquiring telecommunications services for the installation. Ordering officers, appointed by the NETCOM contracting officer, are authorized to place orders up to the dollar limit defined in their appointment orders. NECs will submit all orders exceeding the ordering officer's threshold to the NETCOM contracting officer.
DD Form 2537, Visual Information Caption Sheet	To maintain a system for numbering individual product items based on DODI 5040.02 requirements. Still photographs, motion picture footage, video recordings (excluding those assigned a PIN), and audio recordings, if retained for future use, will be assigned a VI record identification number. All VI material retained for future use will be captioned.

d. Visual information records management. Original local or non-local Army multimedia VI productions and VI products, with their associated administrative documentation, are controlled as official records throughout their life cycle, and disposal in accordance with General Records Schedule 21, DODI 5040.02, this regulation, and DA Pam 25–91. For VI housekeeping files, refer to AR 25–400–2.

e. Customer self-help. Unless an exception or waiver is submitted through the ACOM and granted by DA CIO/G–6, training support centers will provide the full suite of customer self-help support, which includes the production of simple products (for example, briefing charts, sign-out boards, flyers, or flip charts).

f. Recording events. All M/VI products and services are for official use only. As a general rule, social events such as military balls and hails and farewells are unofficial and considered entertainment except where Nationally or historically significant.

5–4. Records management

In accordance with DA General Order 2006–01, the records management function transferred from the DCS, G–1, to the AASA.

a. Records management mission. The mission of records management is to capture, preserve, and make available evidence essential for Army decisions and actions; meet the needs of the American public; and protect the rights and interests of the Government and individuals. This program will operate in accordance with public laws and regulatory guidance. Title 44, United States Code, Chapter 31 (The Federal Records Act) requires the head of each Federal agency to maintain a continuing program for the economical and efficient management of the agency records.

b. Record management regulation. The records management program is defined and described in AR 25–400–2.

c. Records management responsibilities. Army proponent records management duties are specified in paragraph 2–9 under AASA responsibilities, in accordance with DA General Order 2012–01. Requirements at the state level, including statutory, legal, financial, or administrative requirements by the authority of the State's Governor and Adjutant General, will be governed by Title 32 of the United States Code and managed in accordance with State and local policy.

(1) The Director, U.S. Army RMDA has operational responsibility for records management and its associated programs as defined in AR 25–400–2.

(2) ACOM, ASCC, and DRU Records administrators have command or unit-wide responsibilities for ensuring the creation and preservation of official mission records throughout subordinate units and activities. Records administrators will be appointed in writing and registered as records administrators in the ARIMS. Copies of written appointments will be sent to the U.S. Army Records Management and Declassification Agency, 7701 Telegraph Road, Casey Building, Room 102, Alexandria, VA 22315–3860. For more information, see paragraph 2–16 of this publication.

(3) The FOA, staff support agency, separately authorized activity, and tenant and satellite organization RMs will be appointed in writing and registered as RMs in the ARIMS. Copies of written appointments will be sent to the address in paragraph 5–4*c*(2). RMs will adhere to the roles and responsibilities prescribed in AR 25–400–2 and DA Pam 25–403.

(4) IMCOM regional- and installation-level RMs will be appointed in writing and adhere to the roles and responsibilities prescribed in AR 25–400–2 and DA Pam 25–403. RMs will be registered in the ARIMS and copies of written appointments will be sent to the address in paragraph 5–4*c*(2).

d. Life cycle management of records. Refer to AR 25–400–2 for the objectives in the life cycle management of records. Additional objectives include to—

(1) Maintain Army information that meets the definition of a record is the responsibility of all military, civilian, and contractor personnel; commanders; and leaders. See AR 25–400–2 for more information on how to maintain official records.

(2) Control the quantity and quality of records produced by the Army.

(3) Establish and maintain control of the creation of data elements to be placed in records so the information contributes to the effective and economical operations of the Army and prevents the creation of unnecessary records.

(4) Simplify the activities, systems, and processes of record creation, maintenance, and use.

(5) Direct continuing attention to the life cycle management of information from initial creation to final disposition.

(6) Establish and maintain systems or techniques as the Archivist of the United States, in consultation with the Archivist of the Army, as necessary.

(7) Employ modern technologies and cost-effective alternatives for storage, retrieval, and use of records.

(8) Ensure that records are preserved in a manner and on media that meets all legal and archival requirements.

(9) Incorporate standards and technical specifications in all IS functional requirements to ensure the life cycle management of record information.

(10) Ensure the periodic evaluation of records management activities relating to the adequacy of documentation, maintenance and use, and records disposition, at all levels, throughout the information resources management review process.

e. Records management tenets. In executing the mission, objectives, and associated programs, Army activities will—

(1) Simplify recordkeeping methods.

(2) Minimize the burden on commanders, Soldiers, civilians, and contractor personnel.

(3) Establish proactive control over operational records.

(4) Centralize record collection when deployed in theater.

(5) Digitize once with multiple access.

(6) Ensure appropriate command emphasis.

(7) Incorporate records management requirements into training.

f. General policies.

(1) Personal records pertain solely to an individual's private affairs (see DA Pam 25–403). Official records are made or received in compliance with Federal law in the transaction of public business. Correspondence designated personal, private, eyes only, and so on, but relevant to the conduct of public business, are official records. Backchannel messages are official records that are processed under stricter handling and transmission techniques than normal message traffic. All official records are subject to life cycle management procedures and are the property of the Federal Government, not the military member or employee making or receiving them.

(2) A Government official may accumulate extra copies of records. These reference files commonly are invaluable to later generations of staff planners and historians in discovering the rationales of the decision process. For more guidance regarding Government officials accumulating extra copies of Federal records, see DA Pam 25–403.

(3) Army general officers and senior civilian executives (normally limited to senior executive service-level grades) may place reference files that they create during their tenure of office with the Military History Institute without violating the prohibitions discussed above. Moreover, such donations create a single source of information on actions accomplished by high-level officials. The Director of the Military History Institute will provide archival and librarian assistance to the donor. The donor must meet the security clearance requirements of AR 380–5.

(4) Records that may not be removed from the control of the Federal Government for personal retention or donation to any institution without the approval of the Archivist of the United States are identified in AR 25–400–2.

(5) Commanders and agency heads will safeguard official records and properly dispose of them in accordance with policy guidance in this regulation and in AR 25–400–2. Safeguarding against the removal or loss of Federal records includes an annual, locally developed, and mandatory briefing of all military, civilian, and contractor personnel to ensure that all DA personnel are aware that—

(a) Transfer of title and destruction of records in the custody of the Army are governed by specific provisions of 44 USC 33.

(b) There are criminal penalties for the unlawful removal or destruction of Federal records, and the unlawful disclosure of information pertaining to national security and personal privacy. Refer to AR 25–400–2, AR 340–21, and AR 380–5 for more information.

(c) Under the Federal Records Act of 1950, records in the custody of the Army OCONUS may be destroyed at any time during the existence of a state of war between the United States and any other power, when hostile action by a foreign power appears imminent, or if the potential capture of records by the enemy is prejudicial to the interests of the United States. If emergency destruction is performed, the Government official will compile a list of records, a list of records destroyed, their inclusive dates, and the date destroyed. This information will be forwarded to RMDA, 7701

Telegraph Road, Casey Building, Room 102, Alexandria, VA 22315–3860 as expeditiously as theater or operational conditions permit.

(6) In accordance with AR 25–400–2, the ARIMS does not apply to—

(a) Record copies of international agreements covered under AR 550–51 (except those maintained by the Office of the Judge Advocate General).

(b) Publications and blank forms stocked for filling requisitions.

(c) Reference materials and books in formally organized and officially designated libraries.

(d) Personal or private records maintained in the workplace.

g. Record media. Information created within the Army may be recorded on various display media, such as paper, microform, machine-readable format, or presentation media (audio and visual). Approved Army disposition schedules (see AR 25–400–2) apply to all Army-recorded information, regardless of the media upon which recorded. In order to protect the rights and interests of the Army and its members, keep costs to a minimum, and serve the study of history; display or presentation media must be selected for long-term records that best serve the operational needs of the Army and meet statutory scheduling requirements. These decisions are vital considerations in the design stage of information life cycle management. For guidance on VI-specific records management, see 36 CFR 1237.

h. The records management program. The records management program includes the following major subprograms: Army recordkeeping systems management; official mail and distribution management; office symbols; correspondence management; and rule making.

5–5. Publishing and printing

AR 25-30 designates AASA as the functional proponent for the APP. The APP consists of development, production, and dissemination of all official DA publications. The APP also provides oversight of printing, reproduction, self-service copying, and related equipment and operations.

a. Management. The AASA provides centralized control and management of the Army's departmental publishing and distribution system, to include distribution of hard copy and electronic editions of DA publications and blank forms.

b. Statutory restrictions for publications and requirements for printing. Refer to AR 25–30 for policy on restrictions in publishing, printing, and distribution of materials and requirements for all printing and duplicating work.

c. Requisitioning printing.

(1) All Army printing and duplicating (including compact disc-read only memory replication) will be prescribed in accordance with policies in AR 25–30.

(2) Effectiveness and economic printing options will be considered when determining whether in-house or commercial resources will be used in accomplishing mission objectives.

(3) Functional managers at all levels of command will conserve printing, duplicating, and self-service copying resources (including personnel, funds, material, and equipment) consistent with conducting operations essential to mission support.

(4) In the event of and during the initial stages of mobilization, authority is granted to the field to produce any departmental publication (including blank forms) necessary for mission requirements. This automatic authority will remain in effect until otherwise notified by HQDA (SAA–APP), 105 Army Pentagon, Washington, DC 20310–0105.

Section III
Information and Data Security

5–6. Information assurance

IA policy provides the measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Reference AR 25–2 for IA policy, mandates, roles, responsibilities, and procedures for implementing the Army IA 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 Army-managed network. For more information regarding Army IA, see https://www.milsuite.mil/wiki/Portal:Army_Information_Assurance.

5–7. Privacy impact assessments

a. A privacy impact assessment (PIA) is a tool that assesses whether PII in an electronic form is collected, stored, or disseminated in a manner that protects the privacy of individuals and their information. PII is used to distinguish or trace an individual's identity, such as name, social security number, or biometric records; which, when used alone or combined with other personal or identifying information, is linkable to a specific individual. The PIA analyzes how personal information is handled to—

(1) Ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.

(2) Determine the risks and effects of collecting, maintaining and disseminating personal information in an information system.

(3) Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

b. Army system owners will—

(1) Conduct an assessment of all information systems and applications or electronic collections under their purview to determine if PII is collected, maintained, used, or disseminated about members of the public, Federal personnel, contractors, and foreign nationals employed at U.S. military facilities internationally.

(2) Document completion of the assessment using the DD Form 2930, Privacy Impact Assessment. The digital signature PDF version of the DD Form 2930 is required for all PIA submissions. Submit all forms to cio-g6.pia.inbox@mail.mil. Refer to DA Pam 25–1–1 for PIA completion guidance.

(3) Complete PIA data fields in APMS, as required.

c. As the PIA reviewing official, the CIO/G–6, will—

(1) Ensure that PIAs are completed according to the guidance provided in DODI 5400.16.

(2) Ensure that system owners address requirements and initiate action to correct deficiencies.

(3) Ensure that each PIA has been reviewed by the Army information assurance official and the privacy officer.

(4) Maintain a repository of approved PIAs.

(5) Submit an electronic copy of each approved PIA to the DOD CIO, consistent with DOD guidance and OMB Circular A–11, Section 300.

(6) Post all approved PIAs on the CIO/G–6 Web site (http://ciog6.army.mil/) in accordance with current DOD instructions.

d. A PIA must be reviewed and updated every 3 years in conjunction with the C&A cycle as a component of the DOD Information Assurance Certification and Accreditation Process (DIACAP) package. The Army senior information assurance officer will review all PIAs to ensure compliance with information assurance policies prior to CIO approval.

e. The Army Privacy Officer, Office of the Administrative Assistant to the Secretary of the Army will review completed PIAs and confirm compliance with DOD Directive 5400.11, and ensure that systems of records notice issues have been properly identified and evaluated prior to CIO approval.

5–8. Quality of publicly disseminated information

a. Freedom of Information Act. 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 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 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 enterprise portal or other approved controlled-access (private) Web servers as required. Requests for nonpublic data from private individuals and organizations should be coordinated with and referred to the local FOIA or 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.

b. Privileged information. Data files (both paper and electronic) containing privileged attorney-client 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.

c. Functional proponents. The responsible functional proponents will maintain Army data and ensure that the data are readily accessible to whoever requires the information.

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

e. Quality standards for publicly disseminated information.

(1) *Federal quality standards.* Federal agencies are required by 44 USC 3506 to maintain a basic standard of information quality (objectivity, utility, and integrity) and take appropriate steps to incorporate information quality criteria into public information dissemination practices.

(2) *Army quality standards.* Army organizations will establish standards of quality that are appropriate to the nature and timeliness of the information they disseminate. Organizations will not disseminate substantive information that does not meet a basic level of quality. An additional level of quality is warranted in situations involving influential

scientific, financial, or statistical information, which must be capable of being substantially reproduced. (See detailed Army and DOD guidance on implementing information quality requirements in DA Pam 25–1–1 and at http://ciog6.army.mil/.)

(3) *Exempt types of information.* Specific types of information that are not subject to this standard are—

(a) Distribution of information that is limited to Government employees, Army contractors, or grantees.

(b) Intra-Army or inter-Army, or other department or agency sharing Government information, including responses to requests under FOIA; the Privacy Act; Appendix 2, Title 5, United States Code (The Federal Advisory Committee Act); or other similar laws.

Chapter 6
Enterprise Architecture Standards and Certifications

Section I
Enterprise Architecture

6–1. General

This chapter defines the AEA and provides policy and guidance governing the composition and use of architecture documentation within the Army. In addition, see chapter 2 of this publication for unique architecture responsibilities. Supporting EA documents and guidance as well as the Army Architecture community and can be found at http://architecture.army.mil.

a. EA is a strategic information asset base, which defines the mission; the technologies necessary to perform the mission; and the transition processes for implementing new organizations, processes, and technologies in response to changing mission needs. EA includes a baseline architecture, a target architecture, and a sequencing plan (DODD 5144.1).

b. The AEA refers to either an architecture description or an architecture implementation. As an architecture description defined in the current version of the Department of Defense Architecture Framework, the AEA provides a representation of a current or future real-world configuration of resources, rules, and relationships. Once the representation enters the design, development, and acquisition portion of the system development life cycle process, the AEA is transformed into a real implementation of capabilities and assets in the field. The AEA Framework supports the transformation process.

c. In addition to supporting tracking and alignment of Army initiatives and process improvements to enterprise strategy, the AEA supports acquisition, implementation, and management of integrated and interoperable systems that provide required operational capabilities to the Operating Force and the Generating Force as well as business operations.

d. In accordance with the DOD Directive-Type Memorandum 09–013, component architectures and capability set architectures shall be registered through the DOD Architecture Registry System (DARS) to support the DOD decision-making process and further the federation of DOD EAs. DARS is located online at https://intelshare.intelink.gov/sites/dars/default.aspx?PageView-Shared.

