Army Regulation 25–1

Information Management

Army Knowledge Management and Information Technology

Headquarters
Department of the Army
Washington, DC
4 December 2008

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–1
Army Knowledge Management and Information Technology

This major revision, dated 4 December 2008--

- Clarifies Army Knowledge Management goals and practices and states the Army goals for electronic government (paras 1-8 and 1-10).

- Updates the responsibilities pertaining to the management of information technology (chap 2).

- Adds policy on reporting of capital and other information technology expenditures in preparation of information technology budgets (para 3-3*c*).

- Updates policy on investment management, management of information technology through portfolios, and mission area and domain leads (para 3-4).

- Adds policy on Privacy Impact Assessments (para 3-8*f*).

- Adds policy on accelerating the use of commercial-off-the-shelf information technology software and services (para 3-9).

- Updates and adds policy on Army Interoperability Certification; Defense Business Systems Certification; Army Portfolio Management Solution/Army Information Technology Registry (para 3-11).

- Revises and updates policy regarding the Army Enterprise Architecture; requires waivers to Department of Defense Information Technology Standards Registry; provides policy on the implementation of Internet Protocol version 6 (chap 4).

- Updates information assurance policy including the transition from information assurance vulnerability alerts to information assurance vulnerability management and the Defense information technology security certification and accreditation process to the Defense information assurance certification and accreditation process (para 5-1*a*).

- Makes significant changes to chapter 6. Specifically, updates policy on information technology support principles; computing services; network operations; telecommunications systems and services; long-haul and deployable communications; satellite communications systems; Army Web sites services; and information technology support for military construction (chap 6).

- Updates/clarifies/revises policy on visual information combat camera; visual information responsibilities, activities, operations, equipment, and systems; multimedia products; visual information services, records management, and documentation program; and restrictions and controls for visual information production and distribution (chap 7).

- Revises the role of records administrators and managers (para 8-2).
- Replaces policy on statutory restrictions for publications with reference to AR 25-30 (para 9-3).
- Revises policy on requisitioning printing (para 9-5).
- Updates management control checklist (app C).
- Adds mission area and domain leads in support of portfolio management (fig D-1).
- Adds a sample Department of Defense Information Technology Standards Registry Waiver Request (fig E-1).
- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
4 December 2008

*Army Regulation 25–1

Effective 5 January 2009

Information Management

Army Knowledge Management and Information Technology

By Order of the Secretary of the Army:

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

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is 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, the resources supporting information technology, and Army Knowledge Management as a means to achieve a knowledge-based force. This regulation implements 40 USC, Subtitle III; 44 USC, Chapters 35 and 36; 10 USC, Sections 2223 and 3014; and DODD 8000.01. It establishes the Army's Chief Information Officer. The full scope of Chief Information Officer 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, which prescribe specific prohibitions, are punitive, and violations of these provisions may subject offenders to nonjudicial 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 the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

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

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

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 15 July 2005; AR 25-10, dated 1 May 1989; and AR 25-11, dated 4 September 1990.

UNCLASSIFIED

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Chapter 1
Introduction

1–1. Purpose

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

1–2. References

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

1–3. Explanation of abbreviations and terms

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

1–4. Responsibilities

See chapter 2 for responsibilities.

1–5. Recordkeeping requirements

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

1–6. Managing information resources and information technology

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

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

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

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

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

1–7. Information as a resource

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

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

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

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

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

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

1–8. Army Knowledge Management

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

a. The goals of AKM are—

(1) Adopt governance and cultural changes to become a knowledge-based organization.

(2) Integrate KM and best business practices into Army processes to promote the knowledge-based force.

(3) Manage the infrastructure as an enterprise to enhance efficiencies and capabilities such as collaborative work, decision-making, and innovation.

(4) Institutionalize AKO/DKO as the enterprise portal to provide universal and secure access for the entire Army.

(5) Harness human capital for the knowledge-based organization.

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

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

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

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

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

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

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

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

f. Active Army, Army Reserve, National Guard, civilian, and appropriate contractor personnel will make full use of AKO/DKO resources and capabilities.

g. All personnel must become familiar with the AKM strategy and goals. Commanders and activity heads must develop organizational initiatives to support the strategy and goals. The ability to store and find the right information, at the right time, and to deliver it to the right customer must be a major focus at all levels of command and especially with the information management (IM)/IT community of service providers.

1–9. Information transmission economy

Originators of record communications will use the most operationally and cost-effective means of transmission. The choice will be made from an analysis of the perishability, classification, and urgency of the content and the availability of transmission means. See also DA Pam 25–1–1, paragraph 7–1.

1–10. Use of information technology to improve mission efficiency and effectiveness

a. The use of IT facilitates the streamlining of business operations. The Army achieves improvements in customer support, internal processes, and supplier relationships by applying IT to specific business practices.

b. Information in an electronically readable format is easily stored, replicated, distributed, shared, and presented in a manner useful to support Army processes and decision-making. Whenever possible, information will be stored in an electronically readable format and shared horizontally and vertically with those requiring the information. Retention of information stored in electronically readable format for the prescribed period ensures its availability for use in Army decision-making and business processes.

c. The improvement of processes and integration of ISs throughout the organization increases efficiency and results in improved coordination among functional areas and the availability of consistent information. Army functional proponents will work toward total process transformation by implementing integrated, interoperable, enterprisewide, multifunctional, net-centric, and end-to-end services that provide reliable information throughout the enterprise.

d. Title 44, United States Code, Chapter 36, Electronic–Government (E–Gov) Act of 2002, requires Federal agencies to use IT to transform relations with citizens, businesses, and other sectors of government. IT can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient management. E–Gov aims to make the interaction between government and citizens, government and business enterprises, and inter-agency relationships more responsive, convenient, transparent, and inexpensive. The Army has adopted a number of commercial best practices in support of E–Gov principles. The approach emphasizes IT-enabled end-to-end process transformation and the creation of Armywide enterprise processes in support of the Future Force and the American public. The process transformation is based on a "one network, one portal, one database" enterprise philosophy. Army goals for implementing E–Gov include—

(1) Contributing to and participating in Federal E–Gov initiatives rather than creating redundant or agency-unique IT projects;

(2) Posting Army's discretionary grant application packages on Grants.gov (http://www.grants.gov);

(3) Optimizing IT investments to better achieve mission outcomes;

(4) Establishing a direct relationship between IT and mission/program performance to support citizen-centered and customer-focused government;

(5) Providing leadership and support for interoperability, with the adoption of data standards and modernization efforts in lieu of legacy systems incapable of providing upgrades or cross agency support;

(6) Adopting best practices; and

(7) Eliminating unnecessarily redundant or stove-piped investments across the Army.

1–11. User/customer focus and the relationship between the customer and the information technology community

a. The Army IT community provides information capabilities and services for the benefit of Army, Defense, and non-Defense Federal agencies, coalition partners, and the general public. 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 role of IT in support of the Army's missions, the IT community must maintain focus on the needs of its customers.

b. This customer focus should include awareness of the current user requirements, the quantity and quality of the support provided, future customer requirements, and emerging IT capabilities. The Army's employment of IT dictates a robust relationship between the IT community and its customer in which both the customer and the service provider take responsibility for communicating with each other. Each organization's IT management (ITM) process must foster a similar dialogue. Although primary responsibility must be assigned for the various aspects of that process, both IT providers and their customers must remain actively engaged for the process to succeed.

c. Army customers must be sensitive to the IT community's need to be involved in seemingly unrelated management issues because of potential IT impacts to Army organizations. Customers must also be willing to participate

actively in the support process, especially in the definition of their requirements. The IT community must embrace accountability to the customer as an essential element 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 human 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.

1–12. Ensuring quality of information disseminated to the public

a. Section 3506, Title 44, United States Code, requires Federal agencies 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.

b. 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 those situations involving influential scientific, financial, or statistical information, which must be capable of being substantially reproduced. (See detailed Army guidance on implementing information quality requirements at DA Pam 25–1–1, paragraph 7–7, and DOD guidance at http://www.army.mil/CIOG6/references/policy/docs/U0167803.pdf.)

c. Specific types of information that are not subject to this standard are—

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

(2) Intra- or inter-Army or other department or agency sharing of government information, including responses to requests under FOIA, the Privacy Act, the Federal Advisory Committee Act, or other similar laws.

Chapter 2
Responsibilities

2–1. The Army Chief Information Officer/G–6

The Army Chief Information Officer/G–6 (CIO/G–6) will—

a. Serve as principal focal point in Headquarters, DA (HQDA) for IM matters with Congress, General Accounting Office, Office of Management and Budget (OMB), other Federal agencies, DOD, Joint Staff (JS), Army organizations and commands, and other military departments, academia, and industry.

b. Provide functional policy and guidance on IT systems and networks.

c. Serve as CIO for the Army. The responsibilities are to—

(1) Serve as principal advisor to the Secretary of the Army (SECARMY) and other Army leadership on matters related to IT.

(2) Provide oversight of the Army's collection of information and control of paperwork, information dissemination, statistical data, policies and coordination, records management, and FOIA and Privacy Act programs.

(3) Integrate the budget, program management, and acquisition decisions affecting IT to promote Army efficiency and productivity in all of its activities.

(4) Develop IT critical tasks and supporting skills and knowledge for Army personnel to facilitate achievement of the Army mission and goals.

(5) Provide the IT strategic planning perspective to Army's strategic planning process, to include alignment of the IT investment strategy with Army strategic vision, goals, and objectives.

(6) Develop and implement IT performance measurements.

(7) Establish and implement Armywide enterprise architecture (EA).

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

(9) Chair the Army CIO EB.

(10) Provide oversight of the Army Information Assurance (IA) Program.

(11) Provide CIO assessment of IT and National Security Systems (NSS) and CIO certification of major automated ISS.

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

(13) Represent the Army on the Committee on National Security Systems (CNSS).

d. Serve as the Army G–6 for information and signal operations, network and communications security, force structure, equipping, and employing signal forces.

e. Implement the policy and procedures mandated by—

(1) 10 USC 3014 and 2223(b).

(2) 40 USC Subtitle III (Clinger-Cohen Act).

(3) 44 USC Chapter 35, Coordination of Federal Information Policy (includes portions of the E-Gov Act).

(4) 44 USC Chapter 36, Management and Promotion of E-Gov Services (E-Gov Act).

(5) DODD 8000.01.

f. Serve as functional proponent for the AKM transformation, Army Enterprise Portals (that is, AKO/DKO and AKO-S), Army Enterprise Architecture (AEA), and the Army Enterprise Infrastructure (AEI).

g. Provide oversight and coordination for implementation of the policies in—

(1) 44 USC Chapters 29, 31, and 33 (P.L. 94575, Federal Records Management).

(2) 5 USC 552 (FOIA).

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

h. Provide policy oversight and program direction to the U.S. Army Network Enterprise Technology Command (NETCOM)/9th Signal Command (Army) (9th SC (A)) as a direct reporting unit (DRU) of the CIO/G–6.

i. Support the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT)) as the Army Acquisition Executive (AAE) in the acquisition of IT/NSSs, to include these functions:

(1) Serve as member of the Army Systems Acquisition Review Council or similar committee, as required.

(2) Serve as member of the Office of the Secretary Defense (OSD) IT Overarching Integrated Process Team or similar committee.

(3) Serve, as required, as a member of the OSD IT Acquisition Board.

(4) Serve as member of the Test Schedule and Review Committee.

(5) Serve as member of the Defense Acquisition Board (DAB) or similar committee.

(6) Interface, as needed, with program executive officers (PEOs) and program managers (PMs) for those systems that pertain to IT.

(7) Develop and recommend IT acquisition policy to the ASA (ALT).

(8) Serve on the Army Test and Evaluation Managers Advisory Council.

(9) Coordinate Army Acquisition Corps IT issues through the Acquisition Support Center.

j. Lead and manage the AEA.

k. Lead and manage the Army Net-Centric Data Management Program (ANCDMP) and serve as the Army Component Data Administrator (CDAd) under the DOD Data Administration Program. (See also paras 4–9 through 4–14 of this publication.)

l. Lead and manage Army's compliance with E-Gov initiatives and provide general oversight and consolidated reporting of E-Gov activities as part of the Presidents Management Agenda.

m. Provide oversight and direction for the network-centric concepts and management, to include the Army Networthiness Program.

n. Serve as senior authority for telecommunications programs and committees, to include the following:

(1) JS-controlled mobile/transportable telecommunications assets.

(2) The Spectrum Certification Program.

(3) Voting member of the Military Communications-Electronics Board (MCEB) and participant in MCEB activities.

(4) Army "lead" for Joint Transformation Communications Program.

o. Serve as senior authority for Army visual information (VI) and multimedia products as defined in chapter 7 of this regulation.

p. Monitor the operations and structure of the military and civilian personnel management systems to ensure that the Army's requirements for qualified IT personnel are addressed and that IT career development plans, programs, and objectives are established. Duties include—

(1) Serve as the functional chief for the IT Management Career Program-34 (CP34).

(2) Serve as the principal coordination point for designated military specialties.

q. As the HQDA proponent responsible for the information systems supporting command, control, communications, and computers (C4)/IT programs

(1) Serve as the Army focal point for IT system (to include NSS) issues; receive, coordinate, and integrate these issues; and ensure the integration of systems development efforts that cross functional and/or technical lines.

(2) Participate in and provide representation for Planning, Programming, Budgeting, and Execution (PPBE) process decision groups and exercise centralized oversight of IT expenditures for all appropriations.

(3) Develop, coordinate, and implement an IT capital planning and investment management program.

(4) 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.

(5) Promote the application of proven advanced technology techniques, procedures, and methodologies across the Army's management processes and their associated ISs.

(6) Provide CIO validation of requirements for warfighting, administrative processes, and other mission-related processes associated with an IT impact.

(7) Coordinate resource requirements for IT support activities.

(8) Coordinate IT requirements relevant to Army continuity of operations plans (COOPs) 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, and installations.

(9) In conjunction with the Office of the Administrative Assistant to the Secretary of the Army (OAASA), ensure that records management requirements are included in the life cycle of ISs beginning at the initial milestone.

r. Manage, plan, and program for the Army Spectrum Management Program.

s. 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.

t. Provide IT Portfolio Management (PfM) policy and oversee implementation of Mission Area (MA) IT portfolios to ensure they are aligned with Army enterprise solutions.

u. Serve as the Army's MA lead for the Enterprise Information Environment (EIE) MA (EIEMA) to support the DOD EIEMA lead and ensure EIE efforts are traceable to, and fully enable, the required capabilities for the Warfighting and Business MAs.

v. Ensure compatibility and interoperability of IT/NSS with joint, unified, combined, Federal Government, and other Army systems, as required.

2–2. The U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)

The NETCOM/9th SC (A), as a DRU to the CIO/G–6, will—

a. Serve as the single authority assigned to operate, manage, and defend the Army's infrastructure at the enterprise level. See also AR 10–87, chapter 14, and DA Pam 25–1–1, paragraph 6–1.

(1) Manage the "army.mil" and "army.smil.mil" Internet domains and the assignment of subdomains requested by other Army organizations.

(2) Ensure Army IT systems are designed for survival, recovery, and support reconstitution for COOP support requirements.

(3) Organize and chair the AEI technical configuration control board.

(4) Support server and application consolidation, collaboration tools, best business practices, and Web services at the enterprise level.

(5) Provide technical support and evaluation to CIO/G–6 during requirements processing.

(6) Provide for the protection of assigned fixed-station communications facilities and the security of Army contractor telecommunications.

(7) Exercise operational review and coordination of information infrastructure or architectures.

(8) Operate, certify, accredit, and maintain common-user IT services and capabilities.

(9) Exercise technical authority over all organizations that operate and maintain portions of the AEI (that is, the systems and networks) that constitute the LandWarNet (LWN), which is the Army's portion of the GIG.

b. Provide a communications service in support of the news media during field exercises, contingencies, and combat operations when commercial capabilities are not available.

c. Submit validated or approved telecommunications requirements to Defense Information Systems Agency (DISA) for coordination and implementation.

d. Operate, manage, and defend the LandWarNet.

e. Exercise technical authority and configuration management authority for the Army's networks, systems, and functional processing centers; provide guidelines and direction for Army enterprise IT configuration management.

(1) Exercise operational review/coordination authority for any standard system architecture design or device that impacts the AEI.

(2) Provide centralized management and technical authority of IT belonging to or under the purview of regional CIOs (RCIOs), installation Directors of IM (DOIMs), Army Commands (ACOMs), functional activities, and IT CoPs.

f. Manage the Army IA Program.

g. Serve as the responsible Army official for management of the LWN.

h. Exercise network operations (NetOps) over the LWN and all Army Theater Signal Forces.

i. Provide operational management of the Army's Networthiness Program.

j. Manage and provide personnel resources for the NETCOM/9th SC (A) liaison staff for the Installation Management Command (IMCOM) headquarters and the RCIO staff for IMCOM regional directors.

k. Serve as the IT Service Management Program operational authority for the Army in support of the CIO/G–6.

l. Provide combat camera (COMCAM) documentation support for theater Army, joint military operations, and operations other than war, to include developing and maintaining appropriate plans.

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

(1) Exercising Army review, approval, and/or validation authority over telecommunication requests (TRs) for service.

(2) Validating requests for special access requirements to increase survivability and reliability.

(3) Operating and maintaining designated Defense Red Switch Network (DRSN), Army's portion of Military Satellite Communications (MILSATCOM) for Defense Satellite Communications Systems, Defense Information Infrastructure (Microwave and Fiber Optic Cable Systems), Non-Secure Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) routers, Defense Messaging System (DMS) operational requirements, and Defense Switched Network (DSN).

(4) Determining operational requirements for combatant command communications teams in support of the Army.

n. Formulate Army military telecommunications exchange agreements between the United States and regional defense organizations or friendly foreign nations and coordinate the agreements procedural details with the commander of the theater of operations concerned.

o. 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.

p. In support of the information requirements of the JS—

(1) Develop and maintain plans.

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

(3) Determine requirements for mobile/transportable communications assets to support assigned missions and functions.

q. In support of North Atlantic Treaty Organization (NATO) communication requirements for projects involving interfaces between non-DISN NATO and NATO member telecommunications systems—

(1) Participate in negotiations concerning recognized requirements.

(2) Provide overall U.S. management of system-to-system interfaces, unless otherwise directed by the JS.

(3) To the extent that such projects are consistent with budget appropriations and the Secretary of Defense's consolidated guidance, fund validated projects that support U.S., NATO, and NATO-member telecommunications objectives and approved planned interfaces between non-DISN, NATO, and NATO-member systems.

(4) Operate equipment, facilities, and systems (or services) required supporting U.S., NATO, and NATO-member communications objectives as assigned.

(5) As appropriate, assist DISA in representing U.S. interests within NATO communications forums.

r. Execute Army leases of telecommunications services and ensure that such services conform to DOD and National Communications Systems guidance.

s. Manage the administration of amateur radio operations and the Army Military Affiliate Radio System (MARS) program per AR 25–6.

t. Identify and validate unique critical communications circuit requirements considered vital to the Army and submit them to the JS.

u. Serve as the focal point for identifying and analyzing threats to the AEI and its enabling technologies.

2–3. Principal Headquarters, Department of the Army officials

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

a. Serve as 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. Provide information regarding ongoing investment capabilities studies and their results, invitation, and participation in key investment forums to include studies to acquire knowledge needed to execute IT PfM and associated working groups and committees.

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

e. Participate collectively with other Army stakeholders in the IT capital planning and investment strategy process. (Refer to para 3–3 of this publication.)

f. 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.

g. Develop AEA information sets for their respective functional domain areas; act as the integrator for "system of systems" under their purview; and coordinate with CIO/G–6, as needed, on AEA documentation.