6–2. Army enterprise architecture governance

a. Governance activities within the EA life-cycle management influence and direct the policies, procedures, roles, responsibilities, schedules, and appropriate decisionmaking bodies that govern the EA. The governance activities also ensure the EA is integrated with appropriate planning management processes, such as portfolio management, configuration management, resource allocation, and strategic planning efforts.

b. Governance is achieved through the following boards—

(1) The Army Enterprise Board establishes strategic EA guidance and direction.

(2) The LandWarNet Mission Command GOSC approves architecture initiatives, conducts in-process reviews (IPRs), directs trade-offs, shapes the program objective memorandum (POM), approves solutions, and approves release and delivery.

(3) The Enterprise Guidance Board certifies interoperability and integration, validates architectures, establishes technical standards and patterns, and approves implementation; see DA Pam 25–1–1.

(4) Business Systems Information Technology Executive Steering Group advises the CMO on Armywide requirements for the synchronization, integration, prioritization, and resourcing of Army Business IT architectures.

6–3. Complying with Defense Information Systems Registry standards

PEOs and PMs will ensure that their Army systems comply with the mandated technical standards contained in the DISR (https://gtg.csd.disa.mil). Exceptions to this requirement are permitted only via a waiver or an approved change request (CR) as specified in DODI 4630.8 and CJCSI 6212.01. Technical architecture standards associated with

Internet protocol version 6 (IPv6) will follow the guidance in paragraph 6–5*b* of this publication. In addition to DISR guidance, materiel developers must comply with CIO/G–6's technical guidance and standards published in the technical guidance repository: https://www.kc.army.mil/TRM_TOOL/.

6–4. Army enterprise architecture composition

The AEA describes all echelons and aspects of the Army enterprise. The AEA will be managed using a tiered approach and its architectures will be developed in accordance with a rules-based framework approved by the CIO/G–6 and aligned with DOD IT standards, which are published separately in the DISR. See also DA Pam 25–1–1.

a. Unit, segment, or domain architecture guidance. Segment and organizational architectures are components of the AEA. The AEA will include reference models and federated architecture concepts that describe the relationship between architectures at different echelons (such as unit, segment, and domain architectures) by using fit-for-purpose architecture models as required. Domain architecture is developed or sponsored by the domain data stewards. For information on functional roles and responsibilities of the domain data stewards, see paragraph 5–1 of this publication.

(1) Guidance for material solution architectures.

(2) Materiel solution architecture and data must adhere to the current Department of Defense Architecture Framework and CJCSI 6212.01.

b. Architecture Activities. Architecture Activities define the framework of initial activities required for LandWarNet to be designed to provide the information advantage and achieve the desired end. The five core characteristics include the following: enable global authentication and access control; provide information and services from the edge; provide Joint infrastructure; develop common policies and standards; and enable unity of command.

c. Relationships to external architectures. The AEA must conform to DOD IEA and Federal architecture policies and directives. When interfacing with other DOD external components' architectures, the vertical and horizontal alignments must be depicted.

6–5. Internet protocol management

a. Internet protocol address space management.

(1) NETCOM is designated the Army IP management and registration agent. NETCOM will lead the execution of the Army's IP management policy, and the planning and execution of the transition of public-facing servers and services to IPv6. NETCOM is the only Army organization authorized to obtain IP address space from the DOD Network Information Center and will control allocation and assignment of IP address space within the Army.

(2) The roles and responsibilities of Army organizations and agencies involved in the management of the address space allocated by the DOD for unclassified and classified networks are described in chapter 2 of this publication and in a technical authority memorandum published by NETCOM. The process includes roles for appropriate organizations and agencies to verify, validate, allocate, assign, and register IP address space to meet operational requirements.

b. Internet Protocol version 6. IPv6 provides many capabilities, including increased address space, quality-of-service, and mobility enhancements. Army organizations and agencies will upgrade public- and external-facing servers and services (for example, Web, email, domain name system, Internet service provider services, and so forth) to use dual-stack IPv6 by the end of FY 2012; and internal-client applications that communicate with public Internet servers and supporting enterprise networks to use dual-stack IPv6 by the end of FY 2014. Army organizations and agencies with internal network backbones that interface with the NIPRNET must be IPv6-capable to synchronize with the NIPRNET core transition as defined by the DOD. Specifically, any new IP product or system developed, acquired, or produced must—

(1) Be compliant with IPv6 for all application and product features.

(2) Have contractor or vendor IPv6 technical support available for development and implementation and fielded product management.

(3) Apply all of the requirements above to all acquisition systems.

c. Procurement process. During the procurement process, organizations must assess if a vendors product is IPv6-capable or can be made IPv6-capable. Factors to be considered are the following:

(1) Interoperability in heterogeneous environments with IPv4 systems or components.

(2) Vendor certification that—

(a) The vendor commits to upgrade as the DISR IPv6 standard profiles evolve.

(b) The vendor commits to provide IPv6 technical support.

(3) Joint Interoperability Test Command certification and inclusion on the DOD Unified Capabilities Approved Products List (UC APL).

d. Existing information technology and national security systems. Existing IT and NSSs and infrastructure components must be upgraded to incorporate IPv6-capable components and IPv6 features according to schedules developed by the proponent, MATDEV, or sustainment organization. If the system cannot or should not be migrated due to technology or cost considerations, proponents may apply to CIO/G–6 for a waiver.

e. Technical architecture reviews. In accordance with paragraph 6–4*c* of this publication, as part of the architecture

review process the Army CIO/G–6 reviews TA views for the presence of IPv6 standard profiles. Exceptions to the use of IPv6 require a waiver granted by the CIO/G–6.

f. Waiver requests. Requests for waivers should be submitted in accordance with DODI 4630.8. Waivers must include the proponent organization, system name, acronym, POC name, and contact information. The sample waiver request is available at https://www.kc.army.mil/TRM_TOOL/. The CIO/G–6, LandWarNet Architecture Integration Division coordinates the waiver requests.

g. Plan of action and milestones. NETCOM, assisted by representatives from stakeholder organizations and activities will develop a plan of action and milestones (POA&M) and submit it to the CIO/G–6 for approval. The POA&M establishes milestones, with suspense dates, for actions supporting the DOD requirement to upgrade public-facing servers and services managed by or for the active Army, the Army National Guard, and the U.S. Army Reserve to use IPv6. The POA&M must specify any test and evaluation activities that support enabling IPv6 on unrestricted public-facing Web sites.

h. Unrestricted public-facing Web sites. Unrestricted public-facing Web sites that are no longer relevant, useful, or needed for access by the general public must be eliminated. If the unrestricted public-facing Web site is still required, the domain name system and email services must be made available via IPv6 in DMZs or DMZ extensions.

i. Voice-over Internet protocol and Voice-over secure Internet protocol. Organizations that have a requirement to use voice-over Internet protocol (VoIP) or voice-over secure Internet protocol (VoSIP) to perform their missions will implement solutions in accordance with DODI 8100.04, CJCSI 6211, and Army CIO/G–6 guidance. Organizations must use only authorized products listed on the UC APL at https://aplits.disa.mil/. This requirement applies to both VoIP equipment and the associated local area network. Organizations with a requirement to implement VoIP must first submit their request through the local installation NEC. The request will then be processed through the appropriate Signal Command and forwarded to the CIO/G–6, SAS–AOI, 107 Army Pentagon, Washington, DC 20310-0107 for approval. Organizations not located on an installation with an NEC will forward their requirement via the appropriate chain of command, who will then forward the requirement through NETCOM for forwarding to CIO/G–6. The package submitted to CIO/G–6 must include the following: a detailed justification; an operational need statement; architecture; supported organizations or entire installation; impact statement describing results of not receiving an approved waiver; a Bill of Materials; the location where the equipment will be installed or where construction or renovation will take place; an approved requirements document; and, a General Officer or Senior Executive Service endorsement.

j. Unofficial and pay-per-use Internet access and services offered on post. Unofficial and pay-per-use Internet access and services are Morale, Welfare, and Recreation (MWR) Soldier and Family readiness functions. When pay-per-use unofficial Internet services (for example, barracks Internet services or wireless hot-spot service) are to be provided, non-appropriated funds (NAF) contract procedures will be used. These services are authorized to utilize all recognized transmission control protocol/IP Internet applications for unofficial purposes including, but not limited to, Web browsing, Web hosting, VoIP, unofficial email, video mail, and streaming audio and video. Paid and free unofficial Internet access and services are identified in AR 215–1. Access to NEC wired infrastructure and frequency spectrum will be granted to MWR programs to support these unofficial services, paid or free, when it does not conflict with or inhibit other official Army functions. Access to commercial unlicensed frequencies is to be granted as long as there is no interference with official frequencies or uses, and the equipment adheres to FCC regulations or similar host nation specifications when installed. When requested by MWR, NEC frequency managers will direct that other unofficial users of these frequencies be terminated if their use interferes with approved MWR implementation at the same frequency.

Section II
Certifications for Network Operations

This section identifies the certifications that must be obtained before a software or hardware change can be made to the Army's approved network baseline. Prior to operational use, system developers and operators must ensure that all systems and enabling components have been assessed as to their utility, risk of network disruption, and risk of introducing vulnerabilities; and have been properly certified for operations as a component of the approved Army network baseline.

6–6. Army interoperability certification

The AIC process exists to ensure acceptable systems interoperability and to reduce the introduction of vulnerabilities into the Army's operational network. The AIC process is the means to enforce compliance with approved technical guidance and information exchange requirements.

a. The CIO/G–6, Cybersecurity Directorate authorizes AIC testing, issues AIC policy, approves AIC procedures, evaluates test results, and makes recommendations for issuance of an AIC. Additionally, the CIO/G–6 is responsible for the configuration management process associated with making changes to the certified network baseline.

(1) Establishes the FaNS acceptance criteria and approves sites for performing AIC testing.

(2) Approves all changes to the authorized software baseline of the Army's operational network to reduce the introduction of vulnerabilities and prevent negative impacts to systems interoperability.

b. The director of the CIO/G–6, Cybersecurity Directorate certifies systems for connection to the Army's operational network based on favorable interoperability testing and assessment results; see DA Pam 25–1–1.

6–7. Certification of information support plans and tailored information support plans

All IT/NSS (systems or services) acquired, procured, or operated by any component of the DOD require interoperability certification. Interoperability certification establishes that the system or service has a plan for life cycle compliance with net-centric requirements. The Army uses certified information support plans as entrance criteria for AIC testing.

a. The CIO/G–6, Cybersecurity Directorate manages the Army Information Support Plan staffing and approval process. CIO/G–6 is the Army's link with the Joint Staff Directorate for Force Structure, Resource, and Assessment (J–8) and the DOD CIO on information support plan guidelines and program compliance. For more information, see DA Pam 25–1–1.

b. The director of the CIO/G–6, Cybersecurity Directorate is the Army's certifier of information support plans.

6–8. Networthiness certification program

Networthiness is the operational assessment of systems, applications, or devices to determine SISSU; and compliance with Federal, DOD, combatant comander, Service, and agency regulations, policies, and guidelines. Networthiness certification applies to all organizations fielding, using, or managing ISs on the LandWarNet, including COTS and Government off-the-shelf. Activities must obtain a certificate of networthiness before they connect systems and software to the LandWarNet.

a. NETCOM serves as the certification authority to validate from a location-centric view that the resulting infrastructure can support the information system, that there are no negative impacts to the LandWarNet or to other systems from the information system, and that the automated information system can be managed and maintained.

b. The MATDEV or system owner must submit a request for networthiness through the appropriate chain of command to NETCOM (email a request to netcom.hq.networthiness@mail.mil). Developers must obtain networthiness certification for all ISs and supporting elements. For current information and procedures, see the CIO/G–6 Networthiness homepage at https://www.us.army.mil/suite/page/137030/.

6–9. Department of Defense information assurance certification and accreditation process

The DIACAP process ensures that risk management is applied on ISs, including core-enterprise services and Web-based services for software systems and applications. DIACAP defines a set of DOD-wide formal and standard activities, general tasks, and a management-structure process for the C&A of a DOD IS that will maintain the IA posture throughout the system's life cycle.

a. The CIO/G–6, Cybersecurity Directorate is responsible for the Army's C&A process for managing the implementation of IA capabilities and services. CIO/G–6 identifies and assesses the residual risk with operating a system; determines the costs to correct or mitigate IA security weaknesses, as documented in the IT security POA&M; and makes recommendations to the certifying authority.

b. The director of the CIO/G–6, Cybersecurity Directorate is the Army's certifying authority for ISs.

Chapter 7
Installation Information Technology Services and Support

This chapter pertains to automation (computer software, hardware, and peripherals) and IT support for military construction.

7–1. Information technology support principles

a. Information transmission economy and systems discipline. All Army organizations will implement procedures to promote the 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 DODI 8100.04, DODD 8000.01, and DA Pam 25–1–1).

b. Continuity of operations. HQDA and operational organizations (such as JFHQ–States for the ARNG) must ensure the uninterrupted execution of their respective essential missions and functions under all probable conditions. As noted in AR 500–3, the HQDA COOP plan is the model upon which organizations will create their COOP plan, 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, ACOMs, and other separate reporting organizations are required to maintain a COOP plan consistent with AR 500–3. An IT contingency plan is one essential element of COOP. Each C4 and 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 COOP plans must be tested at least annually.

c. Network-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 producers and consumers with 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. The cornerstones of net-centric information sharing are to make data visible, accessible, and understandable while also promoting trust.

7–2. Information technology support services for Army organizations on Army installations

IT support services consist of the following four categories: baseline, enhanced, mission-funded, and mission-unique. These services are described in DA Pam 25–1–1 and at http://ciog6.army.mil/. The current approved C4IM Services List and customer-facing LandWarNet services catalog is located at https://www.itmetrics.hua.army.mil/.

7–3. Service and support agreements with Department of Defense activities

a. Army IT organizations will provide requested support to other DOD activities when the head of the requesting activity determines it would be in the best interest of the U.S. Government, and when the head of the supplying activity determines capabilities exist to provide the support without jeopardizing assigned missions. The service provider will provide an SLA for delivery of IT services. A service and support agreement (SSA) with an associated SLA will be negotiated between the two activities to specify the types and level of services and basis for reimbursement. The supporting NEC must be a participant in the interconnection security agreement (ISA) coordination. Depending upon the scope of the ISA, the respective signal command may be included as a third party.

b. Support agreements with non-DOD activities. Army activities may enter into support agreements with non-DOD Federal activities when funding is available to pay for the support; when it is in the best interest of the U.S. Government; when the supplying activity is able to provide the support; when the support cannot be provided as conveniently or economically by existing DOD services or commercial enterprise; and when it does not conflict with any other agency's authority. These determinations must be approved by the head of the major organizational unit ordering the support and specified in an ISA or SLA.

7–4. Morale, Welfare, and Recreation activities and non-appropriated fund instrumentalities

Use of appropriated funds (APF) on a non-reimbursable basis is authorized to provide communications and data automation support to—

a. MWR activities as outlined in AR 215–1 (see app B–4 of this publication).

b. Temporary duty, permanent change of station, and military treatment facility lodging programs as outlined in DODI 1015.12.

c. Medical holdover (MH) members residing in DOD housing are authorized to use a television with cable or satellite service, Internet service, and telephone service. MH members are responsible for any charges associated with premium cable, satellite service, and long-distance calls. NECs will ensure that sufficient controls are in place to safeguard against private misuse of Government communications.

d. All other Non-appropriated Fund Instrumentalities (NAFIs) as outlined in DODI 1015.15 (Army and Air Force Exchange Service, civilian welfare and restaurant funds, and so on).

(1) NAFI will comply with AR 70–1 and this regulation for acquisition and management of MWR systems that are obtained with APF.

(2) AR 215–4 governs IT supplies and services acquired with NAFI.

(3) NAFI requiring NEC-provided IT support will comply with this regulation and those procedures promulgated by the installation NEC. See also AR 25–13, Army MWR programs and NAF activities.

7–5. Electronic and information technology access for Army employees and members of the public

Title 29 USC 794d, 40 USC 762, and 20 USC 9201 require that agencies provide electronic and information technology (EIT) access to employees and members of the public with disabilities. The access must be comparable to the access available to individuals who do not have disabilities.

a. The law applies to all Federal agencies that develop, procure, maintain, or use EIT. Section 508 of the Rehabilitation Act Amendments of 1998 (29 USC 794d) was enacted to eliminate barriers in IT, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

b. Unless an exception applies (see DA Pam 25–1–1), all Federal or DOD acquisitions of EIT must meet the applicable accessibility technical standards or the functional performance criteria (36 CFR 1194) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board). For more information, see http://www.access-board.gov/.

c. EIT includes equipment or interconnected systems or subsystems of equipment that are used to create, convert, or duplicate data or information. More specific examples of EIT include, but are not limited to, telecommunication

products (such as telephones), information kiosks and transaction machines, Web sites, multimedia, and office equipment (such as copiers and fax machines). Review Web site http://www.section508.gov for further information and training about the laws and regulations pertaining to Section 508 and how to support its implementation. Section 508 is applicable to—

(1) All contracts for EIT supplies and services. Except for indefinite-delivery contracts, it is applicable to all delivery orders or task orders for EIT.

(2) All procurement actions for EIT processed by Government contractors, regardless of the customer being supported.

d. Information managers will make all reasonable efforts to accommodate individuals with disabilities, consistent with the laws cited above and AR 600–7. At no cost to individual activities, the Computer/Electronic Accommodations Program (CAP), at 5111 Leesburg Pike, Suite 810, Falls Church, VA 22041–3206, provides assistive technology accommodations and services to persons with disabilities at the DOD. The CAP operates a Technology Evaluation Center to match people with specific technologies. Funding is available to provide such things as interpreters, readers, personal assistants, telecommunications devices, telephone amplifiers, listening devices, and closed-captioned decoders and visual signaling devices for those with hearing problems. For more information, see DA Pam 25–1–1 and http://www.cap.mil/.

7–6. Installation-level technical support and service

Since NECs cannot provide technical support for things such as troubleshooting and training for all COTS hardware and software products, lists of supported products may be promulgated that restrict the scope of support to the listed products. In establishing such lists and levels of support, installations will not restrict the use of the common infrastructure of any DISR-compliant IS. The lists will not be used as the justification for eliminating competition in contracting. Supported organizations and IT fielding organizations that rely on common network capabilities may deviate from supported product lists only on a "by-exception" basis.

7–7. Tactical use of the secure network on Army installations

In accordance with the concept of the "installation as a docking station," tactical units at their home station in CONUS are permitted to connect to the installation secure network (that is SIPRNET), and sustain security posture in accordance with Army Cyber/NETCOM-published connection and registration TTPs upon direction by a FORSCOM-published connection order. NECs will support connecting tactical units to the SIPRNET as directed by operational order from their theater-level signal command.

7–8. Hardware and software services

a. Thin client computing. In some computing environments, thin client technology offers a lower total cost of ownership, increased productivity, and more robust security than offered by laptops and PCs. Thin client guidance can be found at https://www.us.army.mil/suite/files/21928696/.

(1) Army organizations planning for the refresh or acquisition of additional office automation equipment will consider thin client technology as the preferred office automation solution, and conduct a business-case analysis prior to acquiring thin client equipment.

(2) PC and laptop environment options will be used when thin client solutions cannot satisfy all user requirements and is approved by the senior IM official for an ACOM, ASCC, or DRU.

(3) Army commanders and organizational directors are authorized to transfer their organizations to thin client or hybrid-computing environments as required to meet their mission and resourcing requirements.

(4) The theater-level signal command and subordinate NECs will operate and maintain thin client or hybrid-computing architectures for supported Army organizations on their respective installations, posts, camps, or stations. Each NEC will operate no more than one thin client architecture. This architecture will be scalable to support multiple tenant missions.

b. Authorization and requisitioning. Automation equipment authorized in the Common Table of Allowances (CTA) 50–909; and listed in Supply Bulletin 700–20, applicable modified table of organization and equipment, TDA, or other appropriate authorization documentation; may be requisitioned within authorized allowances without submission of any IT specific planning or acquisition documentation to HQDA. The ACOMs, ASCCs, and DRUs will document the justification of purchase requests that are within their approval authority. The organizations may delegate approval authority to subordinate commands, separate reporting activities, and installations. NECs document justifications for purchase requests within their installation's approval authority. Such procedures will be applicable to all Army tenants on the installation.

7–9. Telework

Authorized individuals may telework according to DOD and Army policy. (See DODI 1035.01 and DA Memo 690–8 for more information.)

7–10. Energy conservation guidelines for information technology equipment

a. General-purpose office equipment, copiers, printing devices, faxes, all-in-one devices, and similar equipment will be turned off at the end of every business day. Computer monitors and peripheral devices, such as speakers, scanners, and external drives, will be turned off when not in use. Consideration should be given to using a power strip for all external devices to ease and consolidate turning off the devices and the associated transformers that are required for these devices.

b. Computer and peripheral devices used in conference rooms, video-teleconferencing, and kiosk environments will be turned off when not in use. Computer and peripheral devices will be turned off when not in use for any extended periods of absence such as vacation or holidays.

c. The central processing unit (CPU) for computers, desktop units, and personal computers can remain on for IT purposes only when the computer is capable of, configured, and enabled with energy-saving features such as standby or low-energy usage modes during periods of operator absence, and the mode is activated after 30 minutes of inactivity.

d. Use of this exception to remain on by use of standby or low-energy modes of operation are authorized only when the computer meets Energy Star compliance and consumes 20 watts or less of energy while in that mode.

e. An exception to leaving noncompliant CPUs on for short periods of after-duty hours is authorized by IT authority when a specific start and stop date, and applicable times for the CPUs to remain on, is stated. The specific impacted computers will be listed with the start and stop date announcement. Start and stop dates and announcements intended to defeat the intent of turning off the noncompliant CPUs when not in use are prohibited.

f. Servers, storage-area network devices, and other network infrastructure are *not* required to be powered off during periods of non-use.

g. For more information on energy conservation for IT equipment, including the use of energy saving features, see DA Pam 25–1–1.

7–11. Information technology support for military construction

Information technology requirements must be identified and funded in all MILCON so that the resulting building has a built-in IT infrastructure that satisfies the occupants' requirements on the Soldier ready date or troop ready date. (See DA Pam 25–1–1.)

a. Planning, designing, and monitoring construction. All project designs must comply with the standards set forth in the Installation Information Infrastructure Architecture (I3A) Technical Criteria, dated February 2010 for non-NIPR systems. Medical MILCON projects have medically unique requirements. UFC 4–510–01 will take precedent over the I3A for medical MILCON projects (see Chapter 10, UFC 4–510–01). SIPR implementation must follow the guidelines set forth in the SIPRNET Technical Guide. The I3A Technical Criteria is located at https://www.us.army.mil/suite/folder/5745483. The SIPRNET Tech Guide is located at https://www.us.army.mil/suite/folder/5744948. NETCOM will synchronize all IT planning, installation and delivery of baseline IT services within the buildings or facilities at the installation for MILCON and medical MILCON. The NEC must maintain close and continuous coordination with the relevant directorate of public works to ensure a complete awareness of all IT functional requirements (including mission-related and base support) for inclusion in the USACE statement of work for construction. If this expertise is not available, the NEC should request assistance from U.S. Army Information Systems Engineering Command (USAISEC) and the using organization to develop the IT functional requirements to support the facility. Upon contract award, a task officer with IT expertise will monitor contractor performance and provide approval or disapproval to the USACE contracting officer's representative.

b. Requirements for floor space intended for information technology systems. The supporting NEC will identify all proposed floor space intended for IT systems to their supporting signal brigade, who will then review the proposed requirements for consistency with single NEC server consolidation and application migration timelines. ARNG elements will coordinate with the ARNG CIO/G–6 for all ARNG component requirements. The CIO/G–6 will coordinate with the occupant and the USAISEC, as appropriate, to validate the required floor space needed for IT systems.

c. Cost estimates and funding. The department of public works will ensure the NEC is included in any planning, designs, and contract negotiations of the IS technical requirements and communication systems for any MILCON projects or renovation projects. The NECs will ensure that IT cost estimates for validated IT requirements are identified for each component supporting MILCON facilities. The appropriate supporting signal brigade will validate and approve the NEC input to the DD Form 1391 (FY__ Military Construction Project Data) prior to submission. The USAISEC must certify all DD Forms 1391 to IMCOM before the respective project review board in accordance with AR 420–1. IT funding and installation responsibilities will be identified for inclusion to the DD Form 1391 in accordance with AR 420–1. The requesting organization and IMCOM will ensure the IT requirements identified in the DD Form 1391 are submitted to the POM manager.

d. Host and tenant relationships. SSAs and interagency support agreements will include IT support for MILCON.

e. Installation information infrastructure. MILCON IT requirements include information system connectivity for both voice and data.

f. Applicability. MILCON IT requirements apply to all sustainment, restoration, and modernization projects.

Appendix A
References

Section I
Required Publications

Unless otherwise stated, all publications are available at: http://www.apd.army.mil/. Department of Defense regulations are available at: http://www.dtic.mil/.

AR 25–2
Information Assurance (Cited in paras 1–5*b*(4), 2–1*c*(9), 2–1*c*(15), 2–2*a*, 2–2*f*(2), 2–16*a*(6), 2–28*a*(6), 2–31*a*(6), 2–31*b*(9), 2–31*b*(10), 4–1*b*(7)(e), 4–1*b*(14), 4–1*c*, 4–1*d*(4), 5–6, C–4*c*.)

AR 25–30
The Army Publishing Program (Cited in paras 2–9*j*(1), 5–3*b*(6), 5–5, 5–5*b*, 5–5*c*(1), C–4*f*.)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in paras 2–9*c*(5), 5–8*a*.)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in paras 1–6*a*, 2–1*c*(9), 2–1*c*(15), 2–4*g*, 2–9*c*(1), 2–16*b*, 2–17*f*, 2–27*b*(3), 2–30*e*, 4–1*a*(5), 4–1*f*(5), 4–2*d*, 5–3*d*, 5–4*b*, 5–4*c*(1), (3), and (4), 5–4*d*, 5–4*f*, 5–4*g*.)

AR 70–1
Army Acquisition Policy (Cited in paras 2–7, 2–30*o*, 2–31*b*(8), 3–4*p*, 7–4*d*(1).)

AR 71–9
Warfighting Capabilities Determination (Cited in paras 2–16*a*(2), 2–17*a*, C–4*b*(17).)

AR 73–1
Test and Evaluation Policy (Cited in para 2–26.)

AR 215–1
Military Morale, Welfare, and Reccreation Programs and Nonappropriated Fund Instrumentalities (Cited in paras 6–5*j*, 7–4*a*.)

AR 215–4
Nonappropriated Fund Contracting (Cited in para 7–4*d(*2).)

AR 340–21
The Army Privacy Program (Cited in paras 2–9*c*(5), 5–4*f*(5)*b*, 5–8*a*.)

AR 360–1
The Army Public Affairs Program (Cited in paras 4–1*b*(7), 4–2*d*.)

AR 380–5
Department of the Army Information Security Program (Cited in paras 1–5*b*(4), 5–4*f*(3), 5–4*f*(5)(*b*).)

AR 380–53
Communications Security Monitoring (Cited in para 1–5*b*(4).)

DA Memo 690–8
Headquarters, Department of the Army Telework Program (Cited in paras 2–4*j*, 2–9*o*, 7–9.)

DA Pam 25–1–1
Information Technology Support and Services (Cited in paras 2–1*c*(16), 2–4*g*, 2–7*o*, 2–16*a*(4) and (10), 2–16*g*, 2–18*h*, 2–29*c*, *k*, *m*, 2–30*a*(5), 2–30*c*, 2–30*j*, 2–31*a*, 2–31*c*(7)(a), 2–31*d*, 3–4*b*, *e*, *f*, *j*, *k*, *m*, *q*, *r*, *s*, 4–1*b*(8), 4–1*c*, 5–2*a*, 5–3*b*(5), 5–7*b*(2), 5–8*e*(2), 6–4, 6–6*b*, 6–7*a*, 7–1*a*, 7–2, 7–5*b*, 7–5*d*, 7–10*g*, 7–11.)

DA Pam 25–91
Visual Information Procedures (Cited in paras 2–1*e*(6), 5–3*b*(3), (5), (11), 5–3*c*, *d*.)