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

i. Manage and oversee the records of respective functional areas to appropriately secure, maintain, and preserve them throughout their life cycle. See also the specific requirements prescribed in paragraph 8–2*e* of this publication.

j. Identify functional requirements for the Army Enterprise portals (AKO/DKO and AKO-S) and participate, as required, in AKO/DKO Advisory Board activities.

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

2–4. Under Secretary of the Army

The Under Secretary of the Army (USA), or designated representative, will—

a. Serve as the Army's MA lead for the Business MA (BMA) to ensure that generating future force efforts are traceable to, and fully support, the required capabilities for DOD Warfighting and EIE MAs.

b. Ensure that a single, integrated architecture for the BMA efforts exists to support the Business Enterprise Architecture (BEA).

2–5. Assistant Secretary of the Army (Financial Management & Comptroller)

In addition to duties listed in paragraph 2–3, the ASA(FM&C) is responsible for the review and co-certification of the CIO/G–6 prepared IT budget, to include Exhibit 300s, IT1 spreadsheets (IT budget summary), and Exhibit 53. The ASA(FM&C), in concert with the CIO/G–6, will jointly co-certify the Army IT budget submission.

2–6. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

Responsibilities for the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) are defined in AR 70–1 and in paragraph 2–3 of this publication. Those ASA(ALT) responsibilities unique to IT are listed below:

a. Serve as the source selection authority or delegate source selection authority responsible for acquisition of IT systems.

b. Direct and review Command, Control, Communications, and Intelligence (C3I) systems; target acquisition systems; and 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 tactical ISs required for strategic and tactical programs.

d. Execute the RDT&E and procurement portions of IT programs and budgets.

e. Oversee the IT base relative to its impacts on the Army Industrial Base.

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

g. Ensure that PMs and PEOs successfully complete developmental interoperability assessments prior to Army Interoperability Certification (AIC).

h. Review and approve the Army position for acquisition category (ACAT) ID and ACAT IAM programs at each decision milestone before the DAB 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.)

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

j. As Executive Architect for System Architectures (SAs), validate Army system views and ensure managed programs develop system views that are integrated with approved operational and technical views.

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

l. Assign to the PEO Enterprise Information Systems the mission to operate and manage AKO/DKO.

2–7. The Office of General Counsel

The Office of General Counsel will, in addition to duties listed in paragraph 2–3—

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.

2–8. The Administrative Assistant to the Secretary of the Army

The Administrative Assistant to the Secretary of the Army (AASA) will, in addition to duties listed in para 2–3—

a. Serve as Archivist of the Army.

b. Serve as the senior Army official for records management and its associated programs as specified in paragraph 8–5 of this publication.

c. Develop and maintain the Army Information Collection Budget required by 44 USC Chapter 35 and chapter 8 of this regulation.

d. Implement records declassification requirements in accordance with Executive Order (EO) 12958.

e. Advise the 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.

f. Implement the Army Privacy Program.

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

h. 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 para 1–12 of this publication.)

i. Implement the Army Publishing Program (APP), to include—

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

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

(3) Serve as 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 (GPO), the Director of Bureau of Engraving and Printing, and the Administrator of the General Services Administration (GSA).

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

j. Operate and maintain the U.S. Army Visual Information Directorate (AVID) in support of OSD, JS, Army activities, other Defense components, and Federal agencies, as required, with AVID managing VI for the internal use of the HQDA as an ACOM.

k. Provide a centralized ready-access online library for customers requiring Army imagery from current operations and other significant events and stock images to support official missions.

l. Serve as the authenticating official for all Departmental publications except Army General Orders, which 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 other components and Federal agencies, as required.

n. Manage IT for HQDA internal use. The AASA is assisted in the execution of the IM function by the HQDA Information Manager (HQIM). The HQIM performs the role of DOIM for HQDA. The AASA will—

(1) Ensure that HQDA staff elements accomplish their assigned internal IM/IT responsibilities.

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

(3) Accomplish all the IM/IT responsibilities for HQDA as those assigned to ACOM commanders (see para 2–15 of this publication).

(4) Provide IM common services to HQDA elements.

(5) Ensure operational information support to HQDA.

(6) Provide an HQDA perspective to the Army IM/IT strategic planning.

(7) Provide IM officer (IMO) support for the Office of the Secretary of the Army; Office of the Chief of Staff, Army (OCSA); and supported activities.

o. Supervise and operate the Defense Telecommunication Service-Washington per DODD 4640.7 and DODI 5335.1.

2–9. The Chief of Public Affairs

The Chief of Public Affairs will, in addition to duties listed in paragraph 2–3—

a. Provide general staff supervision and approval for the release of Army VI products to the public.

b. In concert with the CIO/G–6, provide oversight and control of the content on Army public Web sites.

2–10. The Director of the Army Staff

The Director of the Army Staff (ARSTAF) will accomplish all the IT responsibilities assigned to the principal HQDA officials for the OCSA (see para 2–3 of this publication).

2–11. The Deputy Chief of Staff, G–2

The Deputy Chief of Staff, G–2 (DCS, G–2) will, in addition to duties listed in paragraph 2–3—

a. Provide recommendations to the CIO/G–6 concerning IT investments in the intelligence community.

b. Represent the CIO on the NIP and MIP funded efforts and other intelligence programs.

c. Provide staff supervision for counter-intelligence, 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 sensitive compartmented information (SCI) IA program and procedures pertaining to ISs processing intelligence information.

f. Provide coordination for security certification and accreditation of ISs processing intelligence data.

g. Serve as the Army's representative to the Defense Intelligence Mission Area led by USD (I) for National Intelligence and National Intelligence Technology Infrastructure; coordinate with Army Mission Area and Domain Leads as appropriate to ensure alignment with the Army's IT PfM efforts.

h. Oversee CG, U.S. Army Intelligence and Security Command (INSCOM), as a DRU to DCS, G–2, in his/her responsibilities, in addition to paragraph 2–15, to—

(1) Provide C4/IT-related combat and materiel development requirements and update data input for supporting intelligence, electronic warfare, and security operations to TRADOC, AMC, and FORSCOM.

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

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

(4) Manage and execute NIP and MIP systems maintained by the command.

(5) Provide functional support to the C4/IT PEOs and PMs as designated by the AAE.

(6) Coordinate C4/IT system design of proponent systems with TRADOC.

(7) Serve as the Army's primary interface to the national intelligence community for intelligence related to computer network operations.

(8) Provide relevant information and intelligence to the CG, NETCOM/9th SC (A) (in the CGs capacity as the Deputy for NetOps) to defend the LWN.

2–12. The Deputy Chief of Staff, G–3/5/7

The Deputy Chief of Staff, G–3/5/7 (DCS, G–3/5/7) will, in addition to duties listed in paragraph 2–3—

a. Exercise proponency for C2.

b. Determine requirements for operational information at HQDA.

c. Establish priorities for developing and acquiring materiel and force structure in support of IT programs.

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

e. Develop and approve the strategic and theater/tactical information requirements for strategic C2 programs.

f. Ensure that tactical VI COMCAM documentation support is included in Army operational planning documents for contingencies, emergencies, training exercises, and other peacetime engagements.

g. Ensure that support is included in Army operational planning documents for the collection and transfer of records created by deployed units in contingency operations per AR 25–400–2.

h. Serve as the Army's MA Lead for the Warfighting MA (WMA) and approve, prioritize, and synchronize all LWN capabilities, experimentation, concepts, and operational architecture development efforts for the WMA.

i. Serve as the approval authority for changes to the certified and approved software baselines in the AIC process.

2–13. Assistant Chief of Staff for Installation Management

The Assistant Chief of Staff for Installation Management (ACSIM) will, in addition to duties listed in paragraph 2–3—

a. Provide common-user IT services, including daily IT support requirements, to installation tenants through IMCOM.

b. Integrate the 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 common use IT requirements.

d. Provide HQDA oversight of the Army Family and Morale, Welfare, and Recreation Command (FMWRC), which serves as the proponent and focal point for matters concerning Army morale, welfare, and recreation (MWR) ISs.

2–14. The Judge Advocate General

The Judge Advocate General (TJAG) will, in addition to duties listed in paragraph 2–3—

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

b. Provide legal technology support 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.

2–15. Army Command, Army Service Component Command, and Direct Reporting Unit (as authorized by their respective Headquarters, Department of the Army elements) commanders

For the internal IM/IT responsibilities of their commands, commanders will—

a. Establish a senior IM official (for example, CIO, DCS for Information Management, or equivalent) responsible for implementing the command's IM/IT program. Command senior IM officials will directly supervise the IM staff, related programs, and activities.

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

c. Identify the commands IT requirements and ensure that mission requirements are validated, coordinated, and integrated per AR 71–9. Coordinate with the supporting DOIM to obtain command-unique IT requirements beyond common–use services.

d. Manage 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.

e. Obtain resources to support information requirements through the PPBE process.

f. 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.

g. Coordinate IT plans, programs, and requirements with appropriate IA managers (IAMs) per AR 25–2.

h. Create and maintain IT contingency plans to ensure the uninterrupted execution of essential missions and functions under all conditions. See also para 6–1b of this publication and DA Pam 25–1–2 for more information.

i. Obtain certificates of networthiness, certificates to operate, and AIC for command-unique IT systems.

j. Develop AEA architecture for respective command-unique functions and act as the integrator for "system of systems" under their purview. Coordinate with CIO/G–6 as required.

k. Ensure DISR compliance for designated systems.

l. Implement the ANCDMP as guided by the Army CDAd. (See chapter 4 of this publication for policy on data administration.)

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

n. Manage and oversee command records, in order to appropriately secure, maintain, and preserve such records throughout their life cycle. (See also the specific requirements prescribed in para 8–2*e* of this publication.) Appoint a command records administrator (RA) to oversee the Records Management Program.

o. Ensure that written contingency plans providing for effective withdrawal or destruction of records 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.

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

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

r. Promote a paper-free business environment in the Army through optimum use of electronic business/electronic government technologies.

s. Administer command-level IT performance measurements.

2–16. Army Service Component commanders

ASCC commanders, in addition to those responsibilities listed in paragraph 2–15, will—

a. Develop combat and materiel development plans for IT elements within their command and provide the plans to CIO/G–6, TRADOC, AMC, and FORSCOM as required.

b. Provide data pertaining to all IT functional specifications and relevant materiel development systems and programs to TRADOC as required.

c. Coordinate with TRADOC, AMC, and FORSCOM on matters pertaining to IT combat and materiel development.

d. Maintain POCs with staff elements that recommend new or improved IT-related doctrine, force structure, training, and materiel to TRADOC, AMC, FORSCOM, INSCOM, or MEDCOM.

e. Develop requirement documents and Operational View (OV) input, as needed, to support the respective organization's C2 plans and forward them to TRADOC.

f. Manage satellite communications (SATCOM) assets assigned in support of ground mobile forces.

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

2–17. Commanding General, U.S. Army Training and Doctrine Command

The Commanding General (CG), U.S. Army Training and Doctrine Command (TRADOC) will, in addition to the duties listed in paragraph 2–15—

a. Formulate IM/IT doctrine for the Army.

b. Serve as the Army Operational Executive Architect. (See also chapter 4 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. Incorporate records management training in functional and MOS-producing courses.

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

2–18. Commanding General, U.S. Army Materiel Command

The CG, U.S. Army Materiel Command (AMC) will, in addition to the duties listed in paragraph 2–15—

a. Provide functional support to the PEOs and PMs as designated by the AAE.

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

c. Support the CIO/G–6 in the execution of 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 Forces Command (FORSCOM)

e. Perform system engineering for the combat service support 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 HQDA CIO/G–6.

g. Resource and execute Configuration Management processes, as directed and deemed necessary by the HQDA 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.

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

The CG, U.S. Army Forces Command (FORSCOM) will, in addition to the duties listed in paragraph 2–15—

a. Exercise operational control over NETCOM/9th SC (A) Theater Tactical Signal Brigades for global commitments.

b. Coordinate with COMCAM for current operations and training exercises.

2–20. Commanding General, United States Army Special Operations Command

The CG, U.S. Army Special Operations Command (USASOC) will, in addition to the duties listed in paragraph 2–16—

a. Comply with United States Special Operations Command (USSOCOM) direction for management of information resources within the Special Operations Forces (SOF) Information Enterprise (SIE), as an Army Component Command under the operational control (OPCON) of USSOCOM.

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

2–21. The Army Surgeon General/Commanding General, U.S. Army Medical Command

The Army Surgeon General/CG, U.S. Army Medical Command (MEDCOM) will, in addition to the duties listed in paragraph 2–15—

a. Provide IT-related combat and materiel development plans and data supporting military medical operations to TRADOC, AMC, and FORSCOM as required.

b. Provide medical COMCAM documentation support by ensuring applicability to internal command operational plans and rapid response to wartime, contingencies, joint exercises, and natural disasters.

c. Ensure compliance with 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.

2–22. Commanding General, U.S. Army Corps of Engineers

The CG, U.S. Army Corps of Engineers (USACE) will, in addition to the duties listed in paragraph 2–15—

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

b. Coordinate the documentation of data standards for MILCON and Civil Works data elements.

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

2–23. Chief, Army Reserve, and the Chief, National Guard Bureau

The Chief, Army Reserve (CAR), and the Chief, National Guard Bureau have the same responsibilities as specified in paragraphs 2–13*a*, 2–13*c*, and 2–15.

2–24. Commanders or directors of major subordinate commands, field-operating agencies, separately authorized activities, tenant, and satellite organizations

Commanders or directors of major subordinate commands (MSCs), field-operating agencies (FOAs), separately authorized activities, tenant, and satellite organizations will, based on guidance of their parent organization, accomplish the same IM responsibilities as their parent organization commensurate with their respective mission, size, responsibility, and location.

a. Commanders of subordinate organizations will designate a senior IM official who will have staff responsibility for the supported organization equivalent to the senior IM official at the ACOM or ASCC levels.

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

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

(2) Coordinate with the installation DOIM for common use IT common services.

(3) Designate in writing a subordinate organization RA who will perform duties as described in paragraph 8–2*e* of this publication.

2–25. State Area Command, U.S. Army Reserve Command, or comparable-level community commanders

State Area Command (STARC), U.S. Army Reserve Command (USARC), or comparable-level community commanders will—

a. Establish and maintain a DOIM who has the responsibility to implement the organizational IM program. The DOIM 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 Technical View (TV) 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 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 per AR 25–2.

(7) Perform functions as the single authority to validate the purchase of IT items on the installation.

b. Appoint a records manager responsible for the records management program.

c. Appoint a single installation VI manager.

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

e. Coordinate with the installation DOIM when moving to an Active Army installation.

f. Ensure that fielded systems are networthy and AENIA-compliant.

2–26. Program, project, and product managers and information technology materiel developers

Program, project, and product managers (PMs) and IT materiel developers (IT 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 (TV, OV, and System View (SV)) for their systems with the PEO and management official of gaining commands and installations.

(4) Use the DOD IT Standards Registry (DISR) online tool to build TVs (https://disronline.disa.mil/VJTA/index.jsp).

(5) Coordinate their systems architectures with commands, DRUs, RCIOs, and DOIMs prior to fielding systems.

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

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

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

c. Ensure that all fielded systems are logistically supportable during the life cycle of the system and follow Integrated Logistics Support (ILS) responsibilities per AR 700–127.

d. Ensure that records management requirements are included in systems throughout their life cycle.

e. Develop and prepare Exhibit 300 Business Case(s) for systems as applicable for submission with the IT budget.

f. Submit any new development or modernization intended initiatives or expenditures over 1 million (before obligation) for review by the appropriate OSD Investment Review Board (IRB), certification by the designated accrediting authority (DAA), and certification approval by the Defense Business System Management Committee (DBSMC).

g. Ensure compliance with IA certification and accreditation requirements, the Army's Networthiness Program, and AENIA for all PM-developed IT systems.

h. Ensure that all systems with interoperability requirements achieve AIC by the CIO/G–6 (SAIS–AOJ).

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

j. Ensure that IT materiel testing, acquisition, and support comply with joint, NATO, and American, British, Canadian, Australian (ABCA) (Quadripartite) armies rationalization, standardization, and interoperability agreements and Federal and international standards.

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

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

2–27. Program executive officers and direct-reporting product managers

Program Executive Officers (PEOs) and direct-reporting product managers (PMs) will—

a. Develop AEA architectures (OV, TV, and SV) for assigned systems in coordination with CIO/G–6, consistent with DOD guidance.

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

c. Ensure that all fielded systems are logistically supportable during the life cycle of the system and follow ILS responsibilities per AR 700–127.

d. Develop and prepare Exhibit 300 Business Case(s) for systems as applicable for submission with the IT budget.

e. Submit any new development or modernization intended initiatives or expenditures over $1 million (before obligation) for review by the appropriate OSD IRB, certification by the DAA, and certification approval by the DBSMC.

f. Ensure records management requirements are included in systems throughout their life cycle.

g. Ensure compliance with IA certification and accreditation requirements, Networthiness Program, and AENIA for all PM-developed IT systems.

h. Ensure that compliance with DOD policy regarding accelerated use of Commercial Off-the-Shelf (COTS) IT/NSS by establishing a baseline and documenting progress in this effort.

i. Ensure that all PM-developed systems with interoperability requirements achieve AIC by the CIO/G–6 (SAIS–AOJ).

Chapter 3
Chief Information Officer Management

3–1. Governance

The CIO management focuses on those policies, processes, and organizational responsibilities necessary to accomplish the primary information resources management (IRM) missions in governing legislation and other guidance. Such responsibilities include strategic planning, business process analysis and improvement, IT architecture, resource management (to include capital planning and investment strategy), performance measurements, IT acquisition, IA, and the IT workforce. This chapter covers the required participation of HQDA, ACOMs, ASCCs, DRUs, regions, installations, and other separate Army activities in executing the IRM processes and facilitating CIO mandates. All statements regarding the CIO refer to the Army CIO/G–6 unless otherwise indicated.

a. The Army CIO position is established per 40 USC Subtitle III (CCA) and, as such, is the only federally mandated CIO in the Army.

b. A CIO's primary responsibility is IRM. Governing legislation cited in paragraph 2–1 of this publication directs improved management of agency information resources. The CIO provides advice to the SECARMY and other senior management personnel to ensure that IT is acquired and information resources are managed consistently with established investment decisions and priorities.

c. The CIO process will not routinely address IT systems that are funded under the NIP and MIP or other intelligence programs. Refer to para 2–11 of this publication.

d. The Army CIO EB plays a key role in the management and execution of CIO missions. The CIO EB is the primary vehicle for identifying and resolving enterprise-level CIO issues. Standing and ad hoc committees and working groups may also be established by the CIO or the board under its charter to conduct analyses and research or accomplish a given task. These groups will report recommendations/findings directly to the EB.

e. RCIOs/DOIMs will establish forums similar to the Army CIO EB (for example, councils and boards) for the purpose of developing and implementing IT processes, requirements, acquisitions, and funding decisions. The forums will involve primary customers and command and staff elements at the appropriate levels.

3–2. Information management organizations below Headquarters, Department of the Army

a. Subordinate organizations below HQDA, except as indicated below, may at their discretion designate the senior IM official as a "Chief Information Officer" and establish supporting offices within their organization. Regardless of designation, all IM organizations will comply with the governing legislation; Federal, DOD, and SECARMY guidance; and the appropriate responsibilities delineated in chapter 2 and elsewhere in this regulation. See also DA Pam 25–1–1.

b. Every region under the IMCOM will have an RCIO. The director/commander of the NETCOM/9th SC (A) regional unit is "dual-hatted" as the RCIO of the respective IMCOM regional director. In addition, specific non-IMCOM entities (for example, the USARC, Army National Guard (ARNG), MEDCOM, USACE, FMWRC) constitute virtual regions and will have a "virtual" RCIO. The RCIO duties include the following:

(1) Implement and enforce IM/IT policies, standards, architectures, programs, plans, and budgets for common-user concerns within their assigned regions.