CJCSI 6212.01
Net Ready Key Performance Parameter (Cited in paras 2–30*a*(1), 6–3, 6–4*a*(2).) Available at http://dtic.mil/cjcs_directives/

DOD DTM 09–013
Registration of Architecture Descriptions in the DOD Architecture Registry System (DARS) (Cited in para 6–1*d*.)

DODD 8320.03
Unique Identification (UID) Standards for a Net-Centric Department of Defense (Cited in para 5–2*d*(1).)

DODI 1015.12
Lodging Program Resource Management (Cited in para 7–4*b*.)

DODI 1015.15
Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources (Cited in para 7–4*d*.)

DODI 1035.01
Telework Policy (Cited in para 7–9.)

DODI 5000.2
Operation of the Defense Acquisition System (Cited in para 2–7*j*.)

DODI 5040.02
Visual Information (VI) (Cited in paras 5–3, 5–3*d* and table 5–1.)

DODI 5040.07
Visual Information Production (Cited in para 5–3*b*(4).)

DODI 8550.01
DOD Internet Services and Internet-Based Capabilities (Cited in paras 4–1*b*(3), 4–2*c*.)

OMB Memorandum 10–22
Guidance for Online Use of DOD Web Measurement and Customization Technologies (Cited in para 4–1*b*(15).) (Available at http://www.whitehouse.gov/.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read the publication to understand this regulation. The FAR is available at http://www.acquisition.gov/far/. The U.S. Code is available at: http://www.gpo.gov/fdsys/. Chairman of the Joint Chief of Staff instructions are available at: http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm/. Executive orders are available at: http://www.archives.gov/federal-register/executive-orders/disposition.html/. The Code of Federal Regulations is available at: http://ecfr.gpoaccess.gov/.

Army Directive 2009–03
Army Data Management

AR 5–11
Management of Army Models and Simulations

AR 5–12
Army Management of the Electromagnetic Spectrum

AR 5–20
Competitive Sourcing Program

AR 5–22
The Army Force Modernization Proponent System

AR 12–1
Security Assistance, Training, and Export Policy

AR 25–6
Military Affiliate Radio System (MARS) and Amateur Radio Program

AR 25–13
Telecommunications and Unified Capabilities

AR 25–50
Preparing and Managing Correspondence

AR 25–51
Official Mail and Distribution Management

AR 25–52
Authorized Abbreviations, Brevity Codes, and Acronyms

AR 25–58
Publication in the Federal Register of Rules Affecting the Public

AR 25–59
Office Symbols

AR 27–26
Rules of Professional Conduct for Lawyers

AR 27–60
Intellectual Property

AR 71–32
Force Development and Documentation-Consolidated Policies

AR 115–11
Geospatial Information and Services

AR 190–53
Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 335–15
Management Information Control System

AR 350–1
Army Training and Leader Development

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–40
Safeguarding and Controlling Communications Security Material (U)

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

AR 420–1
Army Facilities Management

AR 500–3
U.S. Army Continuity of Operations Program Policy and Planning

AR 525–27
Army Emergency Management Program

AR 530–1
Operations Security (OPSEC)

AR 550–1
Processing Requests for Political Asylum and Temporary Refuge

AR 600–7
Nondiscrimination on the Basis of Handicap in Programs and Activities Assisted or Conducted by the Department of the Army

AR 640–30
Photographs for Military Human Resources Files

AR 690–950
Career Management

AR 700–127
Integrated Logistics Support

AR 700–131
Loan, Lease, and Donation of Army Materiel

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

AR 710–2
Supply Policy Below the National Level

AR 735–5
Property Accountability Policies

AR 750–1
Army Materiel Maintenance Policy

ACP 123
Common Messaging Strategy and Procedures (Available at http://jcs.dtic.mil/j6/cceb/acps/)

CTA 50–909
Field and Garrison Furnishings and Equipment

DA General Order 2006–01
Transfer and Reassignment of the U.S. Army Records Management and Declassification Agency

DA General Order 2010–26
Establishment of the United States Army Cyber Command

DA General Order 2012–01
Assignment of Functions and Responsibilities within Headquarters, Department of the Army

DA Memo 25–51
Records Management Program

DA Pam 25–1–2
Information Technology Contingency Planning

DA Pam 25–30
Consolidated Index of Army Publications and Blank Forms

DA Pam 25–40
Army Publishing: Action Officers Guide

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 70–3
Army Acquisition Procedures

DA Pam 700–142
Instructions for Materiel Release, Fielding, and Transfer

FM 6–02.40
Visual Information Operations

FM 1–01
Generating Force Support For Operations

DCID 6/3
Protecting Sensitive Compartmented Information Within Information Systems (Available at https://www.us.army.mil/)

Social Media Handbook
The United States Army Social Media Handbook (Available at http://www.slideshare.net/USArmySocialMedia/)

CJCSI 3170.01
Joint Capabilities Integration and Development System

CJCSI 6110.01
CJCS–Controlled Tactical Communications Assets

CJCSI 6211.02
Defense Information Systems Network (DISN) Responsibilities

CJCSI 6215.01
Policy for Department of Defense (DOD) Voice Networks with Real Time Services (RTS)

Joint Publication 1–02
Department of Defense Dictionary of Military and Associated Terms (Available at http://www.dtic.mil/.)

Joint Travel Regulations
(Available at http://www.defensetravel.dod.mil/)

Defense Message System GENSER Message
Security Classification, Categories, and Marking Phrase Requirements. (Available at http://www.fas.org/.)

Defense Supplement to the Federal Acquisition Regulations Subpart 208.74
Enterprise Software Agreements (Available at http://www.acq.osd.mil/.)

Defense Finance and Accounting Service – Indianapolis Regulation 37–1
Finance and Accounting Policy Implementation (Available at http://www.asafm.army.mil/.) DISAC 310–130–1. Submission of Telecommunications Service Requests (Available at Web site https://www.disadirect.disa.mil/.)

DFAS–IN Manual 37–100–FY
Army Management Structure (AMS) (Available at http://www.asafm.army.mil/.)

DOD 4160.21–M
Defense Materiel Disposition Manual

DOD 5500.07–R
Standards of Conduct

DOD 5015.2–STD
Electronic Records Management Software Applications Design Criteria Standard

DOD 5200.2–R
Personnel Security Program

DOD 5400.7–R
DOD Freedom of Information Act Program

DOD 7000.14–R (volume 2B, chap 18)
Department of Defense Financial Management Regulations (FMRs)

DOD DTM 08–037
Policy for Department of Defense (DOD) Interactive Internet Activities

DODD 0–8530.1
Computer Network Defense

DODD 3020.26
Department of Defense Continuity Programs

DODD 4630.05
Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

DODD 5144.1
Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/ DOD CIO)

DODD 5230.09
Clearance of DOD Information for Public Release

DODD 5400.11
DOD Privacy Program

DODD 8000.01
Management of Department of Defense Information Enterprise

DODD 8100.02
Use of Commercial Wireless Devices, Services, and Technology in the Department of Defense (DOD) Global Information Grid (GIG)

DODD 8500.01E
Information Assurance (IA)

DODI 1000.15
Procedures and Support for Non-Federal Entities Authorized to Operate on DOD Installations

DODI 1015.10
Military Morale, Welfare, and Recreation (MWR) Programs

DODI 4000.19
Interservice and Intragovernmental Support

DODI 4630.8
Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

DODI 4640.07
Telecommunications Services in the National Capital Region (NCR)

DODI 5400.16
DOD Privacy Impact Assessment (PIA) Guidance

DODI 8100.04
DOD Unified Capabilities (UC)

DODI 8410.01
Internet Domain Name Use and Approval

DODI 8500.2
Information Assurance (IA) Implementation

DODI 8510.01
DOD Information Assurance Certification and Accreditation Process (DIACAP)

DODI 8551.1
Ports, Protocols, and Services (PPSM)

DODI 8560.01
Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing

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

DRMS Instruction 4160.14
Operating Instructions for Disposition Management (Available at https://www.drms.dla.mil/.)

UFC 4–510–01
United Facilities Criteria Design: Medical Military Facilities (Available at http://dod.wbdg.org/.)

STIG
Security Technical Implementation Guide (Available at http://iase.disa.mil/stigs/index.html/.)

EO 12845
Requiring Agencies to Purchase Energy Efficient Computer Equipment

EO 12958
Classified National Security Information.

EO 12999
Educational Technology: Ensuring Opportunity for all Children in the Next Century

EO 13103
Computer Software Piracy

EO 13423
Strengthening Federal Environmental, Energy, and Transportation Management

EO 13514
Federal Leadership in Environmental, Energy, and Economic Performance

EO 13589
Promoting Efficient Spending

Federal Acquisition Regulation
Government Printing and Binding Regulations (Available at https://www.acquisition.gov/.)

67 FR 36
Volume 67, Federal Register, p. 36 (Available at http://www.archives.gov/federal-register/.)

General Records Schedule 21
Audiovisual Records, Transmittal No. 8, December 1998 (Available at http://www.archives.gov/records-mgmt/grs/grs21.html/.)

Homeland Security Presidential Directive/HSPD 12
Policy for a Common Identification Standard for Federal Employees and Contractors (Available at http://www/archives.gov/.)

OMB Cir A–11
Preparation, Submission, and Execution of the Budget (Available at http://www.whitehouse.gov/.)

OMB Cir A–76
Performance of Commercial Activities (Available at http://www.whitehouse.gov/.)

OMB Cir A–130
Management of Federal Information Resources (Available at http://www.whitehouse.gov/.)

PL 104–208
Federal Financial Management Improvement Act of 1996

PL 107–314
Bob Stump National Defense Authorization Act for Fiscal Section Year 2003

SB 700–20 (EM 0007 FEDLOG)
Cataloging of Supplies and Equipment, Army Adopted Items of Materiel and List of Reportable Items (Available at https://apd.army.mil/.)

5 CFR 2635
Standards of Ethical Conduct for Employees of the Executive Branch

36 CFR Chapter 7
Library of Congress

36 CFR 1194
Electronic and Information Technology Accessibility Standards

36 CFR 1237
Audiovisual, Cartographic, and Related Records Management

2 USC Subtitle F
(P.L. 104–191, also known as Health Insurance Portability and Accountability Act of 1996 (HIPAA)). Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform (Available at http://thomas.loc.gov/.)

5 USC 552
Freedom of Information Act (Available at http://www.justice.gov/.)

5 USC 552a
The Privacy Act

5 USC Appendix 2
The Federal Advisory Committee Act

10 USC 1588 (f)
Authority to accept certain voluntary services

10 USC 2222
Defense business systems: architecture, accountability, and modernization

10 USC 2223
Information Technology: Additional Responsibilities for Chief Information Officers

10 USC 2667
Leases: non-excess property of military departments

10 USC 2686
Utilities and Services: Sale; Expansion and Extension of Systems and Facilities

10 USC 3014
Office of the Secretary of the Army

15 USC 96
Electronic Signatures in Global and National Commerce

17 USC 101
Definitions

17 USC 501
Infringement of Copyrights

18 USC 701
Official Badges, Identification Cards, Other Insignia

20 USC 9201
Adult Education and Literacy

29 USC 794d
(Section 508 of the Rehabilitation Act Amendments of 1998, as amended by Section 2405 of the FY 2001 Military Appropriations Act (PL 105–220)) (Available at http://www.gpoaccess.gov/.) Electronic and Information Technology

31 USC 1341
The Anti-Deficiency Act

40 USC 762
Public Buildings, Property, And Works (PL 100–542, Telecommunications Accessibility Enhancement Act of 1988.)

40 USC Subtitle III
(Clinger-Cohen Act (CCA)). Information Technology Management (Available at http://uscode.house.gov/.)

44 USC 15
Federal Register and Code of Federal Regulations (http://www.archives.gov/.)

44 USC 29
Records Management by the Archivist of the United States and by the Administrator of General Services (Available at http://www.gpoaccess.gov/.)

44 USC 31
Records Management By Federal Agencies (Available at http://www.gpoaccess.gov/.)

44 USC 33
Disposal of Records (Available at http://www.gpoaccess.gov/.)

44 USC 35
Coordination of Federal Information Policy

44 USC 36
Management and Promotion of Electronic Government Services

44 USC 3506
Public Printing and Documents: Federal agency responsibilities

47 USC 5 Sec 225
Telecommunications services for hearing-impaired and speech-impaired individuals

47 USC 5 Sec 611
Closed-captioning of public service announcements (http://uscode.house.gov/search/criteria.shtml/.)

RCS DD–PA (AR)–1381
Visual Information Production Request and Report

RCS CSIM–46
Information Management Requirement/Project Document

RCS CSIM–59
VI Annual Workload and Cost Data Report

ISO 9001:2008
International Standards Organization (Available at: http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm/.)

Section III
Prescribed Forms

Unless otherwise indicated, DA forms are available on the APD Web site (http://www.apd.army.mil); DD forms are available from the OSD Web site (http://www.dtic.mil/whs/directives/infomgt/forms/index.htm/).

DA Form 3903
Multi-media/Visual Information (M/VI) Work Order (Prescribed in table 5–1.)

DA Form 4103
Visual Information (VI) Product Loan Order (Prescribed in table 5–1.)

DA Form 5695
Information Management Requirement/Project Document (Prescribed in para 5–3 and table 5–1.)

DD Form 1367
Commercial Communications Work Order (Prescribed in table 5–1.)

DD Form 1995
Visual Information (VI) Production Request and Report (Prescribed in paras 5–3*b*(1) and C–4.)

DD Form 2537
Visual Information Caption Sheet (Prescribed in table 5–1.)

DD Form 2858
Visual Information Activity Profile (Prescribed in paras 5–3*b*(1) and 5–3*b*(4).)

Section IV
Referenced Forms

Unless otherwise indicated below, the following forms are available: DA forms are available on the APD Web site (http://www.apd.army.mil); and DD forms are available on OSD Web site (http://www.dtic.mil/whs/directives/infomgt/forms/index.htm/).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes for Publications and Blank Forms

DD Form 1391
FY ____ Military Construction Project Data

DD Form 2930
Privacy Impact Assessment

Appendix B
Army Portfolio Management Solution Registration Business Rules

B–1. General

The APMS is used for two primary functions—

a. For compliance reporting, including FISMA, SFIS/FFMIA, E–Authentication, interoperability, privacy and privacy impact assessments, Clinger-Cohen, PKI, and so forth; as well as Defense Business Systems (DBS) that must go before the Defense Business System Management Committee (DBSMC).

b. For portfolio and investment management, to ensure hardware, software or services are managed for strategic alignment, performance, environmental impact, risk, cost, redundancy, and gaps.

c. All Army IT, including computing infrastructure, hardware, software, services, initiatives, prototypes, and investments, regardless of funding source or amount, must be registered or accounted for as a component of another record in APMS. Any system requiring an accreditation or other specific compliance reporting requirement, regardless of funding source or amount, must be registered. IT will not be double reported, but relationships will be identified using the "Parent/Child Relationships" tab.