(2) Oversee shared and common-user IT systems within their region and provide technical oversight and authority over DOIM-provided IT services.

(3) Develop and implement regional IM/IT procedures, as needed, to provide required guidance and direction to respective installations.

(4) Identify and consolidate regional IM/IT requirements. RCIOs will ensure that these requirements are validated, coordinated, and integrated per AR 70–1 and applicable interim guidance.

(5) Facilitate military IT support to civil authorities for Homeland Defense-related activities.

(6) Ensure that written contingency plans providing for effective withdrawal or destruction of records in hostile or unstable conditions are prepared by all installations, to include any element in an overseas area not under the jurisdiction of a major overseas commander.

(7) Ensure compliance with established Army architecture standards.

(8) Maintain a uniform set of IT performance metrics for the regions.

(9) Provide required IA support and oversight to DOIMs within their assigned region.

(10) Review and validate all DOIM MDEP funding and re-programming actions for IMCOM installations in the region to ensure equitable distribution of resourcing of C4/IT across the region.

c. Every ACOM and ASCC will have a senior IM official as a principal staff officer with CIO-like duties. DRUs may have a senior IM official as a principal staff officer if required and designated in writing by the respective HQDA official. The duties pertain to IT support of command functions and exclude common-use IT, except for the development of common-use IT requirements. (See para 2–15 of this publication for a detailed list of responsibilities.)

d. MSCs may establish an equivalent IM official with the same staff responsibilities as an ACOM/ASCC senior IM official. (See para 2–24 of this publication for more specific information.)

e. The installation information manager is designated the DOIM at Army installations. There will be only one DOIM at an installation and a single DOIM at USARC. The installation DOIM will be the single authority for providing common-use IT services (C4IM Service List). The DOIM will be the initial focal point for tenant organizations and activities to obtain support for unique IT services that are not provided in the C4IM Service List. (See also para 6–1k.)

(1) DOIMs are assigned or designated by garrison commanders on IMCOM installations.

(2) The garrison DOIM is the only organization on the installation authorized and responsible to provide common-use baseline services on a non-reimbursable basis to all installation tenants as prescribed by the C4IM Services List.

(3) Installation DOIMs will collaborate with the appropriate TNOSCs to gain visibility over installation networks to achieve situational awareness for all supported units to include deploying force units.

(4) Other activities on an installation will not establish a DOIM but will have an IMO appointed on official orders to coordinate internal IT services with the DOIM. Where no post, camp, or station installation configuration exists, the host command or activity will coordinate with the respective RCIO to identify a DOIM to provide IT support. The IMO is the primary interface between the DOIM and the supported organization(s). Refer to DA Pam 25–1–1, para 6–5, for a complete description of functions.

(5) The STARC is equivalent to an installation for the purposes of providing IT support. (See para 227 of this publication for more information.)

f. Tenant and satellite organizations, separately authorized activities, Government-owned/contractor-operated facilities, regional support activities, USAR regional readiness commands, FOAs, and major staff entities will designate an IMO. The IMO will identify their organization's information requirements to the designated DOIM to obtain support.

3–3. Information management/information technology resource management

The CIO/G–6 will review, prioritize, and support resourcing for IT requirements for Army enterprise solutions during the PPBE processes consistent with DOD policy. See also chapter 2 of DA Pam 25–1–1 and DODD 8115.1.

a. Planning.

(1) Strategic planning. Strategic planning is conducted at many levels. National Military Strategy is derived from the National Security Strategy. The DOD Defense Planning Guidance translates National Military Strategy for the military departments and Defense agencies to develop their own strategic plans. The Army's strategic plan is The Army Plan (TAP). On a more near-term basis, the ASA(ALT) and the DCS, G–3/5/7 publish the Army Modernization Plan, which provides specific information on and direction for battlefield and supporting systems. IT modernization plans are in the Army Modernization Plan annexes.

(2) HQDA IT strategic planning. The Army Vision, the Army Transformation Vision, and the Army Campaign Plan form the basis for the future direction of IT. The broadest strategic IT perspective for the Army is in the CIO/G–6 Strategic Plan and other associated CIO planning documents.

(a) MA and domain leaders and commands will include information requirements in their respective plans.

(b) IT strategic plans below the Army-level will be used for internal planning and execution and will not be submitted to HQDA except when specifically requested by the CIO or other HQDA principal.

(c) These plans will form the basis for applicable resource requests to HQDA.

(d) IT strategic plans should include, at a minimum, the organizational vision, core missions, goals, and priorities.

(e) These plans describe how the vision and goals support the Army strategic vision, missions, and goals; architectural and network-centric developments; and ongoing efforts that conform to the AEA.

(f) The plans will also include any new process improvement efforts that may result in an IT investment, performance measurements in conjunction with organizational processes, and new systems partnerships with other organizations.

(g) The organization's implementation of the Army's IT investment strategy, IT infrastructure changes, acquisition strategy, and IA prerequisites are other areas for consideration.

(h) IT planning guidance at subordinate organizations (below command/RCIO level) is at the direction of the respective commands senior IM official, RCIO, or HQDA functional proponent, as applicable.

(3) IT capital asset planning. Capital planning for IT is an integral part of the IT strategic planning process. Capital planning provides the link between IT investment and mission outcomes as required by the CCA. IT capital planning is an integrated management process focused on achieving a desired business or mission outcome through the continuous selection, control, and life cycle management of IT investments. See also para 2–3 of DA Pam 25–1–1 and DODD 8115.1.

(4) The Capital Planning and Investment Management (CPIM) process includes selecting the IT investments and establishing their priorities throughout the PPBE process 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 (PEGs), 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.

(5) The CIO's investment strategy, together with other acquisition documents, such as the acquisition strategy and program baselines-forms the basis for the Army's IT Capital Plan. The investment strategy uses a performance-based methodology and incorporates enterprisewide performance measures as key criteria. The approved strategy produces the prioritized list of C4/IT investments to be used to support decision-making during the PPBE process and acquisition processes, to include planning, execution, and reallocation purposes.

(6) All IT expenditures (centralized and non-centralized programs, with the exception of NIP and MIP), irrespective of appropriation or dollar threshold, will be included in this annual program review process. Participants include, as a minimum, representatives from HQDA staff elements, USAR, ARNG, IMCOM regions, Army commands, DRUs, and installations.

(7) Command senior IM officials/RCIOs/HQDA proponents should also develop an IT investment strategy to assist in prioritization and funding decisions.

b. Programming.

(1) CIO representatives at the colonel and civilian-equivalent level will participate as members in PEG meetings. These representatives will advise the PEG members on the C4/IT investment strategy, technical implications, architectural compliance requirements, and other factors used in the PEG decision-making process. CIO representatives will participate in all PEG program decisions with C4/IT issues, such as funding (bills, bill-payers, and movement of dollars) and affected Management Decision Evaluation Package (MDEP) changes. The CIO serves as tri-chair with DCS, G–8 and ASA(ALT) for IT programs.

(2) The CIO PEG representatives will ensure that each new and revised program objective memorandum (POM) and unfunded requirement (UFR) submission for an IT system (costing $2 million or more in a fiscal year, or $30 million or more total lifecycle) contains a statement on accomplishing process analysis and that an analysis of alternatives (a business case) was conducted before initiating an investment. A summary of the process analysis and the analysis of alternatives will be provided in each MDEP brief to their respective PEGs, in concert with the Exhibit 300 report (per OMB Circular A–11).

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

c. Reporting of capital and other IT expenditures.

(1) The CIO/G–6 prepares and submits the IT budget bi-annually as part of the Budget Estimate Submission (BES) in September and the Presidents Budget submission in January. These submissions are in accordance with OMB Circular A–11 (Sections 53 and 300) and OSD supplemental guidance in DOD Financial Management Regulation 7000.14R, Volume 2B, Chapter 18, Information Technology Resources and National Security Systems, and other memorandums. The total procurement cost is considered when determining if a purchase is an expense or an investment item in accordance with ASA(FM&C) guidance and Defense Finance and Accounting Service (DFAS) Manual 37100 when adding, replacing, or modifying components to an existing system.

(2) The CIO/G–6 —

(a) Reviews, coordinates, and co-certifies the IT Budget in conjunction with the ASA(FM&C).

(b) Directs and assists the PMs of major IT investments in the preparation of the Exhibit 300 reports.

(c) Provides training and publishes a detailed users guide that includes instructions for completing the Exhibit 300 reports.

(d) Coordinates and presents the Annual Budget briefing to OSD and OMB on the major issues in the IT Budget submission.

d. Budgeting and Execution of C4/IT investments.

(1) HQDA proponents and Army commands will execute their FY IT budgets by selecting one of the following alternatives:

(a) Follow POM guidance and spend the programmed funds on the intended investments as validated by the PEG.

(b) Submit UFRs to the Army Budget Office in the form of input to the funding letter process.

(c) Submit a request for a CIO (AKM Goal 1) waiver for all IT expenditures using non-IT programmed funds that 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. See DA Pam 25–1–1, para 2–6d, for instructions.

(d) Exception to this guidance is the Army Intelligence Systems being funded by NIP and MIP.

(2) The CIO (Goal 1) waiver request assists the Army in ensuring that the HQDA proponents, Army commands, and separate organizations will curtail IT investments unless they have IT-programmed funds or a waiver from the Army CIO.

(3) HQDA proponents, ACOMs, ASCCs, PEOs, and other organizations will not obligate dollars against existing IT requirements using non-IT programmed funds within the year of execution without Army CIO approval.

(4) Senior IM officials and HQDA proponents will monitor IT expenditures to comply with the conditions listed above.

3–4. Portfolio Management

PfM facilitates management of IT resources by giving senior leaders the tools to determine the funding priorities for individual IT systems.

a. PfM is the management of selected groupings of IT investments using integrated strategic planning and architectures, performance measures, risk management techniques, transition plans, and PfM strategies.

b. All IT investments will be managed as part of the Army's IT portfolio.

c. IT investments must support the Army's strategic goals, mission, and interrelated strategies. Investments in unnecessarily duplicative or stove-piped systems will be terminated.

d. Defense business system certifications are required for any business system development / modernization investment costing in excess of $1 million in total DOD funds. Obligation of DOD funds for a business system modernization in excess of $1 million which has not been certified and approved by the DBSMC is a violation of the Anti-Deficiency Act.

(1) Sponsoring organizations which fund a BMA-registered system with development/modernization costs in excess of $1 million in total DOD funds will ensure their investments are reviewed by their domain lead, submit appropriate documentation in-turn to the CIO/G–6 as pre-certification authority and then to the appropriate Defense Business System IRB for approval. Funds may be withdrawn or withheld until the reviews are completed.

(2) Additional details pertaining to DBSMC certifications can be found in the DOD IT Business Systems Investment Review Process. See also http://www.defenselink.mil/DBT/tools_certification.html. (See fig D–1 for a table of MA and Domain leads.)

e. The DCS, G–3/5/7 is the HQDA focal point for oversight of requirements definition, force development, integration, structuring, combat and training developments, resourcing, and prioritization.

f. The DCS, G–8 manages the programming phase of the Army PPBE process to facilitate the development of the Army program and the transition to an Army BES.

g. The CIO/G–6 will—

(1) Ensure that PfM processes are incorporated into, and integrated with, each of the principal decision support systems: Joint Capabilities Integration and Development System (JCIDS), PPBE, and the Defense Acquisition System.

(2) Establish enterprise-level performance measures as an integral component of the transformation strategy, aligned with mission, vision, goals, and objectives.

(3) Review and revise the current process for maximizing the value, assessing and managing the risks of Army IT investments across the Enterprise, and ensuring consistency with evolving DOD policy.

h. The Army Portfolio Review Committee will

(1) Conduct Enterprise Level PfM Reviews.

(2) Adjudicate cross-MA issues when agreement cannot be made at the MA level. This includes the approval of cross MA binning disputes when agreement cannot be made at the MA level.

(3) Validate IT investments/capabilities and strategy influencing and supporting Enterprise IT management.

(4) Review and approve Domain IT investment strategies which are then used in the CPIM process for development of the enterprise IT investment strategy.

(5) Review and approve MA/Domain metrics when applicable.

(6) Serve as final approval authority for MA or Domain removal from the IT PfM Governance Structure.

i. Domain Leads will

(1) Establish Domain IT PfM plans and processes, consistent with specific MA guidance.

(2) Establish and validate Domain level IT investment baseline against Domain designated portfolios.

(3) Serve as the single POC for proposed investments in those capabilities managed by the domain.

(4) Provide and update, as necessary, a plan for reducing and eliminating unnecessarily redundant and stove-piped IT investments/capabilities.

(5) Utilize the Army Portfolio Management Solution (APMS) as the IT portfolio management decision support tool for conducting Domain IT PfM activities and determining within Domains where capability redundancies/gaps exist and where integration of products and services might better support warfighter needs. This process involves developing and maintaining a Domain IT Portfolio of systems by capability, maintaining a baseline of critical capabilities and ensuring IT Investment items are aligned with required capabilities, and identifying and prioritizing investments to satisfy Domain IT capabilities.

(6) Recommend opportunities for cross-Domain integration to continually improve delivery of IT-based capabilities in support of warfighter needs.

(7) Utilize existing DOD processes (JCIDS, PPBE, and Defense Acquisition System) to prioritize, synchronize, and fund opportunities identified by PfM processes.

(8) As required, perform a review as directed by the Business Transformation Agency in compliance with the FY 2005 National Defense Authorization Act which requires an investment review approval by the Defense Business Systems Management Committee be performed for all defense business systems development or modernizations which exceed 1M across the Future Year Defense Program (FYDP).

(9) Evaluate all Domain and sub-Domain proposed IT Portfolio investments based on: capability, AEA products, criticality to mission, interoperability, risk, strategic alignment, performance metrics, and program resources/costs.

(10) Ensure all Domain IT investment reviews focus on capabilities and include the full life cycle costs of IT expenditures.

(11) Participate in enterprise governance forums, as required, to identify opportunities for commonality in PfM techniques and provide solutions that are in the best interest of the enterprise.

(12) Establish and utilize outcome-oriented IT performance measures that are aligned with strategic guidance and the MA balanced scorecard in the Strategic Management System (SMS). Progress will be reviewed and reported through the governance structure.

(13) Establish, in coordination with the MA, key metrics, timelines, and milestones to track IT transformation.

(14) Coordinate, as required, with the DCS, G–3/5/7 and the DCS, G–8 to ensure issues of portfolio/system prioritization and funding are addressed during portfolio reviews.

(15) As appropriate, verify that the portfolio complies with integration/interoperability testing and configuration management of IT investment/capabilities at the Central Technical Support Facility (CTSF).

(16) Develop IT investment strategies that are capabilities-focused.

(17) Identify Domain systems as Legacy, Interim, or Core IT Investments in alignment with the Domains Transformation Plan.

(18) Validate Domain system criticality as mission support, mission essential, or mission critical in accordance with defined standards (DODI 5000.2).

(19) If applicable, identify Investment Tier (1, 2, 3, 4) based on validated funding.

(20) Notify identified ARSTAF functional area leads and APMS-identified primary, secondary, and tertiary stakeholders for investments binned in other MAs and Domains of key investment management and assessment sessions regarding investments binned in those areas prior to investment decisions being made.

j. ACOMs will

(1) Establish and utilize a command governance process that supports MA/Domain use of APMS as the primary portfolio management decision support tool and that provides a command level review of systems in APMS against outcome-oriented IT performance measures.

(2) Appoint command leads to perform PfM responsibilities.

(3) Identify, as required, functional proponents to perform MA and Domain responsibilities.

(4) Ensure IT investment items, to include all networks, are registered in the APMS-Army IT Registry (APMS–AITR) module.

(5) Ensure system owners comply with required data calls and maintain accurate system records.

(6) Ensure that before development of command-unique systems is initiated, the capability requirement is vetted through the appropriate enterprise-level Domain and MA in order to determine that the proposed system is not unnecessarily redundant.

(7) Ensure that all IT expenditures meeting APMS entry criteria are vetted and approved by the appropriate Domain lead before acquiring.

(8) Determine where capability redundancies exist within the Command and where integration of products and services might better support warfighter needs.

(9) Ensure that ACOM portfolios of capabilities are congruent with applicable MA and Domain strategic plans and portfolios.

(10) Maintain System Architectures that are compliant with AEA, MA, Domain, and other DoD/Joint architectures and policies, as appropriate.

3–5. Process analysis and business/functional process improvement

a. Per the CCA, IT investments must provide measurable improvements in mission performance. Prior to making an IT investment and initiating any process analysis or improvement, the following questions must be addressed:

(1) Does the process support core/priority mission functions?

(2) Can the process be eliminated?

(3) Can the process be accomplished more effectively, efficiently, and at less cost by another source (for example, another DOD component, another Federal organization, or the private sector)?

b. For purposes of this regulation, process improvement encompasses such areas as business/functional process improvement, process innovation, and business process re-engineering. Process improvement is an approach for analyzing and revising processes. The objective is to optimize process performance by streamlining procedures, eliminating redundant or unnecessary tasks, and optimizing resource allocations. Process analyses and improvements will not be initiated with a predetermined goal of a materiel solution.

c. All Army organizations at and above the installation level must analyze their missions and revise their mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes (CCA). At a minimum, process owners are accountable for ensuring process analysis and revision, as appropriate, for any IT investment of $2 million or more in a FY, or $30 million or more total life cycle cost. Additionally, any process will be assessed as mission needs change. Process analysis and appropriate revisions will be periodically performed for mission and performance effectiveness.

d. An improved process will include, but is not limited to, any or all of the following actions:

(1) Realigning processes with changed missions.

(2) Adjusting processes in response to changed resources.

(3) Improving customer service.

(4) Reducing cycle time.

(5) Eliminating non-value-added activities.

(6) Streamlining high-cost activities.

(7) Increasing product quality.

(8) Lowering costs of providing services.

(9) Adapting to changing technology and ISs.

(10) Integrating duplicative information across processes.

(11) Creating an integrated environment to promote enterprisewide knowledge sharing.

e. The process owner will determine the level of detail required for analyzing a process. At a minimum, the following must be accomplished:

(1) Validate the organization's mission, goals, and objectives as it relates to the process.

(2) Establish a vision of the improved process (the objective state).

(3) Consider using existing process models, recommended process changes, and implementation plans, if available.

(4) Document the current process and describe its deficiencies. If no current process exists, describe the situation causing the deficiency.

(5) Document the envisioned revised process.

(6) Benchmark and adopt best practices as appropriate.

f. Process analysis and improvements for warfighting requirements will be documented using the doctrine, organization, training, materiel, and leadership, personnel, and/or facilities (DOTMLPF) analysis. (See AR 71–9 and the Chairman, JCS (CJCS) Instruction (CJCSI) 3170.01 for further information on the requirements generation process.) Process analysis and revision via the DOTMLPF method will be accomplished before submitting an initial capabilities document. Process analysis for non-warfighting IT requirements will use the documentation specified in annual guidance. The following areas are generally exempt from formal process analysis as long as no significant process changes are associated with these actions: credit card IT acquisitions below $250,000, replacement parts for existing systems, and routine replacement or upgrade of office automation equipment (for example, upgrading a local area network (LAN) or replacing office computers).

3–6. Chief Information Officer validation of requirements

a. The CIO validates and the Chief of Staff of the Army (CSA) approves all IT/NSS requirements through the review of data on the Capabilities and Army Requirements Oversight Council (AROC) Management System. The CIO/G–6 review focuses on the integrated architectures that reflect the appropriate family-of-systems context to support IT/NSS interoperability requirements. The CIO/G–6 ensures that IT infrastructure requirements to sustain interoperability and supportability requirements are identified in the Army's budget submissions. The CIO/G–6 reviews requirements documentation for interoperability and supportability. CIO/G–6 validation of IT/NSS provides a record that CIO-related statutory mandates have been completed. Validation criteria will include

(1) Determination that non-materiel alternatives were judged to be inadequate per AR 71–9, the JCIDS process, and a process analysis (that is, DOTMLPF analysis) has been completed to make this determination.