B–2. Department of Defense Information Technology Portfolio Repository

The APMS is the feeder system to the Department of Defense IT Portfolio Repository (DITPR). There are two types of registrations in APMS:

a. Department of Defense Information Technology Portfolio Repository-reportable. This includes any investment that requires any compliance reporting, as well as all defense business systems, including modified COTS. Refer to the DITPR Guidance, 2007–2008 for additional guidance on general and specific registration criteria. The guidance can be found on the APMS Resource Center on AKO.

b. Non-Department of Defense Information Technology Portfolio Repository-reportable. This is an investment for which the Army is not the lead agent but uses an Army appropriation. These investments will be reported to DITPR by the owning service component or agency. Command-unique IT is often registered as "Non-DITPR-reportable" using the Command Detail folder in APMS.

B–3. Registration

A video to complete the registration process can be found on the APMS Resource Center Portal. Regardless of registration method (DITPR-reportable or Non-DITPR-reportable) you must complete the entire registration process. The IT can be consolidated under an individual record if, collectively, the IT provides a total capability and the individual components do not have separate compliance-reporting requirements. Mission applications and systems should not be consolidated under a parent network record; the functional proponent or champion of the investment will register the application or system. Network tools and components may be consolidated with the associated network record. One example of IT that could be consolidated under one or more records by the organization is end-user computing IT (see para B–5*h*, below).

B–4. Army Portfolio Management Solution folders

a. For DITPR-reportable items the following folders are required:

(1) Required Data folder.
(2) Financial Data folder.
(3) Decision Support folder.
(4) Joint Common Systems Function List.

b. The following documents are required for Non-DITPR reportable items:

(1) Required Data folder (Army Required and Parent/Child Relationships only).
(2) Financial Data folder.
(3) Decision Support folder.
(4) Joint Common Systems Function List.

c. All applicable types of appropriations must be listed on the Financial Data folder (for example, operation and maintenance, other procurement, RDT&E, MILCON). Identify all hardware, software, and services that support an investment on the Components tab of the Command Detail folder. This information will be used to validate Goal 1 waiver requests.

B–5. Information technology infrastructure and naming conventions

Individual records will be added for the infrastructure investments outlined below, which may include a consolidation of hardware, software, and services. If a record already exists in APMS for your infrastructure, you are not required to change the name to meet the naming conventions described below. If further delineation is necessary for any investment name, use the appropriate office symbol as identified at https://www.arims.army.mil/ and in accordance with AR 25–59.

a. Data centers or continuity of operations plan sites are defined as a collection of computers, data storage systems, and ancillary equipment in a specialized space used for computing resources. For naming convention, data centers will begin with the words DATA CENTER or DC and then the installation, command, or unit name (for example, DATA CENTER–BENNING or DC–BENNING). Data center records include, but are not limited to, the following:

(1) Blade servers and racks.

(2) Mainframe and mini computers.

(3) Storage area and storage area network devices.

(4) Matrix switches used to interconnect equipment.

(5) Optical storage systems.

(6) Tape drives and tape storage devices.

(7) High-speed printers.

b. All IT laboratories and virtual reality and simulation centers or labs, including systems used to test network and computer equipment, operating systems and other software systems, as well as any other lab environments that contain a significant amount of network or computer equipment. For naming convention, labs will begin with the word LAB and then the lab's purpose or unit name and location (for example, LAB–AVIATION SIMULATION–LOCATION). These investments will be binned in the EIEMA Computing Infrastructure Domain.

c. All telephone switching equipment owned by the Army. For naming convention, telephone systems will begin with the words Private Branch Exchange (PBX) or voice system and then the installation name (for example, PBX–MCCOY). These records will be binned in the EIEMA Communications Domain. These records include—

(1) All PBX systems.

(2) All major key systems.

(3) All central office-class switching systems.

(4) VoIP equipment when attached to the PBX or switch, unless provided over the LAN through LAN routers.

(5) All multiplexors, main distribution frames (MDF), intermediate distribution frames (IDF), and other wiring.

(6) The system above would include the cost of telephones purchased to upgrade or support the systems.

d. All networks (including unique or special use) at each installation. Mission applications or systems are not to be consolidated under a network record in APMS (use Parent/Child tab to establish relationship). These records will be binned in the EIEMA Communications Domain. Examples include—

(1) Medical Network (MEDNET).

(2) SIPRNET.

(3) Secure NIPRNET.

(4) Other specialty networks.

e. All regional hub nodes (RHNs), including all satellite, radio, switching, and multiplexing equipment and encryption equipment. For naming convention, regional hub nodes will begin with the words Regional Hub Node (RHN) in the name and then have the regional designation (for example, RHN–NETOPSV1.0). These records will be binned in the EIEMA Communications Domain.

f. All collections of audio and visual conferencing hubs used as switching centers for large shared video or audio teleconferencing, when it is owned by the Army. These records will be binned in the EIEMA Communications Domain. For naming convention, audio and visual (AV) records will begin with AUDIO VISUAL followed by the installation or location and then the organization name (for example, AUDIO VISUAL–SHAFTER–ORG).

g. A common-user infrastructure (CUI) record in APMS is used to collect data for end-user computing hardware, software, and services. The CUI records do not include any IT that requires a stand-alone accreditation or is purchased as a single investment-those require a regular record in APMS. The APMS command administrators may choose to register infrastructure records down to the sub-organization level for better fidelity but will have a minimum of one CUI record to consolidate their end-user computing IT. The CUI records are non-DITPR reportable. These records will be binned in the EIEMA Computing Infrastructure Domain. For naming convention, common-user infrastructures will start with CUI then the command name and the organization office symbol (for example, CUI–COMMAND-office symbol). The CUIs include, but are not limited to the following:

(1) Desktops.

(2) Laptops.

(3) BlackBerry smart phones.

(4) PDAs.

(5) Printers.

(6) Facimile.

(7) Scanners.

(8) Desktop applications that do not require a stand-alone record in APMS.

h. Mission-computing infrastructure is used to support a unique mission requirement that is not a common user infrastructure and not captured as part of another record in APMS. Mission-computing infrastructure includes Web-enabled mission databases or portals not on AKO, and the services contracts that support their development or sustainment. Mission-computing infrastructure will start with MCI, then the command name, the organization, and the type of initiative (for example, MCI–COMMAND–ORGANIZATION–Portal). These records will be binned in the EIEMA Computing Infrastructure Domain.

Appendix C
Internal Control Evaluation

C–1. Function
The function covered by this checklist is the administration of Army IM and IT organizations. This includes key controls for CIO management, command senior IM officials, IA, C4/IT support and services, VI management, records management, and publishing management.

C–2. Purpose
The purpose of this checklist is to assist HQDA, FOAs, ACOMs, ASCCs, DRUs, PEOs, PMs, and installations in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.

C–3. Instructions
Answers must be based on the actual testing of internal controls (such as document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least once every five years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

C–4. Test questions
a. Responsibilities. (chap 2.) Have C4/IT plans, programs, and requirements been coordinated with the appropriate IM and IT managers? (All)

b. Army information technology management. (chap 3.)

(1) Are the duties and responsibilities of the senior information management official clearly designated in the organization's mission and function? (HQDA, region, ACOM, ASCC, and DRU.)

(2) Has the installation clearly established a NEC who has the sole responsibility of implementing the installation's IM and IT program? (IMCOM.)

(3) Has the organization analyzed (and documented the analysis of) its mission and revised mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes? (HQDA, ACOM, ASCC, and DRU.)

(4) Does the organization have a strategic plan that is linked to its mission? Is it periodically updated? (ACOM, ASCC, and DRU.)

(5) Has a forum been established to develop and implement C4/IT procedures, requirements, and priorities? (ASCC and DRU.)

(6) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (HQDA, ACOM, ASCC, and DRU.)

(7) Does the IT investment screening process include addressing the questions in this checklist, resolving all issues prior to making an IT investment, and initiating any process analysis or improvement? (HQDA, ACOM, ASCC, and DRU.)

(8) Does the process support core or priority mission functions? (HQDA, ACOM, ASCC, DRU, and FOA.)

(9) Can the process be eliminated? (HQDA, ACOM, ASCC, and DRU.)

(10) Can the process be accomplished more effectively, efficiently, and at less cost by another Government source (for example, DOD or other Federal agency) or the private sector? (HQDA, ACOM, ASCC, and DRU.)

(11) Does the IT investment process clearly establish who in the organization has the responsibility and authority for making final IT-related investment decisions? (HQDA, ACOM, ASCC, and DRU.)

(12) Are exceptions to the IT investment screening process clearly documented? (HQDA, ACOM, ASCC, and DRU.)

(13) Does the organization require that management evaluations for the IT investment-screening process, as well as scoring, ranking, and prioritization results, be documented (either manually or through the use of automated applications such as a decision support tool)? (HQDA, ACOM, ASCC, and DRU.)

(14) Are IT investment decisions a part of the organization's integrated capital-planning process or are IT projects separated out? (HQDA, ACOM, ASCC, and DRU.)

(15) Does the organization have a process in place to conduct periodic reviews (in-house or via outside consultant or expert) of its current IT investment portfolio to assess alignment with mission needs, priorities, strategic direction, or major process reengineering? (HQDA, ACOM, ASCC, and DRU.)

(16) Does the organization have a process for documenting and disseminating results of this review? (HQDA, ACOM, ASCC, and DRU.)

(17) Are process analysis and improvements for Warfighter processes documented in the initial capabilities document using the doctrine, organization, training, materiel, leadership, and education, personnel, and facilities

(DOTMLPF) requirements methodology as defined by the Army requirements generation process in AR 71–9? (HQDA, ACOM, ASCC, and DRU.)

(18) Have Web-enabling status and future Web-enabling plans been reported within the APMS–AITR? (All)

(19) Have functional managers developed a set of goals and objectives (with performance measures) to gauge overall functional mission improvement? Have accomplishments been reported to enterprise-level managers? (All)

(20) Have performance measures been developed for each IT investment that supports the organizational mission before execution of that investment? (HQDA, ACOM, ASCC, DRU, PEO, and PM.)

(21) Have IT investments been synchronized to overall DOD and Army mission priorities? (HQDA, ACOM, ASCC, DRU, PEO, and PM.)

(22) Are performance measures linked to management-level goals, objectives, and measures? (All)

(23) Are requirements being developed in harmony with the Army's goal of creating an end-state strategy of implementing an ERP business solution throughout a fully integrated Army logistics environment? (HQDA and ACOM)

(24) Are financial, logistics, facilities, human resources, contractors, and other senior Army leaders held accountable for ensuring business processes comply with financial audit standards? (HQDA)

(25) Has the organization published a policy on the issuance of IT devices to employees based upon mission and assigned position rather than the grade or rank of the individual? Does the policy minimize the number of IT devices per employee and provide the least amount required for the assigned mission? (All)

c. Information assurance (see AR 25–2).

d. Visual information (chap 5).

(1) Does the mission guidance include the responsibilities of the VI manager, to include organization structure and responsibilities of all components of the organization, and does it state that this VI manager provides overall policy, plans, and standards for all VI operations? (HQDA.)

(2) Is the VI manager the single staff manager for all VI functions on the installation? (HQDA.)

(3) Are all VI services and equipment, except those specifically exempted by the HQDA, consolidated for centralized VI management? (HQDA.)

(4) Do all VI activities under the theater-level Signal Command's purview have a DVI authorization number (DVIAN)? (HQDA.)

(5) Does the VI manager approve all VI equipment required by AR 25–1, chapter 5? (HQDA.)

(6) Is VI policy being followed for M/VI productions? (For example, DD Form 1995 is used, funds identified up front, PIN registers maintained, Content Discovery and Access Catalog searches conducted, service support contracts awarded for less than 50 percent of the total production cost, non-local Content Discovery and Access Catalog entries, and using JVIS contracting facility.) (FOA and installation.)

(7) Is a production folder maintained for the life cycle of local productions? (HQDA, FOA, and installation.)

(8) Has your VI activity developed and implemented a standard level of agreement document, to including an SOP? (Installation.)

e. Records management (see DA Pam 25–403).

f. Publishing and printing management (see AR 25–30).

g. Enterprise architecture (chap 6). (All, as applicable)

(1) Has the organization developed the appropriate architectures for the Army Knowledge EA to support the DOTMLPF components as mapped to net-centric data and services?

(2) Has the organization developed the appropriate architectures for the mission command architecture that supports JCIDS, acquisition of system of systems and Family of systems, force development, and lessons learned from operations?

(3) Has the organization developed the appropriate architectures for the Army BEA to support the migration of current systems infrastructure, net-centric warfare, enterprise application integration, and business-process modernization; and align with the five DOD BEA Core Business Missions: weapon systems life-cycle management, materiel supply and service management, real property and installations life cycle, human resources management, and financial management?

h. Installation information technology services and support.

(1) Is a process in place for acquiring IT and ensuring all required licensing and registration are accomplished? (NEC.)

(2) Is the NEC the single organization responsible for the oversight and management of installation IT? (NEC.)

(3) Are periodic reviews of current IT being conducted to ensure they are still required and meeting user needs? (HQDA, ACOM.)

(4) Are quarterly reviews of current IT within the APMS–AITR being conducted and have the users verified that they are still required and meeting users' needs? (HQDA, ACOM.)

(5) Are evaluations being conducted of existing systems for obsolescence? (HQDA, ACOM.)

(6) Has a BCA been performed prior to implementing the thin client concept? (NEC.)

(7) Is an accurate inventory being maintained and validated annually for IT equipment? (NEC, IMO.)

(8) Are COOP plans and procedures documented, distributed, and tested at least annually? (ACOM, NEC.)

(9) Has guidance been provided to ensure all software is checked for viruses before being loaded? (NEC.)

(10) Are existing capabilities and assets considered prior to upgrading, improving, or implementing LANs? (Theater-level signal command and NEC.)

(11) Are uneconomical IT service contracts identified and terminated? (All.)

(12) Has the NEC coordinated the acquisition of licenses with the CHESS office prior to entering into an agreement with a COTS vendor? (NEC.)

(13) Are spare capacity and functional expansion of IT being considered or used when new requirements are identified? (All.)

(14) Has the NEC reported the server consolidation status for all of its Army tenants to the Army CIO/G–6? (NEC.)

(15) Are measures being taken to ensure that hard drives are disposed of properly? (NEC.)

(16) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (Signal Command (Theater), and NEC.)

(17) Has guidance been provided to review and revalidate cellular telephones and pagers every 2 years? (Theater-level signal command, and NEC.)

(18) Do procedures require the establishment of a reutilization program to identify and turn in cellular phones and pagers that are no longer required or seldom used? (NEC.)

(19) Is there a requirement for cellular phones and pagers to be recorded in the property book? (NEC.)

(20) Has the NEC implemented accountable billing procedures? (NEC.)

(21) Have maintenance and support strategies been devised to minimize overall systems life cycle cost at an acceptable level of risk? (PEO, PM, and ACOM.)

(22) Have program managers, project managers, and IT MATDEVs coordinated their system architectures and fielding plans with the gaining commands and DRUs, Theater-level signal command, and installation NECs prior to fielding systems? (PEO and PM.)

(23) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (Theater-level signal command, NEC, and IMO.)

(24) Are private-sector service providers made aware that written assurance of compliance with software copyright laws may be required? (Theater-level signal command, NEC, and IMO.)

(25) Are existing portals being migrated to AKO and AKO–SIPRNET? (All.)

(26) Does each Web site contain a clearly defined purpose statement that supports the mission of the organization? (All.)

(27) Are users of each publicly accessible Web site provided with privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service? (All.)

(28) If applicable, does the Web site contain a disclaimer notice for links to any site outside of the official DOD Web information service (usually the .mil domain)? (All.)

(29) Is the Web site free of commercial sponsorship and advertising? (All.)

(30) Is the Web site free of persistent cookies or other devices designed to collect PII about Web visitors? (All.)

(31) Is each Web site made accessible to disabled users in accordance with Section 508 of the Rehabilitation Act? (All.)

(32) Is the operational information identified below purged from publicly accessible Web sites? (All,)

(a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

(c) Personal information about U.S. citizens, DOD employees, and military personnel, to include the following: Social Security numbers; dates of birth; home addresses; directories containing name, duty assignment, and home telephone numbers; names; locations; or any other identifying information about Family members of DOD employees or military personnel.

(d) Technological data such as weapon schematics, weapon system vulnerabilities, electronic wire diagrams, and frequency spectrum data.

(33) Are operational security tip-off indicators in the following categories purged from the organization's publicly accessible Web site? (All.)

(a) Administrative. Personnel travel (personal and official business), attendance at planning conferences, commercial, support contracts, and FOUO information.

(b) Operations, plans, and training. Operational orders and plans; mission-specific training; exercise and simulations activity; exercise, deployment, or training schedules; unit relocation or deployment information; inspection results, findings, and deficiencies; unit vulnerabilities or weaknesses.

(c) Communications. Spectrum emissions and associated documentation; changes in activity or communications patterns. Use of Internet and email by unit personnel (personal or official business); availability of secure communications; hypertext links with other agencies or units; and Family support plans, bulletin board postings, or messages between Soldiers and their Family members.

(d) Logistics and maintenance. Supply and equipment orders and deliveries; transportation plans; mapping; imagery and special documentation support; maintenance and logistics requirements; and receipt or installation of special equipment.

(34) Has the Web site reviewer performed a key word search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible Web sites? (All) Deployment schedules; duty rosters; exercise plans; contingency plans; training schedules; inspection results, findings, and deficiencies; biographies; Family support activities; phone directories; and lists of personnel.

(35) Are existing infrastructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA and ACOM.)

(36) Is the fully qualified domain name (for example, https://www.us.army.mil or http://www.apd.army.mil) for Army sites registered with the Government Information Locator Service at http://defense.gov/RegisteredSites/submitlink.aspx/ and the contact information updated annually?

(37) Are the Web servers IAVA-compliant and placed behind a reverse proxy server?

C–5. Supersession

This checklist replaces the checklist for the administration of Army IM and IT previously published in AR 25–1, dated 4 December 2008.

C–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to CIO/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (cio-g6.policy.inbox@mail.mil).

Glossary

Section I
Abbreviations

AASA
Administrative Assistant to the Secretary of the Army

ACAT
acquisition category

ACOM
Army command

ACSIM
Assistant Chief of Staff for Installation Management

ADCCP
Army Data Center Consolidation Plan

ADS
authoritative data source

AEA
Army Enterprise Architecture

AIA
Army Information Architecture

AIC
Army interoperability certification

AKO
Army Knowledge Online

AKO–S
Army Knowledge Online SIPRNET

AMC
Army Materiel Command

APMS
Army Portfolio Management System

APP
Army Publishing Program

ARIMS
Army Records Information Management System

ARNG
Army National Guard

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

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

ASCC
Army service component command

BEA
Business Enterprise Architecture

C2
command and control

C4
command, control, communications, and computers

C4IM
command, control, communications, and computers for information management

C4ISR
command, control, communications, computers, intelligence, surveillance, and reconnaissance

C4/IT
command, control, communications, computers, and information technology

C&A
certification and accreditation

CAC
common access card

CAP
Computer/Electronic Accommodations Program

CCA
Clinger-Cohen Act

CFR
Code of Federal Regulations

CG
commanding general

CHESS
Computer Hardware, Enterprise Software Solutions

CIO
chief information officer

CIO/G–6
Chief Information Officer, G–6

CJCSI
Chairman of the Joint Chiefs of Staff Instruction

CND
computer network defense

CNGB
Chief, National Guard Bureau

COI
community of interest

COMCAM
combat camera

COMSEC
communications security

CONUS
continental United States

COOP
continuity of operations

CoP
community of practice

COTS
commercial off-the-shelf

CP–34
Career Program 34

CPIM
Capital Planning and Investment Management

CPU
central processing unit

CTA
common table of allowances

DA
Department of the Army

DAA
designated approval authority

DCS
Deputy Chief of Staff

DIACAP
DOD Information Assurance Certification and Accreditation Process

DISA
Defense Information Systems Agency

DISN
Defense Information Systems Network

DISR
DOD Information Technology Standards Registry

DITPR
DOD Information Technology Portfolio Repository

DM
data management

DMZ
demilitarized zone

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DOIM
Director of Information Management

DOTMPLF
doctrine, organization, training, materiel, leadership and education, personnel, and facilities

DPPS
data performance plan system

DRMS
Defense Reutilization and Marketing Service

DRU
direct reporting unit

DSN
defense switched network

EA
enterprise architecture

EB
Executive Board

e–Gov
electronic government

EIT
electronic and information technology

ELA
enterprise license agreement

EO
executive order

ERP
enterprise resource planning

ESA
enterprise software agreement

FAR
Federal Acquisition Regulation

FISMA
Federal Information Security Management Act of 2002

FM
Field Manual

FOA
field operating agency

FOIA
Freedom of Information Act

FORSCOM
Forces Command

FOUO
for official use only

FRP
full-rate production

FY
fiscal year

GIG
global information grid

GOSC
general officer steering committee

GSA
General Services Administration

HIPAA
Health Insurance Portability and Accountability Act

HQDA
Headquarters, Department of the Army

I3A
installation information infrastructure architecture

I3MP
Installation-Information Infrastructure Modernization Program

IA
information assurance

IAM
information assurance manager

IAVA
Information Assurance Vulnerability Alert

IESS
Information Exchange Standards Specifications

ILS
integrated logistics support

IM
information management

IMCOM
Installation Management Command

IMO
information management officer

INSCOM
Intelligence and Security Command

IP
Internet protocol

IRB
investment review board

IS
Information System

ISO
International Standards Organization

ISP
Internet service provider

IT
information technology

ITM
information technology management

JFHQ
Joint Forces Headquarters

JS
Joint staff

JWICS
Joint Worldwide Intelligence Communication System

MATDEV
materiel developer

MEDCOM
Medical Command

MILCON
military construction

MIP
Military Intelligence Program

MOA
memorandum of agreement

MSC
major subordinate command

MWR
Morale, Welfare, and Recreation

NAF
nonappropriated fund(s)

NAFI
nonappropriated fund instrumentality

NATO
North Atlantic Treaty Organization

NEC
Network Enterprise Center

NETCOM
Network Enterprise Technology Command

NIPRNET
non-secure Internet protocol router network

NSS
National Security System

OA
operational architecture

OCONUS
outside the continental United States

OMB
Office of Management and Budget

OV
operational view

PC
personal computer

PEO
program executive officer

PIA
privacy impact assessment

PII
personally identifiable information

PKI
Public Key Infrastructure

PL
public law

PM
program manager

POA&M
plan of action and milestones

POC
point of contact

POM
program objective memorandum

PPBE
planning, programming, budgeting, and execution

PPSS
post-production software support

RDT&E
research, development, test, and evaluation

RM
records manager

RMDA
Records Management and Declassification Agency

SATCOM
satellite communications

SCI
sensitive compartmented information

SECARMY
Secretary of the Army

SIPRNET
secret Internet protocol router network

SLA
service level agreement

SSA
service and support agreement

SSL
secure socket layer

SV
system view

TA
technical architecture

TDA
table of distribution and allowances

TE
test and evaluation

TNOSC
Theater Network Operations and Security Center

TOE
table of organization and equipment

TRADOC
Training and Doctrine Command

TTP
tactics, techniques, and procedures

UID
unique identifier

URL
uniform resource locator

USACE
United States Army Corps of Engineers

USAISEC
United States Army Information Systems Engineering Command

USAR
U.S. Army Reserve

USC
United States Code

USSOCOM
United States Special Operations Command

VI
visual information

VIDOC
visual information documentation

W3C
World Wide Web Consortium

WMA
warfighting mission area

XML
eXtensible markup language

Section II
Terms

Activity
An Army organization. Within the context of the AEA, a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes in support of accomplishing tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element.

Acquisition
The acquiring of supplies or services (including construction) with appropriated funds and for the use of the Federal Government through purchase or lease; whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established; and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

Administrative work processes
Enabling activities that support mission and mission-related processes and functions (for example, manage legal process, performance assessment, combat health support, Family support, and so on).

Army Net-Centric Data Management Program
Establishes policy, guidance, and instruction about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data.

Application
Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, or facilitating email. For purposes of reporting in APMS, applications may be reported as a separate

investment or included in an information system registration. If reported as a separate investment, applications will identify in the dependency tab, the host system it resides on as the parent information system.

Architecture
See enterprise architecture and Army enterprise architecture.

Army business enterprise architecture
The framework of business processes and organizations that support the Army's Warfighters.

Army enterprise architecture
See also enterprise architecture. The AEA transforms operational visions and associated required capabilities of the business and warfighting missions into a blueprint for an integrated and interoperable set of information systems and NSS that implement horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA supports the LandWarNet and is the combined total of all the Army's operational, technical, and system architectures.

Army enterprise infrastructure
The systems and networks that comprise the LandWarNet.

Army interoperability certification
Certification from CIO/G–6 that the candidate system has undergone appropriate testing and that the applicable standards and requirements for compatibility, interoperability, and integration have been met.

Army knowledge management
The Armywide strategy to transform the Army into a network-centric and knowledge-based force to improve information dominance by our Warfighters and business stewards. It includes, but is not limited to, improving processes, technology, and work culture to collaborate, catalog, store, find, and retrieve information; and share this information with Joint, coalition, and international partners as mission needs dictate.

Army Recordkeeping Systems Management
Cost-effective organization of Army files and records contained in any media so that records are readily retrievable. Ensures that records are complete; facilitates the selection and retention of permanent records; and accomplishes the prompt disposition of noncurrent records in accordance with National Archives and Records Administration approved schedules.

Army Web site
A collection of hypertext markup language pages, graphics, images, video, audio, databases, or other media assets at a URL, which is made available for distribution or is distributed or transmitted (with or without limitation) via the World Wide Web for reception and display on a computer or other devices including but not limited to mobile phones, PDA's or interactive television; and whose content is controlled, authorized, or sponsored by an Army organization or representative.

Attribute
A property or characteristic of one or more entities (for example, race, weight, or age). Also, a property inherent in an entity or associated with that entity for database purposes.

Authentication
A security service that verifies an individual's eligibility to receive specific categories of information.

Authoritative data source
A recognized or official data-production source (with a designated mission statement, source, or product), which publishes reliable and accurate data for subsequent use by customers. An ADS may be the functional combination of multiple, separate data sources.

Automation
Conversion of a procedure, process, or equipment to automatic operation. When allied to telecommunications facilities, automation may include the conversion to the automatic operation of the message processing at an exchange or remote terminal.

Bandwidth
The rate at which an amount of data can be sent through a given transmission channel.

Benchmark
A procedure, problem, or test that can be used to compare systems, components, processes, and so forth to each other or to a standard.

Beneficial occupancy date
Construction complete; user move-in dates.

Broadcast
The transmission of radio, television, and data signals through the air waves or fiber optic cable.

Business enterprise architecture
The EA for DOD's business information infrastructure; includes processes, data, data standards, business rules, operating requirements, and information exchanges. The BEA serves as the blueprint to ensure the right capabilities, resources, and materiel are rapidly delivered to Warfighters by ensuring accurate, reliable, timely, and compliant information across DOD.

Business and functional process improvement
A systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes in order to achieve improvements in performance in areas important to customers and stakeholders. (See also DODD 8000.01.)

Capability
In the context of the AEA framework, a capability satisfies a requirement, specifically an IT requirement. For example, an Army headquarters element has the requirement to know the location of all friendly and enemy units in its area of operations. Situational awareness is the capability that satisfies this requirement.

Capital Planning and Investment Management
The CPIM process is to develop C4/IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4/IT expenditures across all functional domains. The CPIM process is collaborative among C4/IT stakeholders, with a focus on C4/IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets.

Closed-circuit television
Point-to-point signal transmission by cable or directional radiation where the audience is limited by physical control or nonstandard transmission.

Command and control
Exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. These functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are used by a commander to plan, direct, coordinate, and control forces and operations for the accomplishment of the mission.

Command and control system
Any system of facilities, equipment (including hardware, firmware, and software), communications, procedures, and personnel available to commanders at all echelons and in all environments; and essential to plan, direct, and control operations conducted by assigned resources.

Command, control, communications, and computers for information management services list
The source document that defines the Army Enterprise baseline and mission IT services provided or supported by the NEC. This list of service definitions is the foundation for the development and publishing of the customer-facing LandWarNet services catalog. The C4IM services listed as baseline are core or common user services that are the responsibility of the Army to centrally fund. Those services listed as "Mission" are the responsibility of the ACOMs/ Mission Commanders to resource. These services are not in the baseline, but are required based on the mission (for example, cell phones, pagers, personal digital assistants) and are grounded by the business processes that enable mission execution in a more efficient and effective manner.