(2) Compliance with DISR standards and architectures (to include OV, SV, and TVs) that focus on the four key net-centric elements: Internet Protocol, secure and available communications, assured sharing, and quality of service measured through the Net-Key Performance Parameters.

(3) Evaluation of emerging technologies for new system solutions and as technical insertions in fielded systems.

(4) Inclusion of outcome-oriented performance measurements.

(5) Compliance with IA requirements.

(6) Inclusion of spectrum management certification.

(7) Evaluation of new or modified requirements against the existing IT infrastructure and systems.

(8) Evaluation and review of the Information Support Plan to assess interoperability, supportability, synchronization, sufficiency, and net-centricity issues.

(9) Other criteria as appropriate.

b. The DCS, G–3/5/7 manages the requirements review process, including the AROC and the Requirements Review Council. The CIO/G–6 participates as a member of these councils to represent the IT perspective on the requirements review process.

3–7. Information technology performance measurements

a. IT performance measurement. 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 against an established baseline.

b. Types of measurements. Organizational performance measures must measure both the effectiveness and efficiency of programs, projects, investments, and so on. These measures must be linked to a stakeholder community and be associated with defined funding lines:

(1) Measures of effectiveness demonstrate that an organization is doing the right things (products, services, and culture change) and achieving at least the intended outcomes (mission effectiveness and customer satisfaction).

(2) Measures of efficiency demonstrate that an organization's investments result in the lowest cost and highest level of productivity.

c. Measurements for IT investments. Performance measures will be developed for each C4/IT investment supportive of organizational missions before execution or fielding of that investment. The performance measures will gauge the value-added contribution of the IT investment to missions, goals, and objectives and provide a clear basis for assessing accomplishment, aiding decision-making, and assigning accountability at each management level. These measures will be directly supportive of the metrics used in the Strategic Management System (SMS), the Army's IT Metrics Program, or other defined programs.

d. Performance measurements in requirement documents. Performance measures in support of IT/NSS will be included in the appropriate documents per AR 71–9.

e. Performance measurement linkages. As performance measures are developed, linkages between management-level goals, objectives, and measures will be maintained. Functional strategic plans will be explicitly linked to the goals and objectives in TAP. IT performance measures contained in these plans will directly link to measures in capital plans or investment strategies.

f. Enterprise level. Enterprise-level IT performance measures will assess Armywide mission accomplishments and will generate outcomes that guide policy direction and strategies. The CIO/G–6 will establish/maintain C4/IT performance measures and provide input data to the SMS. Data from the APMS and the Army's IT Metrics Program (see para 3–7i, below) are two sources from which input can be drawn. IT measures at the Army enterprise level will ensure that

(1) Investments are synchronized with overall DOD/Army mission priorities, cross-functional key performance parameters, and net-centric objectives.

(2) Investments are yielding expected results and acceptable return on investment, including quantifiable improvements in mission effectiveness.

(3) A proactive oversight/insight system is operational and ensures mission benefit, cost, and schedule goals are met.

g. Functional level. IT performance measures at the functional level will assess functional mission outcomes relative

to strategic objectives of the next higher organization. Functional managers at HQDA and commands will develop a subset of goals and objectives with appropriate performance measures to gauge overall functional mission improvement. Accomplishments made at this level will be reported to enterprise-level managers to make Armywide decisions.

(1) IT performance measures will be assessed across multiple projects and initiatives and will focus on managing and improving operations.

(2) Performance will be customer-oriented with an effective outcome priority.

h. Program/project level. Performance measures at the program/project level will assess progress toward accomplishing expected functional mission outcomes and results of IT investments by collecting information (that is, metrics) on the investment's cost, schedule, and performance against an established baseline. Project-level outcomes will be reported to functional-level managers who make functional/operational decisions across programs, projects, or acquisitions. Program/project-level information is—

(1) Typically defined in terms of cost, schedule, and performance rather than goals and objectives.

(2) More detailed and focused on measuring progress toward completing specific tasks rather than on measuring general benefits to the Army.

i. Army IT Metrics Program (installation). This 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 (https://www.itmetrics.hua-.army.mil). Compiled IT metrics data will be used to identify mission capability shortfalls and to support the reallocation of IT investment resources. Refer to the DA Pam 25–1–1, para 2–4j, for complete instructions on this program.

j. Cost-benefit analysis. A cost-benefit analysis must be applied against any proposed performance measurement system. (Refer to DA Pam 25–1–1, para 2–4.)

3–8. Information technology/National Security System acquisition process

The acquisition process begins when an organization's C4/IT needs have been established and approved in the appropriate capability documentation.

a. The acquisition process involves validating requirements to satisfy the users needs; understanding how the business process analysis is accomplished by evaluating outcome and output-oriented performance measurements; monitoring the solicitation and selection of sources, award of contracts, and contract financing; evaluating contract performance; monitoring contract administration and those technical and management functions directly related to the acquisition process per AR 70–1.

b. CIO oversight of IT/NSS acquisition. The CIO will ensure that IT/NSS are acquired and information resources managed within an integrated framework. The CIO provides oversight for IT/NSS during the acquisition approval process (AR 70–1).

c. CIO assessment. The CIO will recommend whether to continue, modify, or terminate Army programs with an IT impact (CCA). CIO assessments, which incorporate multiple factors, will be conducted at the appropriate milestone.

(1) The CIO performs the CIO Compliance Assessment on all ACAT I, II, and Special Interest programs for compliance with statutory and Army regulatory requirements prior to a Milestone Decision. Program, Project and Product Managers (PMs) preparing for a Milestone Decision at the ACAT I, II or Special Interest level must have a CIO/G–6 signed CIO Compliance Assessment memo as required in Annex C of the Modified Integrated Program Summary. (See AR 70–1 and DODI 5000.2 for additional information on acquisition program categories.)

(2) The Army CIO has delegated the CIO Compliance Assessment process for ACAT III level programs and other qualifying programs to the responsible Program Executive Officer (PEOs), Direct Reporting PMs, and Army Commands of the program. The CIO Compliance Assessment process applies to both ACAT and non-ACAT systems and must be completed to support evaluations prior to Milestone Decisions.

(3) The CIO/G–6 will perform these assessments and ensure all Information Technology acquisitions are in compliance with statutory and Army regulations.

d. AIC.

(1) The AIC process will be used to certify horizontal and vertical interoperability of all Army systems - regardless of their ACAT- prior to their release for fielding. This process allows a smoother transition of new systems into the Army's network-centric framework on the LWN. See also AR 73–1, paras 4–2 and 5–3, for more information on testing required to confirm systems interoperability.

(2) The CIO/G–6 (SAIS–AOJ) will provide a memorandum of certification upon successful completion of certification testing. The certification memorandum does not preclude any other certification requirements.

(3) The software baselining process is designed to facilitate the development and sustainment of system-of-systems interoperability. Organizations responsible for acquiring or maintaining specific systems with interoperability requirements will ensure compliance with the Army configuration management software baselining process. MATDEVs will implement software baselining in their respective programs. During the system development and demonstration phase of a system or service, the MATDEV must capture the detailed analyses, known limitations and technical design trade-off decisions that are made in the Information Support Plan. Systems (ACAT II or below) which are not on the OSD

Special Interest List may apply for permission to produce a Tailored Information Support Plan (TISP) through Army CIO/G–6 from the Joint Staff. The TISP format is a simplified format to speed the process. TISP authorization applications should be forwarded to HQDA, CIO/G–6, ATTN: SAIS–AOJ. After the Information Support Plan/TISP is approved by the Army CIO/G–6, it is then reviewed as part of the Joint Staff Interoperability and Supportability Certification process.

(4) To achieve Joint interoperability, PMs must coordinate with the Joint Interoperability Test Center at Fort Huachuca. (For additional information, see http://jitc.fhu.disa.mil/.) PMs and acquisition community should comply with all pertinent DOD policies on IT standards which restrict some IT acquisitions to the Joint Interoperability Test Commands (JITCs) Approved Product List (APL) per P.L. 107–314.

e. Architecture standards. Army systems are required to comply with the mandated standards contained in the DISR (https://disronline.disa.mil/a/DISR/index.jsp). Exceptions to this requirement are permitted via a waiver or approved change request. Complete information on the waiver process is provided in para 4–2 of this publication.

f. Privacy Impact Assessments (PIA).

(1) Army system owners or assigned program mangers will:

(a) Conduct a PIA of privacy issue considerations when procuring, developing, or modifying an IT system to collect information in identifiable form from or about members of the public.

(b) Complete the assessment using the prescribed format located at http://www.army.mil/ciog6/links/privacyimpact.html.

(c) The responsible official will forward the completed PIA to the Office of the CIO/G–6 via e-mail to cio_g6pia@us.army.mil.

(d) Fill out the PIA completion data for the system in the APMS, as required.

(2) The CIO/G–6, as the PIA reviewing official, will—

(a) Ensure that IT being developed and used protects and preserves the privacy of the American public.

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

(c) Ensure that each PIA has been reviewed by the Army Information Assurance Official and the Privacy Officer.

(d) Maintain a repository of approved PIAs.

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

(f) Post all approved PIAs on the Army PIA public Web site (http://www.army.mil/ciog6/links/privacyimpact.html) in accordance with current DOD instructions.

(3) The Director, Office of Information Assurance and Compliance (OIA&C), NETCOM/9th SC (A), will review and ensure that the system complies with IA policies prior to the CIOs approval.

(4) The Army Privacy Officer (OAASA) will review and ensure that privacy issues have been properly identified and evaluated prior to the CIOs approval.

3–9. Accelerated use of commercial off-the-shelf information technology software 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, the Defense Acquisition System, identifies the order of preference for DOD in acquiring capabilities. 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.

a. To ensure compliance with the above policies, each system PEO/acquiring organization will establish and report a baseline of its commercial IT/NSS software assets, non-commercial IT/NSS software assets, commercial IT/NSS services, and non-commercial IT/NSS services. The baseline will be developed and maintained at the system/program level and at a component summary level. It will be reported to the MA domain and will enable Army leaders and managers to determine the current status of commercial IT/NSS software and services, plan for increasing their use, and measure progress toward achieving the DOD goal. For policy on the use of enterprise software agreements, refer to para 6–2e.

b. 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/acquiring organization must annually confirm that its system is in compliance with the above and reports the results achieved toward meeting the goal of increasing the use of commercial IT/NSS in the Army.

3–10. Information management/information technology human capital management

The CIO is responsible for the policy, oversight, and management of the Army Civilian ITM CP34. See also para 2–7 of DA Pam 25–1–1. The CIO will—

a. Define IM/IT competencies and provide career development guidance for Army IM/IT professionals.

b. Provide education, training, and professional development opportunities for Army IM/IT professionals to support effective acquisition, management, and use of IT resources, products, and services.

c. Promote plans, strategies, and initiatives for hiring, training, and retaining civilian personnel in IM/IT areas.

d. Promote collaboration between military and civilian IM/IT career management systems and integrate these efforts into Army institutional training as appropriate.

e. In partnership with TRADOC, ensure that as technology evolves, requisite new competencies are identified and integrated into TRADOC, the Defense Acquisition University, and the IRM College curricula.

f. Serve as the proponent for the Army e-Learning Program.

g. Support the Acquisition Career Management Office for Category R (IT career field) for civilian members of the Army Acquisition and Technology Workforce.

3–11. Registry for major information systems inventory, reduction, webification, and security

a. Army Portfolio Management Solution–Army Information Technology Registry module. The APMS–AITR module is the Army's single authoritative registry for IT investments, capabilities, and systems. The APMS–AITR module is used to manage the mission-critical, mission-essential, and mission support systems reported to the OSD, OMB, and Congress. See also para 9–7 of DA Pam 25–1–1.

b. System owners. System owners are responsible for certifying their APMS–AITR records as accurate and complete. Any system categorized as NSS regardless of ACAT or Mission Assurance Category is, by definition, considered to be a system and shall be reported in the APMS–AITR module. System owners will—

(1) Ensure that all Army applications/systems are correctly registered in the APMS–AITR and that all data fields are correctly updated at all times. Use AKO/DKO for APMS–AITR data entry. (See the APMS home page at https://apms.us.army.mil/.)

(2) Review and update APMS–AITR data at least quarterly.

c. Information Technology investments. IT investments for which the Army is a funding source and/or primary manager (for example, Executive Service of a Joint program, with the exception of intelligence systems which are reported in the Defense Intelligence Mission Area) shall be registered in APMS if the item can be reported without divulging classified information and meets any of the following criteria:

(1) The IT investment item costs more than $25K in any year of the FYDP (including acquisition development/modernization and sustainment costs).

(2) The investment item has undergone or is required to undergo security certification and accreditation per DODI 8510.01, unless the security certification and accreditation is done at a higher system level. (An IT investment item that costs less than $25K in any year of the FYDP (including acquisition development, modernization, and sustainment costs) and is accredited by name on an Army network does not need to be separately registered.)

(3) The IT investment is an Army initiative that has been certified by the Defense Business Management Systems Committee.

d. Information System reduction. The Army's goal is to eliminate unnecessarily redundant or stove piped IT investments through streamlining and system consolidation. System owners and MA and Domain leads will report reduction plans in the APMS–AITR. Standard COTS desktop office automation is exempt from the reporting requirements of this document. Information concerning MA and Domain Leads is provided in figure D–1.

e. Information System webification. All IT systems must be webified (that is, Web-enabled and linked to the AKO/DKO portal) or receive a waiver from the CIO/G–6. Acquiring organizations must report their webification status and future webification plans of their respective systems within the APMS–AITR.

f. Information System security documentation. The Federal Information Security Management Act (FISMA) (44 USC Chapter 35) mandates that the security status of Army ISs be documented, updated, and verified at least annually. The APMS–AITR will be used to implement this requirement.

g. Use of supportive databases. The requirement to use APMS–AITR does not preclude agencies from constructing internal databases to handle system management operations. However, system owners still have the responsibility to keep APMS–AITR updated as the Army's primary source of IT system information.

Chapter 4
The Army Enterprise Architecture

4–1. General

This chapter defines the Army Enterprise Architecture (AEA) and provides policy and guidance governing the composition and use of architecture documentation within the Army. See also chapter 2 of this publication for unique architecture responsibilities.

a. EA is a strategic information asset base, which defines the mission, the technologies necessary to perform the mission, and the transitioned processes for implementing new 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 defined in the current

version of the Department of Defense Architecture Framework (DoDAF). As an architecture description, 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. Purpose. The purpose of the AEA is to support 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. The Army's AEA is used as a framework and decision support tool to guide the maintenance of existing IT investments, acquisitions, and fielding of integrated system-of-systems capabilities. The AEA includes guidance to develop integrated architectures by incorporating OVs (requirements), SVs, and TVs (technical standards) for the Army's operating force and generating force for Army tactical units, functional areas, and installations.

e. The purpose of the AEA is to develop a body of rules that will limit the diversity of IT initiatives and support the development of IT resources systems that are compatible with the Army strategic direction. EA principles and deliverables guide IT decision-making. Standards are the rules that enforce compatible IT development across the enterprise.

f. As an enterprise, the Army transitions from a current or baseline architecture towards their target EA. The AEA can help the Army eliminate unnecessary or redundant processes and reallocate the resources that support them. This chapter outlines the AEA and implements IT-related guidance that applies to the development, promulgation, implementation, management, and maintenance of the AEA. See also chapters 4 and 5 of DA Pam 25–1–1.

4–2. Compliance with Defense Information Systems Registry standards

Army systems are required to comply with the mandated standards contained in the DISR (https://disronline.disa.mil/a/DISR/index.jsp). Exceptions to this requirement are permitted via a waiver granted by the Army CIO/G–6 or an approved change request (CR) as required by DODI 4630.8, para 5.8.2.

a. Prior to milestone B, retired standards will require a waiver. Emerging and non-cited standards will require a CR or a waiver. PMs will submit CRs for emerging and non-cited standards.

b. If the CRs are not approved, or if acquisition schedules do not permit time for the CRs to flow through the DISR process by milestone C, PMs will provide waivers for those standards.

c. Prior to Milestone C decision, emerging, retired and non-cited standards will require a waiver.

d. The waiver request located in figure E–1 can be used to request Army waivers. The CIO/G–6 Enterprise Architecture Division (SAIS–AOE) office coordinates the waiver requests. The U.S. Army Research, Development and Engineering Commands Communications-Electronics Research, Development, and Engineering Center Army Systems Engineering Office (AMSRD–CER–STSEASE) provides a technical review and risk assessment/impact analysis.

e. The Army CIO/G–6 (SAIS–AOE) submits the waiver request with the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DOD CIO for review and concurrence for non-ACAT programs.

f. The CIO/G–6 (SAIS–AOE) reviews waiver requests for mitigation of potential negative impacts on cost, schedule, or performance.

g. Upon a positive recommendation and validation of the request, the CIO/G–6 signs a memorandum directed at the office originating the request, granting the waiver. SAIS–AOE then notifies the appropriate PM. Excluding extenuating circumstances, total processing time for waivers will not exceed 60 days.

h. The CIO/G–6 (SAIS–AOE) submits the granted waiver through ASD(NII)/DOD CIO to the Under Secretary of Defense for Acquisition, Technology and Logistics for review and concur for mission-critical or mission-essential ACAT designated programs.

i. Depending upon the nature of the waiver request, the waiver memo may contain a requirement to provide a DISR compliance transition plan to CIO/G–6 (SAIS–AOE) within 60 days of the date the waiver is granted.

4–3. Composition

The AEA describes all echelons and aspects of the Army enterprise. The Architecture descriptions will be developed in accordance with the current version of the DoDAF and DOD IT Standards, which are published separately in the DISR. See also DA Pam 25–1–1, chapter 4.

a. Where applicable, organizational architectures are components of the AEA.

b. The AEA will include reference models and federated architecture concepts to describe the relationship between the mission area architectures.

4–4. Operational View

Operational view (OV) products must conform to the current approved DoDAF document. OVs provide the operational perspective of the force. AEA development will adhere to the following Army OA community authority: TRADOC is the Army's Executive Architect to serve as the Army's Operational Architect.

4–5. System View

System view (SV) products must conform to the current approved DoDAF document. SVs provide the systems perspective of the force. AEA development will adhere to the following Army systems architecture community authority: ASA(ALT) is the Army's Executive Architect to serve as the Army's Systems Architect.

4–6. Technical View

Technical view (TV) products must conform to the current approved DoDAF document. TVs provide the technical perspective of the force. AEA development will adhere to the following Army technical architecture (TA) community authority: CIO/G–6 is the Army's Executive Architect to serve as the Army's Technical Architect.

4–7. Relationships with external architectures

The AEA must conform to DOD and Federal architecture policies and directives. Interfaces with other DOD components architectures must also be addressed.

4–8. Internet Protocol version 6 (IPv6)

a. Achieving a net-centric operations and warfare environment requires a transition from the Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). IPv6 offers many capabilities including increased address space, quality-of-service, and mobility enhancements that are key to dominating the net-centric warfare environment. The capabilities offered by IPv6 are critical to the Army's transformation to a net-centric knowledge-based force.

b. Before DOD (DISA) enables the NIPRNet core, Army organizations with internal network backbones that interface with the NIPRNet must plan for their networks to be IPv6-enabled to synchronize with the NIPRNet core transition.

(1) The Army must, to the maximum practical extent, ensure that all new IT procurements are IPv6 compliant. Specifically, any new IP product or system developed, acquired, or produced must:

(2) Interoperate with both IPv6 and IPv4 systems and products.