Command, control, communications, and computer systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications, and computers.

Common use
Services, materiel, or facilities provided by a DOD agency or a military department on a common basis for two or more DOD agencies, elements, or other organizations as directed.

Communications
See telecommunications.

Communications network
A set of products, concepts, and services that enables the connection of computer systems for the purpose of transmitting data and other forms (for example, voice and video) among the systems.

Communications security
Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Communications systems
A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

Communities of interest
The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes; and who therefore must have a shared vocabulary for the information they exchange.

Community of practice
A community of practice (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. CoPs cut across formal organizational structures and increase individual and organizational agility and responsiveness by enabling faster learning, problem solving, and competence building; greater reach to expertise across the force; and quicker development and diffusion of best practices. CoP structures range from informal to formal and may also be referred to as structured professional forums, knowledge networks, or collaborative environments.

Compatibility
The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

Compliance
A system that meets, or is implementing an approved plan to meet, all applicable TA mandates.

Component
One of the subordinate organizations that constitute a Joint force. Normally, a Joint force is organized with a combination of Service and functional components. An assembly or any combination of parts, subassemblies, and assemblies mounted together in the manufacture, assembly, maintenance, or rebuild.

Concept
A document or theory that translates a vision or visions into a more-detailed, but still abstract, description of some future activity or end-state, principally concerned with a 3- to 15-year time frame.

Configuration
An expression in functional terms (that is, expected performance) and physical terms (that is, appearance and composition).

Connection fee
The charge, if any, imposed on a subscriber by the cable television franchisee for initial hookup, reconnection, or

relocation of equipment necessary to transmit the cable television signal from the distribution cable to a subscriber's receiver.

Content Discovery and Access Catalog
An online, unrestricted, full-text searchable, standard DOD-wide database containing content description, production, acquisition, inventory, distribution, currency status, archival control, and other data on VI productions and DLC products typically used in military training. Formerly DAVIS/DITIS.

Context
The interrelated conditions that compose the setting in which the Architectures exist. It includes environment, doctrine, and tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

Cookie
A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the hypertext markup language information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Cookies normally expire after a single session.

Cost-effective
Describes the course of action that meets the stated requirement in the least-costly method. Cost-effectiveness does not imply a cost savings over the existing or baseline situation; rather, it indicates a cost savings over any viable alternative to attain the objective.

Data
The representation of facts, concepts, or instructions in a formal manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities to which meaning is, or might be, assigned (see JP 1–02).

Database
A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications.

Data element
A basic information unit template that is built on standard semantics and structures, and that in turn governs the distinct values of one or more columns of data within a row of data within a database table or a field within a file.

Data management
The process of creating a basis for posting, sorting, identifying, and organizing vast quantities of data available to DOD.

Data model
A graphical and textual representation of data needed by an organization to represent achievement of its mission, functions, goals, objectives, and strategies. A data model is represented by its entities, attributes, and relationships among its entities. In the relational model of data, entities are tables, attributes are columns, and relationships are primary and foreign key pairs. Data models may be enriched beyond data structures with both constraints and embedded processes.

Data performance plan
An organized and structured approach to the specification and collection of enterprise artifacts in support of COI objectives, and operate in a common and shared fashion. Data performance planning collects, develops, and maintains these artifacts and is of primary interest to information system professionals charged with ensuring that information systems meet the needs of the COI. These artifacts are often referred to as "metadata."

Data Performance Plan System
A centralized repository for enterprise-wide storing, viewing, and reusing architectures, data models, business rules, and other artifacts associated with functional Army systems.

Data standards
Metadata expressed as ADSs, IESS, UIDs, and XML, and used to guide all data exchanges including those with legacy systems.

Data steward
A subject-matter expert who is under the direction of the Chief Data Officer and is responsible for developing, implementing, and enforcing Federal, Army, and their respective organization's data standards, processes, and procedures.

Defense business system
An information system other than a national security system operated by, for, or on behalf of the DOD. Includes financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. This includes any IT that supports generating force functions as outlined in FM 1–01 or performs functions that can be mapped to the BEA.

Defense Telephone System
A centrally managed system that, in accordance with its charter, provides telephone service to all DOD activities in the area.

Department of Defense Information Technology Standards Registry
DISR is a Joint effort to identify and mandate IT standards for use in the acquisition and development of DOD systems. It focuses on the inter-operability and standardization of information technology and supports net-centric operations and warfare.

Direct-reporting unit
An operational command that reports to and is under the direct supervision of an HQDA element. A DRU executes its unique mission based upon policy established by its HQDA principal.

Doctrine
Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative, but requires judgment in application. Doctrine represents consensus on how the Army conducts operations today.

Domain
An area of common operational and functional requirements. The four domains are C4I, weapon systems, modeling and simulation, and sustainment.

Electronic business (e-business)
A way of performing enterprise activities involving the use of electronic technologies, such as facsimile, email, World Wide Web software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

Electronic government (E–Gov)
The use of Web-based applications and other information technologies, combined with processes that implement these technologies, to: a) enhance access to and delivery of Government information and services to the public, other agencies, and other Government entities; or b) bring about improvements in Government operations that may include effectiveness, efficiency, service quality or transformation.

Electronic mail (email)
An information dissemination and retrieval service accessed through distributed user workstations normally provided through an office automation initiative.

Embedded technology
Specialized hardware and software that is wholly incorporated as part of a larger system or machine. Embedded technologies are the domain of the Warfighter. However, embedded technology is more than a tool necessary for operating the equipment to a capability of collecting, storing, and transmitting data. Embedded technology requires a strategic partnership between the warfighting and Army CIO/G–6 communities to ensure a seamless distribution of warfighting data Armywide. Embedded IT must comply with LandWarNet standardization, compatibility, inter-operability and security standards prescribed by the Army CIO/G–6.

Enterprise
The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise architecture
A strategic information asset base, that defines the mission, information, and technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. An EA includes a baseline architecture, a target architecture, and a sequencing plan (see 44 USC 3601).

Enterprise authoritative data source registry
An enterprise capability that enables a holistic view of DOD data sources, their relationships, and their responsible governance authorities. It is a Web-enabled interface with streamlined ADS registration and discovery capabilities that support the visibility of DOD data needs and the attribution of those needs to one or more authoritative bodies responsible for meeting or otherwise fulfilling those needs. For more information, see https://metadata.ces.mil.

Enterprise data
Data shared across systems, applications, and processes by organizations, branches, divisions, and other sub-units in the enterprise.

Enterprise information environment
The common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or assure, LANs, campus-area networks, tactical networks, operational-area networks, metropolitan-area networks and wide-area networks. The EIE is also composed of GIG organizational, regional, or global-computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The EIE included a common set of enterprise services, called Core Enterprise Services, which provide awareness, and delivery of information on the GIG.

Enterprise Multimedia and Visual Information Service Center
The VI activity that provides general support to all installation, base, facility or site organizations or activities. It may include motion picture, still photo, television, and audio recording for nonproduction documentary purposes, their laboratory support, graphic arts, VI libraries, and presentation services.

Enterprise network
The connection of all components, departments, organizations, and locations into a single standardized, compatible, interoperable, and secure intra-Army network. The single intra-Army network (Army enterprise network) integrates all systems in the Army (and all systems outside the Army requiring data exchange with the Army) to provide seamless information superiority that supports the Army's Joint, interagency, intergovernmental, multinational operations, and business missions. This translates to system-wide engineering, common strategy and architecture, and a single concept of operation and authority for network operations. The Army's enterprise is prescribed by the Army CIO. Enterprise network operations are under the single authority of Army Cyber Command.

Environment
The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.

Exhibit documents
Exhibit 53s and 300s are reporting requirements established by the Office of Management and Budgets for an agency's IT investment portfolio.

Extensible Markup Language
A tagging language used to describe and annotate data so that the data can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension.

Extranet
Similar to Government Intranet, an Extranet includes outside organizations, vendors, industry partners, and individuals outside the DOD GIG to facilitate inter-business transactions, such as placing and checking orders, tracking merchandise, and making payments. Extranets require access control via authorized external certificates.

Facsimile
A system of telecommunications for the transmission of fixed images with a view to their reception in a permanent

form. These images include typewritten and handwritten documents, fingerprint records, maps, charts, operations overlays, sketches, and low-resolution photographs.

Federal personnel
Officers and employees of the Government of the United States, members of the Uniformed Services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DOD dependents are considered members of the general public.

Federated architecture
An approach for EA development, which is comprised of a set of coherent but distinct entities or architectures, or the architectures of separate members of the federation. The members of the federation participate to produce inter-operable, effectively integrated EA. The federation sets the overarching rules of the federated architecture, defining the policies, practices, and legislation to be followed; as well as the inter-federated procedures and processes, date interchanges, and interface standards to be observed by all members of the federation. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission.

Franchise
Authorization, or renewal thereof, issued by a franchising authority; whether such authorization is designated as a franchisee, permit, license, resolution, contract, certificate, agreement, or otherwise, which authorizes the construction or operation of a cable system.

Franchisee
Any individual or partnership, association, joint stock company, or trust corporation who owns or controls, is owned or controlled by, or is under common ownership or control with such person.

Function
Within the context of the AEA framework, a synonym for activity.

Functional proponent
Commander or chief of an organization or staff element that is the operative agency charged with the accomplishment of a particular function(s) (see AR 5–22).

Global Information Grid
The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers, and support personnel.

GuardNet
The IT infrastructure of the National Guard securely supporting the NGB Joint team using nationwide information systems and a mission-command network spanning 11 time zones, 54 States and territories, and the District of Columbia at approximately 3,000 separate locations. GuardNet provides ARNG access to the Army's LandWarNet and Joint access to Air Force network services in those States.

Hardware
The generic term dealing with physical items as distinguished from the capability or function, such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. In data automation, the physical equipment or devices forming a computer and peripheral components. (See also software.)

Imagery
A pictorial representation of a person, place, thing, idea, or concept, either real or abstract, used to convey information.

Information
Any communication or representation of knowledge, such as facts, data, or opinion; in any medium or form including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Assurance Vulnerability Alerts
Positive control mechanism that pushes alerts and advisories about IA security vulnerabilities to IA personnel. IAVA also requires the tracking of response and compliance to the messages.

Information enterprise
The holistic, end-to-end approach of a variety of IT activities and tasks, which include infrastructure management, DM, networking, system engineering, database and software design and management, and the administration of entire systems resulting in an Armywide capability that covers the entire life cycle of information and knowledge. IE includes matters involving information technology, network defense, and network operations contributing to the Army's LandWarNet and DOD GIG. The Army's IE is the core domain of the Army CIO/G–6, which includes the people, processes, and technology that resource and deliver IT services and support Armywide.

Information exchange standards specification
A narrowly scoped data model that facilitates data exchange and interoperability between COIs.

Information management
Planning, budgeting, manipulating, and controlling information throughout its life cycle.

Information management office or officer
The office or individual responsible to the respective commander, director, or chief responsible for coordinating service definition, management oversight, advice, planning, and funding coordination of all IT and IM requirements (business and mission) for the organization. The IMO assists the commander, director, or chief in exercising responsibility to effectively manage the organization's IT and IM processes and resources that enable the organization's business and mission processes.

Information requirement
The expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or recordkeeping systems, whether manual or automated.

Information resources management
The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, maintenance, utilization, dissemination, and disposition of information, regardless of media. Includes the management of information and information-related resources and systems, whether manual or automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information; and the acquisition and use of automatic data processing, telecommunications, and other IT.

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, the terms "application" and "information system" are both IT investments describing a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see JP 1–02).The application of IT to solve a business or operational (tactical) problem creates an information system.

Information technology
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used 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).)

Information technology architecture
An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic and information resources management goals.

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

Infrastructure
The shared computers, ancillary equipment, software, firmware, and similar procedures; and services, people, business processes, facilities (such as 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 IT 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 that depend on the installation for support.

Integrated Information Technology
Modular IT that can operate independently or on multiple platforms.

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.

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

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

Internet Protocol version 4 interoperable
An IPv6-capable system, or product capable of receiving, transmitting, and processing IPv4 packets.

Internet Protocol version 6-capable
A system or product meeting the minimal set of DISR-mandated requirements (appropriate to the product class) necessary to be interoperable with other IPv6-capable products in DOD deployments.

Internet Protocol version 6-enabled
IPv6-capable systems or products with the IPv6 functionality turned on–implying that IPv6 packets can be properly processed by that system, product, or component.

Internet service provider
An organization that provides other organizations or individuals with access to, or presence on, the Internet. Most Internet service providers also provide extra services including help with the design, creation, and administration of Web sites; training; and the administration of Intranets.

Interoperability
The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.

Intranet
A computer network that functions like the Internet. Uses Web browser software to access and process the information that employees need, and is located on computers within the organization or enterprise. A firewall is usually used to block access from outside the Intranet. Intranets are private Web sites.

Land Warrior Network
The Army's portion of the DOD GIG. LandWarNet is a universally accessible, standardized, protected, and economical network enterprise. LandWarNet seamlessly delivers network capabilities and services supporting the Army's Joint, interagency, intergovernmental, multinational operations, and business missions.

Life cycle
The total phases that an item progresses through from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

Management decision evaluation package
A nine-year package of dollars and manpower to support a given program or function. The management decision evaluation package justifies the resource expenditure.

Measure
One of several measurable values that contribute to the understanding and quantification of a key performance indicator.

Message (telecommunications)
Recorded information expressed in plain or encrypted language, and prepared in a format specified for intended transmission by a telecommunications system.

Metadata
Information describing the characteristics of data; information about data; or descriptive information about an organization's data, data activities, systems, and holdings.

Metrics
The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.

Mission
A group of tasks and their respective purposes, which are assigned to military organizations, units, or individuals for execution.

Mission area
A defined area of responsibility with functions and processes that contribute to mission accomplishment.

Mission-related
Processes and functions that are closely related to the mission (for example, the mission of "Direct and Resource the Force" has the mission-related functions of planning, programming, policy development, and the allocation of resources).

Morale, welfare, and recreation programs
Military MWR programs (exclusive of private organizations as defined in DODI 1000.15) located on DOD installations or on property controlled (by lease or other means) by DOD or furnished by a DOD contractor, which provide for the mission sustainment and community support of authorized DOD personnel.

Multimedia
The synchronized use of two or more types of media, regardless of the delivery medium.

National security system
Any telecommunications or information system operated by the United States Government. The function, operation, or use of which involves: 1) intelligence activities; 2) cryptologic activities related to national security; 3) C2 of military forces; 4) equipment that is an integral part of a weapon or weapons system; or 5) matters critical to the direct fulfillment of military or intelligence missions (see the CCA).