(3) If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features as required by Army's schedule.

(4) Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(5) This specifically applies to all acquisition systems with a Milestone C date of 1 October 2003 or later.

c. 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) Vender 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) JITC certification and inclusion on the APL.

d. Existing IT/NSS systems and infrastructure components must be migrated 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. The Army must include progress reports on meeting the requirement as part of its EA transition strategy.

f. As part of the architecture review process, per para 4–6 above, 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.

g. Requests for waiver should be submitted to CIO/G–6, ATTN: SAIS–AOE (IPv6 Transition) and must include the proponent organization, system name, acronym, POC name, and contact information.

4–9. Army Net-Centric Data Management Program (ANCDMP)

a. The Army Net-Centric Data Management Program (ANCDMP) establishes policies and procedures intended to control the production and applicability of data standards required to ensure data interoperability for data exchanges among ISs used in the Army. The ANCDMP addresses data standards creation and implementation as it applies to automated systems, applications, data exchanges, databases, record and document management, and information presentation within and across warfighting and business systems.

b. The ANCDMP facilitates the dissemination and exchange of information among organizations and ISs throughout the Army, DOD, and the Federal Government. The ANCDMP implements the information standards portion of the DISR and the DOD Net-Centric Data Strategy. Net-centricity is dependent upon the ability to locate and retrieve information and services regardless of where they are stored. A common data management strategy is essential to allowing authorized users to access required information. See also DODDs 8260.1 and 8320.2. (See para 1–7 of this publication for information sharing restrictions.)

c. The ANCDMP manages information requirements from data models and business rules within their mission, organization, and functional contexts down to data-element and data-value levels of detail.

d. The ANCDMP facilitates internal, joint, and combined interoperability through the standardization and use of common data standards.

e. The ANCDMP facilitates the specification of standard data management services and conformance test requirements and represents these requirements to data management standards committees, as appropriate.

f. The ANCDMP improves data quality and accuracy and minimizes the cost of data production and data maintenance.

g. The ANCDMP applies to all IS passing information through Army networks and/or Army IT assets in the net-centric information environment.

h. All data will be protected per AR 25–2 and AR 380–5.

(1) Data security classification will be identified and maintained as part of the data standards documentation if independent of specific use.

(2) COOP analyses will be conducted for data and metadata per the DOD Net-Centric Data Strategy.

i. MA and Domain leads, system owners, PEOs, and PMs will ensure their data architectures comply with Army and DOD data requirements by developing and maintaining data performance plan (DPP) artifacts in a DPP system (DPPS) environment wherein the standards, policies, procedures, data models, and business rules reside and are employed as appropriate.

4–10. Army data standards management

a. Data standards (specified in the DISR and other guidance documents and expressed as authoritative data sources (ADSs), information exchange standards specifications (IESSs), enterprise identifiers (EIDs), and eXtensible Markup Language (XML)) will be used to guide all data exchanges, including those needed to support legacy systems. Data management requirements will be included in IT planning documents.

b. All Army organizations producing or using data standards (ADS, IESS, EID, XML) will

(1) Ensure that only Army-approved data standards are used in systems.

(2) Register new data standards in the appropriate part of the DPPS, as needed.

(3) Provide input to Army data standards reviews.

c. The Army CDAd is responsible for oversight and development of Army data standards policy, guidance, and procedures. The Army CDAd will

(1) Identify institutional Army COIs, COI leads, and COI data administrators (COIDAds), who are responsible for data standards in their functional areas.

(2) Develop data standards strategies, implementation plans, and performance measures.

(3) Create, deploy, and maintain the DPPS in support of the ANCDMP. The DPPS is the Army vehicle through which COIs will support the DOD Metadata Registry.

(4) Establish a governance structure to oversee data standards implementation, including processes and procedures, working groups, tools, training, and other resources.

(5) Act as the Army focal point for data standards activities, to include coordinating with DOD and external organizations.

(6) Develop and maintain a list of mandated, Army-approved data standards.

(7) Provide input on program milestone reviews to ensure compliance with data management policy.

d. COIDAds will

(1) Identify COI data standards producers to carry out data management and standards actions for the organization and serve as liaisons between functional experts and technical personnel.

(2) Identify funding requirements in support of the data standards producers for their institutional COI.

(3) Develop data standards strategies, implementation plans, and performance measures.

(4) Create, deploy, and maintain DPPS content in support of the ANCDMP.

(5) Review the data structure of assigned data standards in the DPPS at each milestone and at five-year increments after system deployment.

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

f. To ensure valid implementation of data standards Armywide, COIDAds will manage ADSs, IESSs, EIDs, and XML.

g. Data standards producers will

(1) Use the DPPS. The DPPS is a centralized, metadata repository used for the procedural storing, universal viewing, and selective reuse of (all, or parts of) architectures, data models, business rules, and other DPP artifacts of functional Army systems. The DPPS content will be used to perform technical reviews of Army's functional data requirements. Information about Army data/metadata will be maintained and controlled in the DPPS as part of the standard metadata documentation.

(2) Use data standards.

(3) Use data standards documentation in ISs design documentation from the DPPS.

(4) Use data standards in newly developed and redesigned applications and, when feasible, in existing systems.

(5) Submit candidate data standards for approval to the respective COI maintaining the affected IESS early in the IS life cycle.

4–11. Authoritative data sources (ADSs)

a. The owner of Army reference data will make the coded data values available as an ADS to ensure maximum reuse and interoperability. These value sets will be stored in the DPPS.

b. Data synchronization requirements will be identified and documented as part of the ADS documentation.

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

d. Army IS PMs and/or managers will implement Army enterprise-level ADSs in their ISs.

e. Data standards producers will

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

(2) Synchronize ADS implementations with the standardized versions managed and published by those organizations with ADS Management Authority.

4–12. Enterprise Identifiers (EIDs)

a. All Army data collected and maintained in databases designated to support net-centric warfare capabilities will use globally unique EIDs to ensure full data integration, referential integrity, and data interoperability.

b. Data standards producers will

(1) Use EIDs in both specified legacy and all new ISs to ensure maximum data integration and data interoperability.

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

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

(4) Use EIDs 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 EIDs.

(5) Support and ensure that all pertinent data resources identified via globally unique EIDs 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 EIDs will be documented and published in the DPPS to facilitate exchanges by other users.

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

4–13. Information exchange systems specifications (IESSs)

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

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

(2) 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.

(3) Uses approved data types and coded domains.

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

(5) Has key attributes identical with or directly derivable from key attributes specified in the IESS. Alternatively, 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 EID from the ADS.

b. 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 supports the respective information system.

c. 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.

d. PM/MATDEV responsibilities:

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

(2) Respective COI(s) will review and/or approve submissions to the DPPS.

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

e. Data standards producers will—

(1) Use Federal Information Processing Standard 184 (IDEF1X) and the approved database standard (that is, Army National Standards Institute Standard Query Language 2003 Core) as their base set of data model artifacts and create necessary supporting business rules and processes as required by the DPPS to specify all IESSs. To ensure maximum interoperability, the IESSs must be implemented through software that reliably conforms to the DPPS.

(2) Add to the list of relevant tools any evolving structured languages for creating IESSs, if sufficient governmental and commercial support develops for them.

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

(4) Use International Standards Organization (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:

(a) ISO 11179 data elements from Joint COIs.

(b) ISO 11179 data elements from Army COIs mapped to those elements from Joint COIs.

(c) ISO 11179 data elements from other Federal department COIs mapped to those from Joint COIs.

4–14. Extensible Markup Language (XML)

a. All XML tags for use in data exchanges will be derived from the pertinent IESS adopted by the COI engaged in such data sharing and reuse activities. For ease of use, the physical data table and column names from the data models contained in the DPPS will be used for the generation of XML tags. However, logical names from the DPPS may also be used to enhance readability. If that is the case, an appropriate set of eXtensible Stylesheet Language/Transformation files to transform the tags into a form that facilitates the automated import into IESS-conformant databases will be provided and maintained by the COI.

b. 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 Metadata Registry.

c. Data standards producers will—

(1) Use World Wide Web Consortium (W3C) technical specifications holding 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.)

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

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

(b) XML implementations must not use proprietary extensions to XML-based specifications.

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

(4) Use existing XML components whenever practical vice developing new XML components. When selecting existing XML tags, Army activities will adhere to the order of precedence (highest to lowest) listed in (a), (b), and (c) below. The order of precedence 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.

(a) Joint COI IESS-based tags.

(b) Army COI IESS-based tags.

(c) Federal department COI IESS-based tags.

(5) Ensure that all Army XML business standards are at the enterprise level of the entire Army.

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

Chapter 5
Information Assurance

5–1. Mission

FISMA requires all agencies (DOD/Army) to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency or ISs used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (Title 44, Section 3544 (a) (1) (A)). Per DODD

8500.1, DODI 8500.2, and AR 25–2, Information Assurance, provides the means to ensure the confidentiality, integrity, availability, authentication, verification, protection, and non-repudiation of information processed by Army ISs. IA provides a measure of confidence that the security features, practices, procedures, and architectures of an IS accurately mediates and enforces the security policy. Interconnected systems create shared risks and vulnerabilities where an intruder has only to penetrate the weakest link in order to exploit the entire network. The value of information must be measured in terms of how critical it is to the authenticity and integrity of the data and is as important as the confidentiality of that information. IA includes security of information and related systems, C2, physical, software, hardware, procedure, personnel, networks, communications (COMSEC), operations, intelligence, and risk assessment.

a. IA Vulnerability Management (IAVM). IAVM is a process within the IT/NSS system that provides for a sensing of valid information about events and the environment, reporting information, assessing the situation and associated alternatives for action, deciding on an appropriate course of action, and issuing messages directing corrective action. Additionally, IA protects those ISs essential to the minimum operations of the Army. They include, but are not limited to, telecommunications, weapons systems, transportation, personnel, budget, common use IT, and force protection. See also AR 25–2, para 4–24.

b. IA components will be integrated to protect information and ISs from the wide-ranging threats to the Army's critical information infrastructures, to include the basic facilities, equipment, and installations needed for the function of a system, network, or integrated network that will support the national security of the United States and the continuity of government communications.

c. IA enhances effective C2 of friendly forces by protecting critical information infrastructures from unauthorized users, detecting attempts to obtain or alter information, and reacting to unauthorized attempts to obtain access to or change information. These measures focus on the integrity, confidentiality, availability, authentication, verification, protection, and non-repudiation of the infrastructures and the information contained within. IA-enabling technologies such as Public Key Infrastructure (PKI) and biometrics will be used to enhance information protection.

5–2. Management structure for information Assurance

An appropriate management structure will be established at all levels to implement the IA program per AR 25–2 for the protection of critical ISs and infrastructures. Commanders will appoint, as appropriate, personnel who are responsible for enforcing the Army IA program processes.

a. ACOMs; ASCCs; DRUs; PEOs; direct reporting PMs; CAR; Chief, National Guard Bureau; FMWRC; RCIOs; and the Office of the AASA (serving as the HQDA ACOM Commander) will each establish an IA program and appoint an information assurance program manager (IAPM) to manage their respective IA programs and to serve as the commander/director/activity head's IA representative. The IAPM will be accountable for establishing, assessing, enforcing, and reporting the effectiveness of the IA program within that organization.

b. The scope of each IA program includes ISs that may be unique to that organization. For complete descriptions of the IAM and IASO positions, reference paras 3–2d and 3–2f, respectively, of AR 25–2.

c. The IAPM will ensure the appointment of the appropriate number of IA personnel as necessary to execute the IA duties and responsibilities.

d. The RCIO IAPM will ensure the installation IAM and IA network officer(s) are appointed for each installation or cluster of small posts/camps/stations within the region.

e. Army organizations are responsible for disseminating IA policy standards, mandates, and IAVM messages and for reporting compliance in accordance with HQDA policy.

5–3. Information system certification/accreditation

a. All ISs and networks will be subjected to an established certification and accreditation process that verifies the required levels of IA controls are achieved and sustained for compliance.

b. Only IA products from the Army's IA APL available at https://informationassurance.us.army.mil will be used. ISs and networks will be certified and accredited per the Army's implementation of the DOD Information Assurance Certification and Accreditation Process (DIACAP) Guidance and Director of Central Intelligence Directive (DCID) 6/3. The DIACAP considers the importance of information relative to the achievement of Army goals and objectives, particularly the war fighters combat mission.

c. NETCOM/9th SC (A) has overall responsibility for ensuring that all ISs are properly certified and accredited in accordance with the DIACAP. System owners, PEOs, and direct reporting PMs will be responsible for certification and accreditation of enterprisewide and unique systems that they own and operate. The DIACAP will be applied to all systems requiring certification and accreditation throughout their life cycle (see also AR 25–2, chap 5). Where applicable, all IA-related Government-off-the-shelf (GOTS) and COTS hardware, firmware, and software components and IT products used in the AEI must be evaluated and acquired in accordance with the DODD 8500.01 and other applicable national and DOD policy and guidance identified in this chap or in AR 25–2, chapter 4.

d. Special Access Program (SAP) system accreditation authorities will be retained at the HQDA level. SCI SAP/SAR system accreditation authority will be retained at the DCS, G–2 as designated by DIA. The CIO/G–6 will appoint

the DAA as the SAP accreditation authority for systems that process SECRET SAP information. (See also AR 380–381 and AR 25–2.)

5–4. Software security

a. Controls will be implemented to protect system software from physical and logical compromise, subversion, or tampering. All software to be used on Army information systems and networks will be managed through a configuration management control process and be approved by the DAA prior to installation and operation on LANs. Systems administrators will ensure all systems use Army Gold Master (AGM) security configurations. Any deviations from the AGM security configuration must be approved by the DAA and included in documentation made available to all SAs, IASOs, IAMs, and DOIMs.

b. When database management systems (DBMS) containing classified information are used, the classified identifiable element (for example, word, field, or record) within the database must be protected according to the highest security classification of any database element. If the database cannot provide field protection, then it should provide record protection to the highest security classification level of the fields within the record. Database systems that do not provide protection at the record or field level will be restricted to operation in the dedicated or system high security mode. In all cases, the DBMS must meet the minimum trust requirements. (For more information, refer to AR 25–2.)

c. All software packages providing IA services will have appropriate evaluation/certification prior to use and must be selected from Army IA APL first. If no product exists, then follow the Army policy identified in AR 25–2, para 4–20 on IA tools selection process. Other evaluated IA products may be used based on a valid justification and approval from the CIO/G–6 as the Enterprise DAA. Agencies responsible for distribution of software security products will comply with DIACAP after the product IA protection profiles have been validated by the National Institute of Standards and Technology/National Security Agency (NSA) National Information Assurance Partnership program. (For more information, refer to AR 25–2 para 4–20 and NSTISSP No. 11.)

d. Developers of Army systems are mandated under FISMA to include appropriate security features in the initial concept exploration phase of the life cycle system development model. Software will be independently tested and verified to ensure that it meets the minimum standards for security and reliability prior to release for operation. See also AR 70–1, para 5–7.

5–5. Hardware security

Hardware-based security controls represent an important factor when evaluating the IA and security environment of any Army system. The absence of hardware-embedded security features or the presence of known hardware vulnerabilities will require remediation in other elements of the security and IAVM programs. Developers of all Army systems that include hardware will include IA and security requirements in the design, development, and acquisition of the system, software, and physical environment of the system. Only approved ports and protocols may be used per DODI 8551.1. See also DISA's Ports, Protocols, and Services (PPS) Assurance Category Assignments List at https://powhatan.iiie.disa.mil/ports/index.html.

5–6. Procedural security

All commanders (or equivalent heads of activities), to include IMCOM region directors/RCIOs will identify key IA personnel to establish and enforce standard procedures to perform the following functions:

a. All information system security incidents will be investigated to determine their causes and the cost-effective actions to be taken to prevent recurrence. When security fails and there is a penetration, either successful or unsuccessful, the incident will be reported. Suspected or actual incidents will be reported through the chain of command to the Regional Computer Emergency Response Team/TNOSC.

b. During an information emergency, intrusion, or exploitation, IA personnel below the ACOM/ASCC/DRU level will report the occurrence to their commander and the next-highest IA level (who will then report it further up the IA reporting chain). IA personnel are responsible for timely reporting. They are also responsible for ensuring that Army IA alerts and advisories are reviewed and that corrective measures are taken and reported.

c. Any information system that processes data in a sensitive compartmented information (SCI) environment will ensure its equipment used for processing, handling, and storing is in compliance with Intelligence Community Directives.

d. User identification and authentication systems must support the minimum requirements of accountability, access control, and least privilege and data integrity. The IAM or designee is responsible for overseeing the generation, issuance, and control processes and ensuring that all systems are HSPD12 compliant. Common Access Card (CAC)/PKI login/authentication will be used on all systems without waivers from the CIO/G–6.

5–7. Personnel security

a. All positions where personnel have or require access to an IT system will be designated as an IT position in accordance with AR 25–2. Personnel assigned to designated positions must meet the security investigation requirements defined in DOD 5200.2R. (See AR 25–2, para 4–14, for further information.)

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

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

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

5–8. Communications Security (COMSEC)

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

5–9. Risk management

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

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

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

c. Implementation of countermeasures.

d. Periodic review of the risk management program.

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

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

Chapter 6
Command, Control, Communications, and Computers/Information Technology Support and Services

6–1. Information technology support principles

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

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

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

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

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

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

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

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

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

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

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

d. Official uses of telecommunications and computing systems.

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

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

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

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

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

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

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

(1) Do not adversely affect the performance of official duties by the employee or the employee's organization.

(2) Are of reasonable duration (normally five minutes or less) and frequency (twice per day), and, whenever possible, are made during the employee's personal time, such as during lunch, break, and other off-duty periods.

(3) Are not used for activities related to the operation of a private business enterprise.

(4) In the case of long distance (toll) calls, are—

(a) Charged to the employee's home phone number or other non-Government numbers (third party call).

(b) Made to a toll-free number.

(c) Charged to the called party if a non-Government number (collect call).

(d) Charged to a personal telephone card.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

or more of the standards listed in the C4IM Services List. Army activities desiring enhanced IT services will request and obtain these services from the installation DOIM on a reimbursable basis. Army activities and DOIMs will enter into support agreements for enhanced services.

(3) Mission-funded services - These services are specifically designated as "mission funded" in the C4IM Services List, Army activities will reimburse the Garrison DOIM for these services unless the DOIM determines that DOIM operations cannot reasonably provide the required service.

(4) Mission-unique services - These services do not appear on the C4IM Services list since the list only includes the most commonplace IT services. Resourcing and provisioning for these services are the responsibility of the tenant activity. If the unique mission service (lab, test range, and so on) interfaces in any way with the installation IT infrastructure, activities will submit acquisition plans to the installation DOIM for review and comment. After receiving DOIM comments, Army activities may acquire mission unique IT services by—

(a) Providing mission services with internal organization resources.

(b) Obtaining contract support for mission services.

(c) Reimbursing DOIM for mission services. Army activities and DOIMs will enter into support agreements for mission services provided by DOIM.

(5) Contract support will be obtained using existing Army enterprise contracts available from Computer Hardware, Enterprise Software and Solutions (CHESS) (formerly known as the Army Small Computer Program). Refer to paragraph 6–2 for additional information on the use of CHESS.

l. Service and support agreements with DOD activities. 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. A service level agreement (SLA) will be established for delivery of IT services. An inter-Service support agreement (ISA) 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 DOIM must be a participant in the ISA coordination. Depending upon the scope of the ISA, the RCIO(s) may be included as a third party.

m. 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; it is in the best interest of the U.S. Government; the supplying activity is able to provide the support; the support cannot be provided as conveniently or economically by existing DOD services or commercial enterprise; and 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/SLA.

n. MWR activities and nonappropriated fund instrumentalities (NAFI). Use of appropriated funds (APF) on a nonreimbursable basis is authorized to provide communications and data automation support to—

(1) MWR activities as outlined in AR 215–1 (see app B–4 of this publication).

(2) TDY, permanent change of station, and military treatment facility lodging programs as outlined in Enclosure 3 of DODI 1015.12.

(3) Medical Holdover (MH) members residing in DOD housing. MH members are authorized the use of a television with cable/satellite service, Internet service, and telephone service. MH members are responsible for charges on premium cable/satellite service and long-distance calls. DOIMs will ensure that sufficient controls are in place to safeguard against private misuse of Government communications.

(4) All other NAFI(s) as outlined in DODI 1015.14 (Army and Air Force Exchange Service (AAFES), Civilian Welfare and Restaurant Funds, and so on).

(a) NAFI will comply with AR 70–1 and this regulation for acquisition and management of MWR systems that are obtained with APF.

(b) AR 215–4 governs IT supplies and services acquired with NAFI.

(c) NAFI requiring DOIM-provided IT support will comply with this regulation and those procedures promulgated by the installation DOIM. See also appendix B-4, Army MWR programs and nonappropriated fund (NAF) activities.

o. IT support for telework.

(1) Telework is defined as an arrangement in which a government employee or member of the Armed Forces performs assigned official duties at an alternative worksite on either a regular, recurring, or ad hoc basis (not applicable while on official travel or checking e-mail). Contractors' work sites are determined by the contracts in force. The functional proponent for telework, DCS, G–1, is responsible for promulgating human resource management policy on telework. The telework alternative site is a place away from the traditional worksite that has been approved for performance of official duties. An alternate worksite may be an employee's home or a telecommuting center established for use by teleworkers. See additional information on the DOD telework program in DODD 1035.1, on the DOD telework Web site at http://www.cpms.osd.mil/telework.aspx, and in DA Pam 25–1–1, paragraph 7–6 and appendix B.

(2) Use of Government IT resources (such as computers, facsimile machines, modems, and so on) for telework is authorized, contingent upon availability of funds and certain conditions that are approved by the installation, which can vary from one installation or activity to another. Government-furnished computer equipment, software, and communications, with appropriate security measures, are authorized for any regular and recurring telework arrangement. A

telework agreement that outlines the terms, conditions, and limitations of IT support for the arrangement is required before the employee commences regular/recurring telework. A telework agreement template and safety and supervisory checklists are available in DA Pam 25–1–1, appendix B. Where approved by the DAA, the use of employee-owned computers and equipment for telework is authorized. All telework agreements will address mandatory IA requirements and be approved by the DAA prior to implementation. Use of resources to fund limited operating costs associated with communications (for example, Digital Subscriber Line, cable modems, and analog dial-up lines) within an employee's residence as an alternative worksite may be determined by the local commander. (IT resources for telework resources are not intended for individuals who occasionally check e-mail from their residences.)

(3) Remote access to the Army portion of the GIG for telework purpose must be by a remote access server or approved Virtual Private Network connection and use of a CAC. Official government data must not be saved to the local data storage area of employee-owned equipment; it must be stored on the user's network data storage area.

p. Electronic and Information Technology (EIT) access for Army employees and members of the public. Title 29 USC 794d, 40 USC 762, and 20 USC 9201 require that agencies provide employees and members of the public who have disabilities access to EIT that is comparable to the access available to employees who are not individuals with disabilities.

(1) 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.

(2) Unless an exception applies (see DA Pam 25–1–1, para 7-5*e*), all Federal/DOD acquisitions of EIT must meet the applicable accessibility technical standards and/or the functional performance criteria (36 CFR 1194) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board at www.access-board.gov).

(3) 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, worldwide Web sites, multimedia, and office equipment (such as copiers and facsimile (fax) machines). Review Web site 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—

(a) All contracts for EIT supplies and services. Except for indefinite-delivery contracts, it is applicable to all delivery orders or task orders for EIT.

(b) All procurement actions for EIT processed by Government contractors, regardless of the customer being supported.

(4) Information managers will make all reasonable efforts to accommodate individuals with disabilities, consistent with the laws cited above and AR 600–7. The Computer/Electronic Accommodations Program (CAP), 5111 Leesburg Pike, Suite 810, Falls Church, VA 22041–3206, provides assistive technology accommodations and services to persons with disabilities at the DOD for no cost to individual activities. 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 for the deaf, telephone amplifiers, listening devices, closed captioned decoders, and visual signaling devices for those with hearing problems. (See paragraph 7-5 of DA Pam 25–1–1 and http://www.tricare.osd.mil/cap/ for more information.)

q. Installation-level technical support and service.

(1) Every DOIM will establish an installation-level help desk. See paragraph 6–4f of DA Pam 25–1–1. The help desk is the installation's first level of problem resolution and is the user's primary POC for IT and networking problems. Help desks normally will determine the type of reported system problem within defined response times outlined in a service agreement; report the status of the problem; and maintain a historical database associated with problem resolution. It also will provide a central repository for technical advice and solutions for networked systems, information processing accountability support, hardware exchange, and repair service support.

(2) Since DOIMs cannot provide equal technical support (for example, 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 on an exception basis only.

6–2. Computing services

a. Centralized IT contracts. The CHESS Office is the primary source for establishing commercial IT contracts for hardware, software, and services. The use of CHESS contract offerings makes purchasing more efficient through volume buying, thereby simplifying and centralizing IT lifecycle management throughout the Army enterprise.

(1) Organizations will use the CHESS, to the maximum extent possible, to purchase COTS software, desktops, and

notebook computers regardless of dollar value and for all other IT purchases greater than $25K. If a requirement cannot be satisfied based on this criteria against a CHESS contract, a waiver may be granted. Requests for waivers will be submitted through the CHESS Web site at https://chess.army.mil.

(2) The CHESS, in conjunction with the IT E-Commerce and Commercial Contracting Center, will conduct semi-annual consolidated buys for desktop and notebook computers.

(3) CHESS will, based on their ability to satisfy an organization's requirements, notify the acquiring organization if they may consider other DOD and federal activity contract capabilities. Other DOD and federal activity contract capabilities may be considered, if CHESS contracts do not meet requirements

b. AKM Goal 1 Waiver for IT initiatives. Refer to paragraph 3–3*d* for waiver requirements for the use of non-IT programmed funds for IT initiatives.

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

(1) The fee-for-service rates will be coordinated between the CIO/G–6 and the DOD providers for service provided to Army activities. Army activities will be assisted by the CIO/G–6 in resolving issues with provision of, and funding for, services from DOD providers.

(2) Coordination is required with the supporting DOIM in the determination of 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 organizations or facilities using an Army IP address must obtain Networthiness. See also DA Pam 25–1–1, paragraph 6–5*b*.

d. Area Processing Centers (APC) and server consolidation.

(1) APCs are the Army's enterprise environments located in DOD facilities where NETOPS, functional, and common-services information is stored, replicated, and managed. The architectural design of APCs will provide an enterprise services computing platform for the Army to improve network security, operational effectiveness of the information infrastructure, and reduce the Army's total cost of ownership for IT. Administration and management of functional mission systems located at either the APC or the Installation Processing Nodes (IPN) are the responsibility of the mission system owner. Engineering analysis and performance testing will be performed on all functional applications to insure applications performance specifications are met and maintained within operational specifications. Army IPN are extensions of APCs, located within DOIM facilities on select post, camps, and stations to provide a hosting environment for mission specific applications accessed only by local installation users. IPNs may host mission-specific applications on a permanent or temporary basis. Both APCs and IPNs will be operated, managed, and protected by NETCOM/9th SC (A). Common APC services will include: C4IM baseline services, messaging, discovery, collaboration, enterprise system management, enterprise-managed IT services, storage, mediation, user assistance (service desk), application services, and IA.

(2) DOIMs on each post will consolidate servers for Army tenants residing on the post at an APC or at the IPN or other designated server farm location approved by the RCIO. See also DA Pam 25–1–1, paragraph 9–4. Army tenants on each post will assist the DOIM in consolidating servers to locations specified by the DOIM. Army Defense-funded activities, to include NAF activities, will consolidate their IT assets within their own server farms. The DOIMs will establish agreements with supported tactical units for the use and management of tactical LAN servers. DOIMs will coordinate with the respective installation commander and Army tenants to develop the necessary requisite memorandums of agreement and service-level agreements to provide the resources to support server consolidation.

e. Office automation. See also DA Pam 25–1–1, paragraph 9–2*d*.

(1) *Office equipment.* Office equipment includes thin client workstations, desktop personal computers (PCs), servers, notebook computers, hand-held computers, and personal digital assistants (PDAs). Peripheral devices include any device designed for use with PCs to facilitate data input, output, storage, transfer, or support functions such as power, security, or diagnostics.

(2) *System software.* System software includes software required for PCs or thin client operations (for example, operating systems). Office automation applications include word processing, spreadsheets, e-mail, task management, graphics, and databases that do not require the greater computational power of special-purpose workstations.

(3) *Enterprise software licenses.*

(a) The Defense Supplement to the Federal Acquisition Regulations (DFARs), subpart 208.74, requires DOD components to purchase from the DOD inventory before buying the product from another source. When an activity requires a COTS product, the supporting DOIM will determine if it is available from CHESS, the Army's representative for the DOD Enterprise Software Initiative (ESI). See also DA Pam 25–1–1, paragraph 9–1*a*. Enterprise software agreements (ESAs) negotiated with specific software publishers or their agents provide the best available prices, terms, and conditions. The DOD ESA is the DOD implementation of the Federal-wide SmartBUY (Software Managed and Acquired on the Right Terms) program.

(b) An enterprise license agreement (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. The CHESS is the Army's designated Software Product Manager and exclusive source for all software through the ELAs.

(c) 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 DOIM. The DOIM 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 DOIM must notify the Army's ESA manager, CHESS, so that CHESS may improve the existing ESA prior to the DOIM's executing any other agreement. The acquiring DOIM will refrain from purchasing COTS before coordinating with CHESS regarding the establishment of a new agreement that may meet the requirement. 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 listed in para 6–2*a* above and the DOD ESI Web site, which lists all ESI-managed software, is located at http://www.esi.mil.

(4) *Thin Client technology.* In many computing environments thin client technology offers a lower total cost of ownership, increased productivity, and more robust security than offered by laptops and PCs. 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. PC and laptop environment options will be used only when available thin client solutions cannot satisfy all user requirements and is approved by the ACOM, ASCC, or DRU senior IM official.

(5) *Software control.* Users will not install new software packages, software upgrades, free software, freeware, shareware, unlicensed open source software, and so on, without the approval of the organizational DAA. Unauthorized software may contain harmful viruses or defects, which can result in the loss of data or system failure. Additionally, the use of such software may create configuration management problems, violate software copyrights or licensing agreements, or cause other difficulties. (See paragraph 5–4 for COTS software installation approvals.)

(6) *Leasing IT 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 in determining the required level of approval. Requests for leases will be validated consistent with procedures for DOIM validation of other acquisitions. See also DA Pamphlet 25-1-1, paragraph 11–2*e*.

(7) *PDAs.* PDAs with network or wireless interface capability will be managed and accounted for as PCs. Refer to paragraph 6–4*c* of this document for policy on acquiring wireless devices.

f. Purchase of energy-efficient computer equipment. All purchases of microcomputers, including PCs, monitors, and printers, will meet the Environmental Protection Agency Energy Star and green requirements for energy efficiency per EO 12845.

g. Standard software applications. Army activities will minimize the proliferation of software applications that provide similar sets of operational capabilities. For information on the Army IT PfM Program, reference paragraph 3–4 of this publication.

(1) *Approved applications.* Software applications that satisfy substantially the same set of operational requirements as that of approved standard applications will not be developed or acquired unless approved through the IT PfM process. Redundant applications will be eliminated. (See paragraph 3–11 of this publication for more information on the goal to reduce and webify applications and paragraph 3–4 for more information on the IT PfM program.)

(2) *COTS/GOTS.* COTS products or existing GOTS software applications will be preferred to funding new application development. The suitability of COTS or GOTS applications for satisfying operational requirements will be evaluated prior to initiating a development effort. Evaluation should include not only identification of COTS or GOTS products that can satisfy DOD, Army, or system-specific requirements, but also an assessment of the likelihood that the product or subsequent versions of the product will be available and supported throughout the life cycle of the system.

(3) *Open source software.* 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 GOTS software, to include—

(a) Comply with applicable systems security policy (see para 5–4) and;

(b) Be configured in accordance with DOD-approved security configuration guidelines available at http://iase.disa.mil/.

(c) Be certified for interoperability (see para 3–8*d*).

(4) *System fielding.* AR 700–142 and Networthiness Certification, per paragraph 6–3*c*, will apply when fielding software applications to multiple installations for standardized use in table of distribution and allowances (TDA) organizations. To implement total package fielding for software applications, IT MATDEVs and gaining organizations will—

(a) Field IT with 100 percent logistics support when prevailing conditions permit. IT MATDEVs will coordinate with the supporting DOIMs and ensure that all IT components (for example, communications, computer platforms, and system software) are fully supportable and interoperable.

(b) Develop and coordinate the materiel fielding plan (MFP) for fielding and acceptance of the software application. If the fielding process is sufficiently complex, iterative software fielding plans will be used to consolidate the resources required to successfully field new software versions. Coordination must include the commands' senior IM officials and installation DOIMs. Each gaining installation will be provided with the final MFP six months prior to the receipt of the new system. NETCOM/9th SC (A) Enterprise Systems Technology Activity (ESTA) ensures systems being fielded comply with the Networthiness process.

(c) Develop MFP per DA Pam 700–142, appendix F.

(5) *Equipment.* Employees requiring IT support will be provided with the appropriate equipment to access required software applications and data.

(6) *Software support.* IT MATDEVs with responsibility for the development of a multi-command software application will initiate its postproduction software support (PPSS). IT MATDEVs will plan, program, and budget for PPSS until the transition of PPSS responsibilities to the designated life cycle software engineering center, software development center, or central design activity is completed. The IT MATDEV will include planning for PPSS and its estimated cost in milestone decision reviews or in-process reviews, as applicable.

(7) *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. Commands and other users will not independently make changes to a software configuration item without approval from the DAA. Source code for these applications will not be provided to users unless it is authorized by the assigned software support activity and the system owner. The configuration manager will establish and promulgate procedures that identify using organizations, track when usage by an organization ceases, and permit users to make recommendations on required PPSS changes and enhancements. The Army Systems Architect ASA(ALT) must approve the cancellation of PPSS for any software application approved for standardized use.

h. Collaboration tools suites standards.

(1) All Army activities (operational (tactical) and institutional) investing in or implementing collaborative tools will use the enterprise collaboration services and tools on AKO/DKO to the greatest extent possible. The AEI Technical Configuration Control Board (AEI Tech CCB) maintains a list of enterprise collaboration tools and services on the APL, located on the AKO/DKO AEI Tech CCB Homepage (https://www.us.army.mil/suite/page/137449). 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 not met by current capabilities, they are required to submit those requirements to the Army CIO/G–6, ATTN: SAIS–GKM Division, for approval prior to implementing to a collaboration solution. Collaboration capabilities are defined as services/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) The Communications Electronic 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.

(3) This policy will be considered for C4/IT resourcing reviews and recommendations for funding. Army activities investing in collaborative tools should—

(a) Coordinate with CIO/G–6, ATTN: SAIS–GKM, to ensure that the capability is not currently available or will not be available in the near future within the enterprise.

(b) Working through their DOIMs, utilize established DOD/Army ESA through the CHESS Office whenever possible. Available ESAs can be accessed at the CHESS Office Web site: https://chess.army.mil.

i. Authorization and requisitioning. Automation equipment authorized in Common Table of Allowances (CTA) 50–909 and listed in Supply Bulletin (SB) 700–20, applicable modified table of organization and equipment (MTOE), TDA, or other appropriate authorization documentation, may be requisitioned within authorized allowances without submission of any IT specific planning or acquisition documentation to HQDA. 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. DOIMs document justifications for purchase requests within their installation's approval authority. Such procedures will be applicable to all Army tenants on the installation.

j. Property book accountability. Hardware will be accounted for, using the appropriate supply regulations addressing 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 also paragraph 9–1*e* of DA Pam 25–1–1.

k. Redistribution and disposal of IT assets.

(1) The screening, redistribution, and disposal of IT equipment are completed through the Defense Reutilization and Marketing System (DRMS). DRMS is the DOD-wide program for asset visibility, resource sharing, and asset redistribution. The Defense Logistics Agency is the responsible official of DRMS for DOD.

(2) The process for disposal of IT equipment is consistent with the process used for all other excess property. For further guidance and clarification on the processes and communications flow for the disposal of excess IT equipment,

installation DOIMs should contact their installation property book officer for guidance on reutilization, transfer, and donation programs for excess IT equipment or visit the DRMS Web site at http://www.drms.dla.mil. See also DRMS Instruction 4160.14, Volume IV, DOD 4160.21–M, and DA Pam 25–1–1, paragraph 11–3.

(3) DRMS supports EO 12999 through the DOD Computers for Learning Program. Refer to Web site https://www.drms.dla.mil/cfl-online for more information on this program.

(4) Per DOD policy, all hard drives of unclassified computer equipment leaving the custody of DOD must be overwritten, degaussed, or destroyed in accordance with the associated security risk of the information contained within the drive. See also DA Pam 25–1–1, paragraph 11–3*c*.

l. Proprietary software copyright protection. Users must agree to abide by the provisions of any license agreement before using the software. The user must protect proprietary software from unauthorized use, abuse, or duplication. Unless authorized by the copyright owner, Army users may copy proprietary software only for limited purposes (such as an archival copy) under the provisions of 17 USC 117. (Also see para 7–7.) The DOIMs must educate users on software copyright protection and maintain an inventory of software licenses purchased for use on all Army computers on their respective installations. Unlicensed and unauthorized software must be removed from Army computers. Army's private-sector service providers are also subject to software copyright laws and may be required to provide written assurances of compliance (EO 13103).

m. Life cycle depreciation and refresh. In planning life cycle requirements and calculating economic benefits of automation IT, three years from the initial date of installation will be used as the metric for obsolescence of common-use IT. Serviceability, maintainability, and utility will also be used as factors to consider in specific life cycle replacement decisions. This metric may vary according to mission requirements. System planning should include provisions for product upgrades during the projected life span to cover potential obsolescence, lack of vendor support, support of IA and requirements, and incorporation of alternative products or technologies when such changes are justifiable and cost-effective.

n. Computing services networthiness. All computing software, equipment, and devices using an Army IP address must achieve Networthiness Certification (see para 6–3*c*).

6–3. Network Operations

Network Operations (NetOps) is the operational framework to operate and defend the GIG to ensure information superiority. The employment of NetOps achieves assurance of system and network availability, information protection, and information delivery.

a. U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC (A)) is responsible for Army NetOps and for providing technical guidance on NetOps to Army organizations. See also DA Pam 25–1–1, paragraph 10–2.

b. Army Enterprise Network Operations Integrated Architecture (AENIA) is the baseline Enterprise NetOps architecture for the Army's LWN. As an integrated architecture, AENIA provides an enterprise level Army statement of NetOps requirements through the Operational, Systems, and Technical views. It also provides the warfighting capabilities underpinnings for NetOps systems and functional requirements.

c. The Networthiness Certification Program manages the specific risks and impacts associated with the fielding of ISs and supporting efforts, requires formal certification throughout the life cycle of all ISs that use the IT infrastructure, and sustains the health of the AEI. Networthiness Certification is concerned with the identification, measurement, control, and minimization of security risks and impacts in IT systems to a level commensurate with the value of the assets protected. Networthiness Certification applies to all organizations fielding, using, or managing ISs on the AEI/LWN, to include COTS and GOTS. Activities must obtain a Certificate of Networthiness before they connect hardware/software to the LWN.