Negotiation
The communication (by any means) of a position or an offer on behalf of the United States, DOD, or any office or organizational element thereof; to an agent or representative of a foreign Government (including an agency, instrumentality, or political subdivision thereof); or of an international organization in such detail that the acceptance in substance of such position or offer would result in an international agreement. The term also includes any communication conditional on subsequent approval by higher authority, but excludes mere preliminary, exploratory, or informal

discussions or routine meetings conducted with the understanding that the views communicated do not and will not bind any side. (Normally, the approval authority will authorize the requesting command to initiate and conduct the negotiation.)

Networthiness
Risk management accomplished through the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the Army enterprise.

Nonappropriated fund(s)
Cash and other assets received from sources other than monies appropriated by the U.S. Congress. (NAF must be resources of an approved NAFI.) NAF are U.S. Government funds, but they are separate and apart from funds that are recorded in the books of the U.S. Treasury. NAF are used for the collective benefit of the authorized patrons who generate them.

Nonappropriated fund instrumentalities
Every NAFI is legally constituted as an "instrumentality of the United States." Funds in NAFI accounts are Government funds, and NAF property, including buildings, is Government property. However, NAF are separate from APF of the U.S. Treasury. They are not commingled with APF and are managed separately, even when supporting a common program or activity.

Nonpublic data and information
Data and information that is personally identifiable, subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive.

Objectives
Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.

Operational architecture
Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.

Operational view (architecture)
A description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish or support a warfighting function. OV defines the type of information, frequency of exchange, and tasks supported by these information exchanges.

Operational requirement
A formally established, validated, and justified need for the allocation of resources to achieve a capability to accomplish approved military objectives, missions, or tasks.

Organizational messaging
Correspondence used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies official position, or issues official guidance is considered an organizational message.

Performance management
The use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet goals, and report on the success in meeting goals.

Performance measure
A quantitative or qualitative characterization of performance.

Performance measurement
The process of assessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of outputs (how well they are delivered to clients and the extent they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives.

Persistent cookies
Cookies that can be used to track users over time and across different Web sites to collect personal information.

Personally identifiable information
Information that can be used to distinguish or trace an individual's identity (for example, their name, social security number, and biometric records), or when combined with other personal or identifying information that is linked or linkable to a specific individual (for example, date and place of birth, mother's maiden name).

Planning, programming, budgeting, and execution process
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Platform
A weapon system, system of systems, or support system designated by a DOD component as the basis for analyzing core capability requirements.

Platform information technology
Refers to computer resources, both hardware and software, which are physically a 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.).

Portfolio management
The management of selected groupings of IT investments using integrated strategic planning, integrated architectures, performance measures, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with PfM are binning, criteria development, analysis, selection, control, and evaluation.

Printing
The processes of composition, platemaking, presswork, and binding (including micropublishing) for the production of publications.

Privacy impact assessment
An analysis of how personal information is handled to: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (b) determine the risks and effects of collecting, maintaining and disseminating personal information in an information system; and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a way to ensure compliance with applicable laws and regulations governing privacy.

Process
A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place, which also has a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process owners
HQDA functional proponents, ACOMs, and others who have responsibility for any mission-related or administrative work process.

Procurement and contracting
Purchasing, renting, leasing, or otherwise obtaining supplies or services from non-Federal sources. Includes description (but not determination) of supplies and services required, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration. Does not include making grants or cooperative agreements.

Proponent
An Army organization or staff that has been assigned primary responsibility for materiel or subject matter in its area of interest.

Public
The people or a citizen of the United States not affiliated with the Government.

Public key infrastructure
An enterprise-wide service (for example, data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption, and digital signature) that supports digital signatures and other public key-based

security mechanisms for DOD functional enterprise programs. Includes the generation, production, distribution, control, and accounting of public key certificates. PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key, and are issued by a reliable certification authority.

Public Web site on the Internet
Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet or anyone who can access a Web site through a browser.

Publications
Items of information printed or reproduced, whether mechanically or electronically, for distribution or dissemination to a predetermined audience. The items are generally directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by and for the Army.

Publishing
Actions involved in issuing publications. Involves creating, preparing, coordinating, approving, processing, printing, and distributing or disseminating publications.

Record
All books, papers, maps, photographs, machine readable items (such as, disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical-recording media, film slides, transparencies, or other documentary materials regardless of physical form or characteristics) made or received by any entity of the DA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data.

Records centers
Locations established in CONUS to receive and maintain records with long-term or permanent value, pending their ultimate destruction or accession into the National Archives.

Records management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with information creation, information maintenance and use, and information disposition in order to achieve adequate and proper documentation of the policies, transactions, and effective and economical management of DA operations.

Records management program
A program that includes elements concerned with the life-cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information Act and Privacy Act.

Satellite communications
DOD use of military-owned and military-operated SATCOM space systems that use Government frequency bands, and commercial SATCOM systems provided by commercial entities using commercial frequency bands. SATCOM is further defined to include DOD's use of other allied and civilian SATCOM resources as appropriate (See CJCSI 6250. 01).

Service level agreement
A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.

Sensitive compartmented information
Classified national intelligence concerned with or derived from intelligence sources, methods, or analytical processes, which are required to be protected within formal access-control systems established and overseen by the Director of National Intelligence.

Software
A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compiler, library routines, manuals, and circuit diagrams); usually contrasted with hardware.

Spam
Widely disseminated "junk" email.

Standard
Within the context of the AEA, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also establish requirements for the selection, application, and design criteria for materiel.

Standards view (architecture)
The standards view is the set of rules governing the arrangement, interaction, and interdependence of parts or elements of the architecture description.

Strategic planning
A continuous and systematic process whereby guiding members of an organization make decisions about the organization's future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured.

Subscriber
Any person, group, organization (including concessionaire), or appropriated or NAF activity that procures services made available pursuant to the terms of the franchise agreement.

Support agreement
An agreement to provide recurring common use IT services to another DOD or non-DOD Federal activity.

Synchronization
Coordinating and aligning the development of the AEA in both timing and direction for mutual reinforcement and support. See data synchronization.

System
An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JP 1–02). Within the context of the AEA, systems are people, machines, and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; or produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry, the terms "application" and "system" are used synonymously–a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (for example, the application of IT).

Systems architect
Responsible for the integration and oversight of architecture for IT and NSS from a systems perspective.

Systems architecture
Descriptions, including graphics, for systems and interconnections providing for or supporting functions.

System owner
The system proponent and the agency or organization that establishes the need for the IT system. Develops requirements, provides funding, designates who will manage data entry, and aligns requirements with APMS standards.

System view (architecture)
A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. The system view defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms, and specifies system and component-performance parameters. It shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems.

The Army Plan
This plan is a 16-year strategic planning horizon that includes the 6-year span of the program, plus an additional 10 years. The Army Plan presents comprehensive and cohesive strategic, midterm planning and programming guidance that addresses the Army's enduring core competencies over this time period.

Task
A discrete event or action that is unspecific to a single unit, weapon system, or individual; and that enables a mission or function to be accomplished by individuals or organizations.

Technical architecture
The technical architecture provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed.

Telecommunications
Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

Telework
Working at an alternative site via electronic means.

TEMPEST
An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment. These investigations are conducted in support of emanations and emissions security.

Thin client
The use of client-server architecture network that depend primarily upon the central server for processing activities that focus on conveying input and output between the user and the remote server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server. Many thin client devices run only Web browsers or remote desktop software, which means that all significant processing occurs on the server.

Third-party cookies
Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by various companies that oversee the banner ads that appear on many Web sites.

Uniform resource locator
A Web address that a person uses to direct a browser program to a particular Internet resource (for example, a file, a Web page, an application, and so on). All Web addresses have a URL.

Unique identification
A system of establishing globally unique identifiers within DOD, and serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships.

Unique identifier
A character string, number, or sequence of bits assigned to a discrete entity or its associated attribute, and serves to uniquely distinguish it from other like and unlike entities. Each unique identifier has only one occurrence within its defined scope of use.

User
Any person, organization, or unit that uses the services of an information processing system. Specifically, it is any table of organization and equipment (TOE) or table of distribution and allowances (TDA) command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, or otherwise applying DOTMLPF products for the accomplishment of a designated mission.

User fee
The periodic service charge paid by a subscriber to the franchisee for service.

Video
Pertaining to bandwidth and spectrum position of the signal that results from television scanning and is used to produce an electronic image.

Video teleconferencing
Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video. Includes full-motion video, compressed video, and sometimes freeze (still) frame video.

Vision
A description of the future; the most abstract description of the desired end-state of an organization or activity at an unspecified point in the future.

Visual information
Information in the form of visual or pictorial representations of person(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog, digital, and high definition video recordings; hand-generated or computer-generated art and animations that depict real or imaginary person(s) or thing(s); and related captions, overlays, and intellectual control data.

Visual information activity
An organizational element or a function within an organization in which one or more individuals are classified as VI specialists, or whose principal responsibility is to provide VI services. VI activities include those that expose and process original photography; record, distribute, and broadcast electronically (video and audio); reproduce or acquire VI products; provide VI services; distribute or preserve VI products; prepare graphic artwork; fabricate VI aids, models, and displays; and provide presentation services or manage any of these activities.

Visual information documentation
Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, and are usually not controlled by the recording crew.

Visual information equipment
Items capable of continuous or repetitive use by an individual or organization to record, produce, reproduce, process, broadcast, edit, distribute, exhibit, and store visual information. Items otherwise identified as VI equipment, which are an integral part of a non-VI system or device (existing or under development), will be managed as a part of that non-VI system or device.

Visual information functions
The individual VI processes, such as production, documentation, reproduction, distribution, records preservation, presentation services, VI aids, fabrication of model and displays, and related technical services.

Visual information library
A VI activity that loans, issues, and maintains an inventory of motion media, imagery, or equipment.

Visual information management office
Staff office at command, FOA, or other management level established to prescribe and require compliance with VI policies and procedures, and to review operations.

Visual information materials
A general term that refers collectively to all of the various VI still and motion films, tapes, discs, or graphic arts. Includes the original, intermediate, and master copies, and any other recorded imagery.

Visual information production
The combination of motion media with sound in a self-contained, complete presentation, developed according to a plan or script for purpose of conveying information to, or communicating with, an audience. A production is also the end item of the production process. Used collectively, VI production refers to the functions of procurement, production, or adoption from all sources, such as in-house or contract production, off-the-shelf purchase, or adoption from another Federal agency.

Visual information products
VI media elements such as motion picture and still photography (photographs, transparencies, slides, film strips); audio and video recordings (tape or disc); graphic arts (including computer-generated products); models; and exhibits.

Visual information records
VI materials, regardless of format, and related captions and intellectual control data.

Visual information resources
The personnel, facilities, equipment, products, budgets, and supplies that comprise DOD visual information support.

Visual information services
Those actions that 1) result in obtaining a visual information product; 2) support the preparation of a completed VI

production such as photographing, processing, duplicating, sound and video recording, instrumentation recording, and film-to-video transferring, editing, scripting, designing, and preparing graphic arts; 3) support existing VI products such as distribution and records center operations; and 4) use existing VI products, equipment, maintenance, and activities to support other functions such as projection services, operation of conference facilities, or other presentation systems.

Warfighter
A common Soldier, sailor, airman, or marine by trade, from all Services who joins in a coordinated operation to meet a common enemy, a common challenge, or a common goal.

Warfighting requirements
Requirements for ACAT I–IV systems or IT capabilities in direct use by or support of the Army Warfighter in training for and conducting operational missions (tactical or other), or for connecting the Warfighter to the sustaining base.

Weapon System
A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

Web portals
Web sites that serve as starting points to other destinations or activities on the Web. Initially thought of as "home base" Web pages, portals attempt to provide all of a user's Internet needs in one location. Portals commonly provide services such as email, collaboration centers, online chat forums, searching, content, newsfeeds, and other.

Web site
A location on the Internet; specifically it refers to the point of presence location in which it resides. All Web sites are referenced using a special addressing scheme called a URL. A Web site can mean a single HTML file or hundreds of files placed on the Internet by an enterprise.

World Wide Web
A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses; also referred to as the "Web."

Section III
Special Abbreviations and Terms

ADB
Army Data Board

ADCCP
Army Data Center Consolidation Plan

ADMP
Army Data Management Program

AE
Army enterprise

AMVID
Army Multimedia and Visual Information Directorate

AMVID/PAD
AMVID/Production Acquisition Division

APL
approved product list

BSIT–ESG
Business Systems Information Technologies - Executive Steering Group

CB
consolidated buy

CDAC
Content Discovery and Access Catalog

CDO
chief data officer

CLS
common levels of support

CMO
chief management officer

CND-SP
Computer Network Defense-Service Provider

CR
change request

CUI
common-user infrastructure

DARS
Department of Defense Architecture Registry System

DBS
Defense Business System

DBSMC
Defense Business System Management Committee

DIMOC
Defense Imagery Management Operations Center

DQMP
data quality management process

DQMS
data quality management system

DREN
Defense Research and Engineering Network

DSL–A
Data Services Layer-Army

DVIAN
Defense visual information activity number

EADS
enterprise authoritative data source

EIEMA
Enterprise Information Environment Mission Area

EMC
enterprise multimedia center

EOP
external official presence

EPEAT
Electronic Product Environmental Assessment Tool

ESG
executive steering group

ESI
enterprise software initiative

FaNS
Federated Net-Centric Sites

FDM
functional data manager

GFEA
generating force enterprise activity

IE
information enterprise

IEA
information enterprise architecture

IPv4
Internet protocol version 4

IPv6
Internet protocol version 6

ISA
interconnection security agreement

LandWarNet
Land Warrior Network

MA
mission area

MDR
DOD Metadata Registry

MH
medical holdover

M/VI
multimedia/visual information

NIE
Network Integration Evaluation

NIP
National Intelligence Program

NOSC
network operations and security center

OBT
Office of Business Transformation

OCL
object constraint language

PAD
Production Acquisition Division

PfM
portfolio management

RDF
resource description framework

SC
Signal Command

SFIS/FFMIA
Standard Financial Information Structure/Federal Financial Management Improvement Act

SIS
service interface specification

SISSU
security, interoperability, supportability, sustainability, usability

STIG
Security Technical Implementation Guide

UC
unified capabilities

UC APL
Unified Capabilities Approved Products List

UCore
Universal Core

VIOS
Visual Information Ordering Site

VoIP
voiceover Internet protocol

VoSIP
voiceover secure Internet protocol