(1) The CIO/G–6 establishes policy and oversight of the Army Networthiness Certification Program and monitors, reviews, and assesses the networthiness of systems during the acquisition process.

(2) NETCOM/9th SC (A)/ESTA will—

(a) Issue certificate of networthiness (CoN) for new or enhanced systems or capabilities prior to allowing them to connect to the AEI.

(b) Conduct random audits of AEI to ensure only networthy systems are connected.

(c) Define, review, and update networthiness criteria.

(d) Publish and maintain networthiness criteria procedures.

(3) Installation DOIMs and DAAs will—

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

(b) Ensure that all systems have received a CoN prior to allowing them to field or connect within their respective networks.

(c) Support NETCOM/9th SC (A) and NETCOM RCIO in the networthiness certification process by identifying specific issues and recommendations for overcoming the obstacles to achieving a CoN.

(4) NETCOM/9th SC (A) serves as the certification authority to validate from a location-centric view that the

resulting infrastructure can support the information system, there are no negative impacts to other systems from the information system, the information system does not introduce any security vulnerabilities, and the AIS can be managed and maintained. This validation ensures that—

(a) IT systems are documented and validated for supportability, security, compatibility, integration, manageability, and interoperability requirements.

(b) System infrastructure and interfaces are identified, coordinated, approved, and implemented.

(c) Appropriate architecture (to include AENIA) and systems design are incorporated into the overall networthiness process to ensure that new systems or their capabilities will not adversely impact the AEI.

(5) The MATDEV or system owner must submit a request for networthiness through the appropriate chain of command to NETCOM/9th SC (A) (e-mail to army.networthiness@us.army.mil). Developers must obtain Networthiness Certification for all ISs and supporting elements. (See AKO/DKO CIO/G–6 Collaboration Web site (https://www.us.army.mil/suite/page/137030) for current information and procedures.)

6–4. Telecommunications systems and services

Telecommunications provide the ability to gather and disseminate information through the transmission, emission, and reception of information of any nature by audio, visual, electro-optical, or electromagnetic systems. This section pertains to telecommunications systems and services, to include data networks, telephones (including cellular), pagers, radios, satellites, fax machines, video teleconferencing, voice over Internet protocol (VoIP), commercial television services, and others. These services provide the warfighter and sustaining base the telecommunications technology solutions needed to achieve their operational objectives. See also DODI 4640.1 for additional guidance on telecommunications equipment and services. Long-haul telecommunications are covered in paragraph 6–5.

a. Telephone systems and networks. Telephone support is provided through a combination of common-user and dedicated networks.

(1) DSN is the official DOD switched voice network and is the preferred telecommunications means for C2 users. However, if DSN cannot be used in a timely manner, or if the person being called does not have DSN service, other long-distance services may be used. The CJCSI 6215.01 provides the policies for all DSN/DRSN usage. DODI 8100.3 provides policy, procedures for test, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches, switched data, and services on DOD voice networks. Refer to paragraph 3–8 for interoperability testing requirements.

(2) Networx will be used for non-C2 administrative voice services. Networx services will be used for commercial access unless other commercial voice services can be accessed without the expenditure of APF to increase the number or type of existing commercial circuits. NETCOM/9th SC (A) is the Army's responsible official for Networx service contracts. All requirements for Networx will be submitted to NETCOM/9th SC (A) (ESTA–TT) for service provisioning.

(3) Telecommunications services in the National Capital Region. Washington Interagency Telecommunications Services provides centralized administrative telecommunications service for DOD in the National Capital Region (NCR) per DODD 4640.7 and DODI 5335.1, thus eliminating the necessity for each component to establish, operate, and maintain duplicative facilities. Tactical and special intelligence telecommunications are exempted from this directive.

(4) DODI 8100.3 requires an annual inventory of all telecommunications switches connected or to be connected to the DSN, Public Switched Telephone Network, and DRSN. The annual inventory requirement is satisfied by annually reviewing and updating, the information (as required) in the System Network Approval Process (SNAP) database and ensuring all new switches are registered. Therefore, switches are required to be registered into the SNAP Database. The Web site for registering switches into the SNAP database can be found at https://cap.nipr.mil/index.cfm.

b. Classes of telephone service. A DOD criterion classifies telephone service in military departments. Army telephones served by Government-owned or commercial telephone systems are classified as official (classes A, C, and D) or unofficial (class B) per Defense Finance and Accounting Service - Indianapolis Regulation 37–1, chapter 13. The class of service code consists of two alphanumeric characters. The first character indicates if the line is for official or unofficial use. The second character indicates the billing category. Classes of telephone service are identified in appendix B.

c. Requests for wired and wireless telephone and telephone-related service.

(1) *BASECOM funding.* The supporting DOIM will be the focal point for all common-use BASECOM on the installation or the supported area and the initial focal point for tenant organizations and activities to obtain support for unique BASECOM requirements not provided in the C4IM Service List. BASECOM falls into one of four categories of services listed in paragraph 6–1*k* of this document and is funded on a reimbursable or non-reimbursable basis depending on whether the service requested is on the C4IM Services List. If an Army user is in a location where there is no DOIM support available, the user will coordinate procurement directly with the NETCOM/9th SC (A). A lack of DOIM support does not negate the requirement to procure devices and service through the NETCOM/9th SC (A) or the use of the BPAs.

(2) *Service requests.* DOIMs will submit BASECOM service requests to NETCOM/9th SC (A) (ESTA-TT) with a

courtesy copy provided to the respective RCIO office. NETCOM/9th SC (A) will obtain BASECOM telecommunications service requests - such as local central office trunks, commercial business lines, and Foreign Exchange (FX) trunks/lines via consolidated local service contracts that are competed among interested service providers. NETCOM/9th SC (A) will satisfy requirements for BASECOM local leased telephone services through BASECOM consolidated contracts and wireless requirements via blanket purchase agreements (BPA) contracts. DOIMs will obtain operation and maintenance (O&M) for installation telephone plants through NETCOM/9th SC (A). Those interested in acquiring local leased telephone and telephone-related services should e-mail the POC at the following e-mail address: armybasecom@conus.army.mil. If the existing consolidated contract cannot be used to satisfy the requirement, NETCOM/9th SC (A) will competitively award a new contract to satisfy the requirement. NETCOM/9th SC (A) will determine whether an existing consolidated contract will be modified or if a new contract is required to fulfill service requirements. (See DA Pam 25–1–1, chap 10.)

(3) *Work orders.* DOIMs will submit a DD Form 1367 (Commercial Communication Work Order) against an existing consolidated contract when acquiring telecommunications services for the installation. DOIM ordering officers, appointed by the NETCOM/9th SC (A) contracting officer, are authorized to place orders up to the dollar limit defined in their appointment orders. DOIMs will submit all orders over the DOIM ordering officer's threshold to the NETCOM/9th SC (A) contracting officer.

(4) *Wireless.* NETCOM/9th SC (A) (ESTA-TT) is the exclusive POC for procuring wireless services and devices such as cellular telephones, pagers, wireless data devices and related airtime service. When procuring wireless services and devices, all Army users are required to utilize the ordering procedures established by NETCOM/9th SC (A) and procure the services from established BPAs.

(5) *Central procurement.* In the event that a desired PDA or wireless service is not on the Army's BPAs, a request for exception to procure from other sources will be submitted to NETCOM/9th SC (A). The exception will be evaluated on a case-by-case basis and no action will be taken to procure the services from other sources until approved by NETCOM/9th SC (A). Use of the Army's BPAs will ensure the requirements are being fulfilled using the best available option for service and pricing.

d. Long distance calling.

(1) *Direct dial.* Callers will place long-distance telephone calls directly, without assistance from the post switchboard operator (that is, direct-dial capability), when telephone switching systems have either a call detail reporting capability or an automatic telephone number call data identification system.

(2) *Control and accounting.* The DOIM will ensure that callers at Army installations without either a call detail reporting capability or an automatic identification system will use a standardized control and accounting system with report capability to manage use of official telephone service.

(3) *Installation switch.* Installation switches will be programmed to utilize DSN as the primary network where available; otherwise, the most economic route will be selected.

(4) *DSN.* (See paragraph 6–4*a*(1), above.)

(5) *Networx.*(See paragraph 6–4*a*(2), above.)

(6) *Local procedures.* The installation commander will determine the local procedures for handling incoming official collect calls.

e. Verification of bills and payment for telephone services.

(1) *Verifying bills.* Federal statutes require certification of long-distance telephone calls as official before paying for them. The office of the installation DOIM has certification responsibility. The purpose of verification is to collect payment from those making unofficial calls. Per U.S. Comptroller General decision B-217996, (21 October 1985), DOIMs need not verify every call. Other procedures, such as statistical sampling or historical data, may be used to satisfy the statutory requirements if they provide a high degree of reliability or certainty that certified calls are official. The DOIM will establish local verification procedures for use when necessary to certify bills or categories of bills as official (for example, repetitive one-time service bills for installation, removal, or relocation of instruments). (See DA Pam 25–1–1, appendix C.)

(2) *Networx verification.* The DOIM will use judgment sampling to verify bills for Networx. The DOIM will credit the amount collected to the account that originally paid the bill. The GSA is the Government's contracting agency for Networx.

(3) *Billing and payment.* The TCO or other designated official will review telephone billing and usage (to include phone cards) monthly. Federal agencies must pay interest or late charges if they do not make payments by due dates. The receiving unit (addressees) must "date-stamp" all telephone bills immediately upon receipt. The DOIM will use the "date-stamp" to determine the payment due date when an invoice or contract does not show a due date.

f. Use of calling cards (includes prepaid and postpaid cards) and Government Emergency Telecommunication Services (GETS) cards.

(1) *Approval.* Installation commanders will approve the acquisition and use of telephone calling cards.

(2) *Accountability.* DOIMs (or designated IMOs) will establish and maintain accountability procedures for telephone calling cards.

(3) *Certification.* Telephone calling cardholders must sign a local certification that acknowledges receipt of the telephone calling card and warns against loss and fraudulent and unofficial use.

(4) *Misuse.* Individuals who misuse telephone calling cards are subject to disciplinary action.

g. Official telecommunications services in personal quarters of key personnel. Official voice (telephone), data (SIPRNet/NIPRNet), and video service is authorized for key personnel whose positions require immediate response and/or have a direct bearing on the timely execution of critical actions. Key personnel will be designated based on functional position and mission impact. Official service installed in quarters of key personnel will meet, as a minimum, the following conditions and arrangements:

(1) *Access to local exchange.* Official service will not have direct-dial access to the local commercial exchange system.

(2) *Access to DSN.* Direct-dial access to the DSN and Defense Telephone System is permitted. Official service in personal quarters will be class-marked for DSN and local on-post service only. All other services will be provided through the on-post switchboard operator (that is, Networx and commercial telephone exchange service will be routed through the local installation switchboard operator) or a local command operations center.

(3) *Restrictions.* Service will be restricted to the conduct of official Government business for C2 or tactical purposes.

(4) *Separation of official and personal use services.* Personnel selected for official telecommunications service in their on-post quarters must provide, at their own expense, any of these services for the conduct of personal, unofficial business. This separate service will be from the local commercial exchange or the Government-furnished exchange, if authorized for local use.

(5) *Spouse volunteer.* Installation commanders have the authority to install telephone lines and other necessary telecommunication equipment and pay for the installation charges for the equipment when a spouse or volunteer with "official volunteer status" (pursuant to 10 USC 1588(f)), works out of the home. For more information, see DA Pam 25–1–1, paragraph 7–3*b*.

(6) *Multiline instrument.* The use of multiline instruments or electronic key systems to terminate official and unofficial lines in approved on-post quarters is authorized. Government-owned voice, data, and video systems should be used when it provides the lowest cost to the Government. In calculating lowest cost, consider the costs of reworking cable, removing and replacing instruments or key systems, purchasing instruments or key systems, and so on, for current and future occupants.

(7) *Classified.* Access to classified networks will be reviewed in accordance with AR 25–2 and approved on a case-by-case basis. Access controls/procedures will be documented in writing.

h. Secure wired and wireless communications equipment. This term encompasses all of the devices used to secure telephone communications, to include, but not limited to: secure telephone unit (STU), secure telephone equipment (STE), secure cellular, and secure wireline terminals.

(1) *Equipment requirements.* Secure phone communication is critical to most agencies and units and should be used as needed to assure voice and data communications security. Secure wireless devices will communicate securely with any device that is Future Narrowband Digital Terminal-compatible, such as the secure wireline terminals and upgraded STU IIIs and STE. These secure devices may only be used for classified conversations or transmissions when the devices are loaded with an NSA-approved Type 1 key and only to the level designated by that key.

(2) *Use with standard telephone.* Secured wired and wireless devices can be used with standard telephone equipment, International Maritime Satellites (Inmarsat), PCs, and unclassified fax machines to provide security that is not present in those unsecured devices. Only NSA-approved secure wired and wireless devices will be used to encrypt data from portable computers when operating on any telephone network.

(3) *Secure key.* Secured wired and wireless devices are unclassified, controlled cryptographic items without the PIN/crypto ignition key (CIK) loaded or in place; however, with the PIN/CIK in place, the devices assume the level of the key and may not be left in unattended environments except for specific circumstances allowed by AR 380–40 (that is, approved vaults and SCI facilities). Secure wireless cellular devices will be procured via normal COMSEC channels. NETCOM/9th SC (A) will procure secure wireless service (coverage). Organizations may submit inquiries and requests to acquire secure wireless service to armybasecom@conus.army.mil.

(4) *Environment.* When talking at a classified/sensitive level, personnel will observe procedures required for secure environments, to include maintaining distance from uncleared individuals. The cognizant security authority should implement a common-sense approach to acoustic security concerns.

(5) *Notification.* Organizations conducting classified or unclassified operations will notify all attendees in advance of prohibitions or limitations on carrying such devices into the operational area.

i. Automated service attendant. DOIMs will establish and provide installation operator services either on a local installation basis or a centralized/regional basis. The types of services provided will be determined by each DOIM.

j. Telephone service charges. Charges for installation telephone services will be included in the assignment of charges for telephones services provided from Government-owned or commercially leased telephone systems.

k. Authorized telecommunications services. Telecommunications services authorized for specific installation activities are identified in appendix B. See paragraph 6–1*n* for policy regarding MH members.

l. Pay per use and unofficial telephones. Pay per use switched telephone service (coinless and coinbox) and other unofficial telecommunications are MWR functions. NAF contract procedures will be used, and contractor fee payments per these contracts will be paid to the NAFI. These services will be managed by MWR in accordance with ARs 215–1 and 215–4.

m. E-mail. Broadly defined, e-mail includes COTS e-mail systems and Web mail (see DA Pam 25–1–1, para 10–6).

(1) *Grammar and usage.* E-mail constitutes official business communications and will be constructed in a clear, concise, and effective manner. The text of an official e-mail must be free of errors in grammar, spelling, and usage in order to ensure its effectiveness and efficiency.

(2) *Subject line.* The subject line of an official e-mail should meaningfully and adequately identify the content or topic of the message.

(3) *Font style.* E-mail users will use font styles and sizes that enhance the reader's ability to read and understand the message. A font with a point size smaller than 10 or larger than 14 should be avoided. Refer to AR 25–50, paragraph 1–20, for appropriate font styles, sizes, and colors.

(4) *Abbreviations and Acronyms.* Write out all acronyms and abbreviations the first time used. Use standard abbreviations and acronyms in accordance with AR 25–52. Generally, use the standard rules for abbreviations found in AR 25–50.

(5) *Identification of POC and Office/Contractor status.*

(a) The POC of any type of correspondence will be identified by military rank or civilian prefix, name, office, telephone number, e-mail address, and fax number, if appropriate.

(b) In addition to (5)(*a*) above, contractor support personnel should clearly indicate their contractor status.

(6) *Etiquette.* When writing an e-mail, some common rules of etiquette apply—

(a) Refrain from using all capital letters in electronic correspondence.

(b) Maintain a professional tone in correspondence.

(c) Refrain from using "Reply All" when a reply to a specific individual or individuals is more appropriate.

(d) Refrain from misusing the priority mark. Mark an e-mail as "high priority" sparingly and only when there is an urgent need to give the marked message priority over routine message traffic.

(7) *Use of encryption.* E-mail requiring data integrity, message authenticity, or nonrepudiation of DOD sensitive information, other than personal information sent by information-privileged individuals, volunteers, or Reservists, will be signed using DOD-approved certificates. The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates. A DOD PKI encryption certificate will be used to sign and encrypt sensitive information for transmission via e-mail. Further, sensitive information transmitted in e-mail messages must be clearly labeled to show its sensitivity, such as "Sensitive - Privacy Act Information." Signature/encryption will be used to send information that is—

(a) Protected by the Privacy Act (5 USC 552a). (The Privacy Act includes protection of personally identifiable information.)

(b) Identified as FOUO.

(c) Protected under HIPAA. (See also paragraph 2–21*c* and References.)

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

(8) *Bandwidth usage.* DOIMs are required to develop local procedures on bandwidth usage and encourage processes to reduce bandwidth demand. The amount and type of control on bandwidth usage will depend upon the organization's mission. When using e-mail, the following bandwidth restrictions are in effect:

(a) Only mission-essential attachments will be transmitted. Users will utilize file compression tools for each attachment that exceeds five megabytes (MB). Users must limit the combined size of individual e-mail transmissions to 20 MB, including attachments and the total number of copies sent (for example, the number of recipients). Unnecessary embedded graphics are to be avoided, including avatars (personal symbols) and e-mail backgrounds.

(b) When internally staffing documents within an organization, place the documents in an internally accessible area on AKO/DKO Files, shared drives, or approved organizational intranets instead of sending documents via e-mail.

(c) When sharing documents external to an organization, place documents in the aggregate on AKO/DKO Files or on an approved organizational Web server and provide the link/uniform resource locator (URL) where the documents are located. DOIMs/IMOs will inform users that sending links/URLs is preferable to distributing documents by e-mail to a large number of people. Activities will use AKO/DKO and AKO-S portals as the primary tools for collaboration.

(9) *AKO/DKO registration.* Soldiers, civilians, and contractors who are authorized e-mail accounts are required to also have AKO/DKO Web mail. To register, log on to https://www.us.army.mil. Follow the instructions under "Register for AKO." SIPRNet users must also have AKO-S accounts. Army e-mail users will use their AKO/DKO Web mail address for all official business transactions and as their permanent e-mail address within all Army business processes or systems (that is, personnel, medical, payroll, legal, and other systems).

(10) *Use of official government e-mail service.* Only AKO/DKO Web mail or other Government-provided e-mail services (as designated by the local DOIM) are permitted. E-mail 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. The AKO/DKO Program Office, DOIMs, and IMOs of deployed units will ensure that the "auto-forward" default settings on AKO/DKO Web mail and local e-mail restrict individuals from automatically forwarding their e-mail messages to commercial (private) addresses. There is no prohibition for manually forwarding e-mail messages, one at a time, after opening and reading the content to ensure that the information is not sensitive or classified. Users will archive e-mail and dispose of non-record items on a routine basis.

(11) *E-mail administration.* Local e-mail procedures will provide for implementation of sound e-mail account management consistent with guidance in this regulation and other Army security guidance. DOIMs will establish local procedures to ensure that—

(a) System administrators are assigned and trained.

(b) System administrators establish office accounts to receive organizational correspondence. Office POCs will manage the office's organizational e-mail accounts and will minimize the number of users sharing the passwords for office accounts.

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

(d) Passwords are protected and stored to 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.

(12) *E-mail records.* Army policies for records management apply to e-mail traffic. Designated records managers (RM), records coordinators (RCs), and records custodians will monitor the application of records management procedures to e-mail records. E-mail backup storage is not considered "records archiving." Reference chapter 8 of this publication and AR 25–400–2 for more information on preserving e-mail communications as records.

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

(14) *Defense Management System.* Refer to paragraph 6–5*e* for policy on the DMS.

n. Use of the Internet (World Wide Web). Users of the Internet (World Wide Web (WWW)) are encouraged to make it their preferred and routine choice to access, develop, and exchange information. Access to the Internet is authorized according to the controls applied by the Web site owners. Refer to paragraph 6–7 below for policy on management of Army Web services.

o. Internet service providers. The only authorized access from Army computers, systems, and networks to the Internet is through a DISN-controlled and 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 (ISP). For exceptions, the organization must submit a waiver request for validation by the DOIM through chain of command to HQDA, CIO/G–6 (SAIS–AOI).

(1) *Exceptions to use commercial providers.* Army organizations may acquire commercial Internet service (for example, to provide e-mail service and Web access) for users that do not or cannot have access through an Army, DOD, or other Government gateway. However, these organizations will not have any NIPRNet connectivity. DOIM validation is required before any official access services can be obtained from an ISP. DOIMs will ensure the proposed network architecture complies with security requirements and makes efficient use of available bandwidth.

(2) *Unofficial service.* Internet connections for educational (off-duty or non-duty related) or unofficial MWR activities are permitted, but no computer, system, or network used for these purposes can be connected to the NIPRNet. Units in the field may obtain ISP service for these purposes (for example, for communicating with family support groups in the sustaining base) using unit funds established and managed per AR 215–1, chapter 5, section IV. Refer also to AR 215–4, which governs IT supplies and services acquired with NAF. These Internet connections will be coordinated through the DOIM with the NETCOM/9th SC (A) support office prior to connection.

(3) *Cost for unofficial service.* The cost to procure Internet access via an ISP is a communications cost under the appropriate IT budget line(s). Army funds will not be used to provide Internet access to Army housing or quarters unless sufficient justification exists, on a case-by-case basis (for example, key command personnel with a genuine need for service at any/all hours, and so on). Unofficial, free, or pay-for-use Internet access is to be managed by MWR in accordance with ARs 215–1 and 215–4.

(4) *Commercial ISP in quarters.* Nothing in this regulation precludes occupants in Army housing and quarters from obtaining commercial ISP services for their own personal use, provided the cost is borne by the occupant(s).

p. Video teleconferencing (VTC). This policy applies to all Army VTC activities and capabilities (including videophones, desktop, and PC-based devices). A VTC facility designated as a baseline service will be managed by the installation DOIM. The DOIM is responsible for establishing common-user VTC procedures and guidelines for the respective garrisons. The DOIM or other designee will approve all VTC systems. All items will meet the DOD Video Conferencing Profile (Federal Telecommunications Recommendation 1080B–2002 standards). Army activities will use contract vehicles managed centrally by the CHESS as the first source when acquiring VTC equipment and services. Refer to paragraph 6–2 for policy on waivers to the use of CHESS contracts. Funding for equipment and personnel to operate, maintain, and install VTC facilities is in accordance with the Army baseline service agreement. Also see DA

Pam 25–1–1, paragraph 10–8, for implementing procedures. The DOIM or other designee will approve all VTC systems, to include those VTC systems used for mission purposes.

(1) *VTC for intelligence.* All intelligence activities requiring SCI-secure VTC capability will use the Joint Worldwide Intelligence Communications System (JWICS) or an equivalent SCI VTC medium and will be managed by the Army intelligence organization where the JWICS is installed.

(2) *Fixed facility VTC.* VTC fixed (permanent) facilities, which cost over the Other Procurement, Army (OPA) threshold will be validated by the requesting DOIM, approved by the chain of command, prioritized by the respective commander, and funded by CIO/G–6. VTC investment items are DA-controlled with cost thresholds established by Congress.

(3) *DISN Video Services (DVS).* DISA provides the DVS global contract as the vehicle to enable a DVS network/system to interoperate multiple conferences with fixed systems, roll-about VTC equipment, and portable VTC terminals. Installations that require common-user conference facilities should utilize the DVS global program for its connectivity/interoperability features.

(4) *Budget submission for VTC.* DOIMs will plan for expense and investment VTC systems to meet their current and projected needs. Requirements for investment equipment will be developed and forwarded annually, along with the requirement identified in paragraph 6–4*p* above by each DOIM. This submission is the basis for establishing annual funding increments for system replacement. DOIMs will plan for expense and investment VTC equipment through installation resource management channels as part of their annual operating budget and for inclusion in the IMCOM POM submissions.

(5) *Investment VTC.* The VTC program provides for the annual identification, funding, and acquisition of requirements for COTS VTC investment (DA-controlled) equipment. Requirements will be collected annually via a memorandum during the first quarter of each FY for the next FY. As functional proponent for the VTC program, the CIO/G-6 establishes acquisition priority numbers for all investment VTC systems.

q. Communication monitoring and recording. Army policy permits communications monitoring or recording, provided that the information to be acquired is necessary for the accomplishment of the Army mission. Lawful monitoring and recording of Army telecommunications and IT systems will be conducted per applicable directive (that is, AR 380–53 and AR 25–2 for IS security monitoring; AR 190–53 for law enforcement purposes; AR 380-10 for electronic surveillance, and DODI 8560.01 for COMSEC). Monitoring includes, but is not limited to, active attacks by authorized entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information placed on or sent over DOD computer systems, may be monitored. E-mail, personal user files and directories, and any use of the Internet or records created by Internet use are subject to monitoring, inspection, and audit by command or agency management or its representatives at any time, with or without notice. Use of the DOD computer system indicates that the user consents to monitoring and understands that the command or agency has a right to inspect and audit all information, including e-mail communications and records created by Internet use.

r. Telephone/IS directory. Each DOIM is responsible for maintaining a telephone/IS directory that provides local organizations' telephone numbers.

(1) *Publishing directories.* Each Army installation will publish an organizational telephone/IS directory at least annually (see DA Pam 25–1–1, para 7–9). The names of individuals will be included only by exception determined by the local public affairs officer (PAO). When the telephone exchange serves several installations, the main installation publishes the directory and includes listing for the sub-installations. Installations may publish directories separately, as a subsection of the local community telephone directory (published by the local telephone company) or as a subsection of a local installation guide (published by public affairs office). Combination local telephone directories and post directories or installation guides and installation directories may contain commercial advertising separate from the directory section. Electronic versions of the directory will be placed on that community's page on AKO/DKO or AKO-S, as appropriate, but not on the Internet. Every effort will be made to publish e-directories and avoid printing and distribution costs. (See also paragraph 6–4*n*, above.)

(2) *Releasing telephone/IS directories to the public.* All installation directories will be unclassified. Installation telephone/IS directories (organizational only) may be released to contractors through the Government procuring or administrative contracting officer. Under no circumstances will directories containing names, home addresses, and telephone numbers be released to the public or placed on any Web site without access controls and prior approval of the organization's Privacy Act official. Approval from the organization's Privacy Act official and security official are required prior to posting personal information on AKO/DKO or other private Web site. If posted on AKO/DKO, the information will be further restricted to those individuals with a need-to-know.

(3) *The AKO/DKO Community Pages.* The AKO/DKO Community Pages will be utilized for publishing directories containing individuals' names and office information. AKO/DKO White Pages are the primary tool for individual locator information.

s. Commercial television service. Commercial television service (satellite, cable, and broadband services) provide television programs through a distribution system to standard television or radio receivers of subscribers who pay for such service.

(1) *NAFI authority.* Facilities that provide commercial television service are commercially owned and operated. The installation commander is the franchising authority. When appropriate, the installation commander may designate a NAFI to be the franchising authority. Overall staff management of commercial television service is the responsibility of the ACSIM/FMWRC at the Army level and will be executed at the local level at the discretion of the installation commander.

(2) *Franchise.* Commercial television service is primarily intended for the use and enjoyment of personnel occupying quarters (barracks rooms, temporary lodging facilities, and Family housing) on military installations and in this regard should be considered the equivalent in purpose to MWR activities. DOD installations are commercial television service franchising authorities for the purpose of the applicable commercial television service laws. As a result, installations may issue a franchise, which grants a commercial television service company access to the installation and designated rights-of-way to permit the commercial television service company to serve its subscribers. The individual subscriber to the commercial television service contracts directly with the commercial television service company for unofficial service and is responsible for payment of subscription fees and no APF are involved. Provisions of the Federal Acquisition Regulation (FAR) are applicable only when a DOD component subscribes to commercial television service for official DOD business and APF are utilized for payment of subscriber fees.

(3) *Use of Appropriated Fund(s).* The provisions of the FAR are applicable to obtaining services when an Army activity subscribes for official DOD business and APF are utilized for payment of subscribers' fees.

(4) *DOIM validation.* DOIM validation is required before any official services can be obtained.

(5) Provisions of AR 215–4 are applicable to obtaining services when an official transient lodging activity provides these services and NAF are used.

(6) *Non-exclusive franchises.* Army policy is to provide for non-exclusive franchises only. A franchising authority may not grant an exclusive franchise and may not unreasonably refuse to award additional franchises. The award of a franchise is not a procurement by the Army and is not governed by the FAR. The franchise agreement must not obligate the Army to procure commercial television services for official purposes. If services are to be procured using APF, they will be procured by contract in accordance with the FAR and its supplements.

(7) Use of Appropriated Fund(s). APF available for morale and welfare purposes may be spent for user and connection fees for services to APF activities that serve the community as a whole per AR 215–1. Examples of these activities are hospital patient lounges and barracks day rooms. (Refer to appendix B for additional guidance.)

(8) *Subscription.* No Army member will be coerced to subscribe to a franchisee's services.

(9) *Programming.* Installations will not use government funds or personnel to produce free programming solely for the benefit of a commercial television service company.

(10) *Installation channels.* The Army will require that the commercial television service franchisee reserve on-installation channel(s) for use by the installation. This channel(s) will be provided at no cost to the Government. The channel(s) reserved for Government use need not be activated at the same time as the rest of the commercial television service system. The channel(s) may be activated at any subsequent time at the option of the Government. When the channel(s) is activated, the following restrictions apply:

(a) Official programming. The Army must avoid both the fact and the appearance of underwriting a commercial television service system.

(b) Advertising. Program materials for use on command information stations will not contain commercial advertising or announcements.

(c) Non-Army use. During the periods of Government use, the reserved command channels may not be broadcast off-installation to non-Army subscribers.

(d) On-installation programming support. The installation PAO will support installation programming by providing advice, assistance, and command information materials and topics.

(e) Operational control. The PAO will have operational control of the reserved command channels.

(f) Official programming. Official programming is generated from installation VI activities. The provisions of AR 360–1 address requests to use closed circuit television (CCTV), commercial television service, or other systems for internal public affairs purposes.

(11) *NAF activities.* The expenditure of APF to expand Government-owned commercial television services to provide entertainment television service to NAF activities or individual persons is not authorized unless such expenditures are justified under provisions of AR 215–1.

t. Global Broadcast Service (GBS). GBS provides a command-responsive, continuous, high data-rate stream of video, data, imagery, and other information broadcast via satellites to deployed, on the move or garrisoned forces worldwide. Although a primary purpose of the GBS is to serve the needs of C2 and intelligence dissemination, the GBS also serves to deliver training and MWR information services. Such services include the Armed Forces Radio and Television Service (AFRTS), commercial cable news/weather services and other desired broadcast services for deployed units. User reception of broadcast information will be through issued GBS receiver terminals.

u. Portable, mobile, cellular, and wireless telephones and devices.

(1) *Requirements.* These types of telephones will not be used in lieu of established "wired" telephones. These devices are to be used for official business and authorized use only and may be approved for handheld portable use

and/or installed in Government vehicles. Official use of these phones will be limited to requirements that cannot be satisfied by other available telecommunications methods and are authorized when warranted by mission requirements, technical limitation, feasibility, or cost considerations. Authorized personal use of cellular phones is subject to the same restrictions and prohibitions that apply to other communications systems. (See paragraph 6–1*e* for authorized use.)

(2) *Examples.* Examples of appropriate applications for these telephones are as follows:

(a) Emergency management and emergency restoration situations.

(b) Specifically designated projects and/or mission-unique requirement (for example, work being performed in geographically remote areas, or work where continuous communication is required).

(c) Safety of personnel, unit, or organization security.

(d) Fly-Away or Drive-Away kits/sets for contingency purposes.

(3) *Cellular telephone vulnerabilities.* Cellular telephones are useful during emergencies but should not be considered the primary or total solution to emergency communications requirements due to inherent vulnerabilities and limitations of cellular technology. Examples of such vulnerabilities are as follows:

(a) Damage to or displacement of cells (that is, the actual broadcast/rebroadcast towers and systems that are the enabling support for this technology).

(b) Cellular system overload and/or overloading of the Public Switched Network.

(c) Geographic limitations on areas served and signal strength.

(d) Unless encrypted, provide no privacy or security and are easily monitored by third parties.

(4) *Local policies.* Commanders will develop procedures for all subordinate organizations to implement policy on acquiring and using cellular phones. Justification of need will be included in requesting documentation. Activities will establish a reutilization program to identify and turn in cellular phones that are no longer or seldom used. All devices will be managed as accountable items. Vendor cellular phone plans will be reviewed quarterly to identify and switch to plans that cover the organization's needs at the lowest overall cost. Installation DOIMs will procure all wireless services through NETCOM/9th SC (A). Refer to paragraph 6–4*c* for central procurement policy for wireless devices and services.

(5) *Audits.* The DOIM will implement software audit procedures that trigger immediate reviews of cellular telephone usage and notification by the vendor when notable spikes in calling occur. Notable spikes are a prime indicator that cellular telephone integrity has been compromised.

(6) *Data adapters.* Cellular telephones may be used with Personal Computer Memory Card International Association data adapters to greatly enhance the ability of remote or mobile users to pass data files to/from home stations. These adapters do not provide any security or encryption.

(7) *Security.* DOIMs will educate cellular telephone users in policies and procedures to prevent security violations and inappropriate use.

(8) *PIN numbers.* Organizations must require PIN numbers for user log-in to cellular phones to prevent unauthorized use.

(9) *Lost cellular phones.* Users should immediately report stolen or missing cellular phones to the DOIM office so that service can be canceled or suspended to prevent illegal use/charges.

(10) *Usage.* The following are examples of practices to avoid:

(a) Automatically forwarding office and residence phone calls to government cellular phone numbers.

(b) Automatically forwarding cellular phone calls to office or residence phone numbers.

(c) Using a cell phone while operating a vehicle on a military installation unless a hands-free device is used (exceptions include emergency responders). Other cell phone usage restrictions may apply under state law in the U.S. or under foreign national laws in OCONUS.

(d) Using cellular phones in geographic areas outside of the area of service coverage and where usage incurs roaming charges. If in doubt, check with the local DOIM before making any phone calls.

(11) Sensitive transmissions. All wireless communications devices that are used to transmit sensitive information must be encrypted when connected to the installation network in accordance with AR 25–2.

v. Secure cell systems. Tactical units in a deployed environment will use only the Army's encrypted secure cell systems.

w. Beepers, pagers, and PDAs. When beeper/pager functions are part of the features of a cellular telephone or PDA, the item will be managed the same as a cellular telephone. (See para 6-4u, above.) All Army organizations will use NETCOM/9th SC (A) BPAs established to provide economies of scale. The scope of beepers/pagers service will be authorized based upon geographic service areas.

x. Integrated equipment. Information managers will proactively seek solutions, such as integrated fax servers, that maximize service to customers while minimizing costs. Efforts should be made in conjunction with users to reduce or eliminate the need for hard copy materials. Unclassified fax machines can send secure faxes when used with STU/STE devices to encrypt transmissions, up to the security level for which the STU/STE is keyed.

y. Army management of electromagnetic spectrum. AR 5–12 governs Armywide spectrum management. The CIO/

G–6 designates the Army Spectrum Manager, responsible for promulgating spectrum policy and planning guidance for Army operations, training, and acquisition.

z. Radio System Support Services.

(1) *Installation requirements.* Requirements for entry into existing networks will be identified to the installation DOIM. Installation radio system support comprises nontactical, user-operated, radio-networks, systems, facilities, equipment, and information services required to support host and tenant activities at the installation level.

(2) *Usage.* Installation radio systems support services consist of fixed, trunked, mobile, and portable radio systems. Installation radio system support services are authorized when existing ISs cannot satisfy mission essential requirements. Requirements for installation radio support system services will be justified based upon operational necessities and an economic analysis. COTS equipment available on Army-negotiated contracts will be utilized unless otherwise justified. Availability of radio frequency assignment will be assured before procurement action is started. All installation information radio operations will be established and maintained in accordance with the security requirements of AR 25–2.

(3) *MARS.* The MARS provides DOD-sponsored emergency communications on a local, national, or international basis as an adjunct to normal communications. The Army MARS program is addressed in AR 25–6. Commanders and agency heads will support and encourage MARS and amateur radio activities and avoid, within the limitations imposed by military exigencies, any action that would tend to jeopardize the independent prerogatives of the individual amateur radio operator.

aa. Leasing of Government-owned telecommunications assets.

(1) *Outside plant facilities.* If requested, Government-owned outside plant telephone facilities, inside plant telephone facilities, or antenna space may be leased to commercial telephone/radio companies in accordance with the provisions of this regulation, AR 700–131, and applicable installation memorandum of understanding. Outside plant facilities, inside plant facilities, and antennas are classified as IT equipment and accounted for as such. Outside plant facilities include installed or in-place telephone cable (copper and fiber optic) and their associated connecting terminals, telephone poles, manholes, and duct bank systems. Inside plant facilities include installed or in-place telephone frames, switches, electronic equipment, multiplexes, and fiber optic electronic equipment.

(2) *Lease to vendors.* The leasing of plant facilities to vendors is permitted and encouraged. Leasebacks provide a means for the installations to cover the maintenance and repair of cable plant facilities. Leasing of telecommunications facility assets requires a formal lease agreement. The DOIM is required to maintain a current inventory of cable plant facilities leased to vendors.

(3) *Compensation.* Compensation paid by telephone companies for lease of any Government-owned APF facilities (cable pair, equipment, manholes, antenna space, and so on) will be in the form of a credit toward the existing monthly bill when possible (also referred to as "payment-in-kind"). If a credit to the existing monthly bill is not possible, a check can be accepted. In accordance with 10 USC 2667, checks will be made payable to the U.S. Treasury under receipt account 97R5189, Lease of DOD Real Property for Army, to be redistributed to the leasing organization via DA. Terms of the reciprocal lease agreement will provide that the Government may, according to its needs, reacquire any leased asset.

(4) *NAF revenue.* The revenue from the lease of NAF telecommunications assets will be deposited into the NAF activity's fund.

(5) *Shared usage.* When leasing telecommunications services, the leasing activity will make every effort to lease in the name of the U.S. Government to permit the shared use of communications services, facilities, or installations among U.S. Federal departments and agencies.

(6) *OCONUS leases.* OCONUS leasing activities will follow this practice in negotiating for new or revised existing services or facility leases, and negotiating new or renegotiating existing status of forces, base rights, or other intergovernmental agreements, unless notified that the Secretary of State has determined such action inconsistent with foreign policy objectives of the United States.

bb. Wireless Priority Service (WPS) and Wireline GETS. WPS and GETS provide an end-to-end nationwide wireless and wireline priority communications capability to key national security and emergency preparedness personnel during natural or man-made disasters or emergencies that cause congestion or network outages in the Public Switch Network (PSN). WPS and GETS are complementary to each other to ensure a high probability of call completions in both the wireless and wireline portions of the PSN. WPS is a service added to the wireless phone after the phone has been issued to the user. Requests for WPS service must be submitted to the DOIM or the local GETS/WPS program manager. The DOIM or the GETS/WPS program manager will submit the request for WPS service to the NCS who will assign the authorization to the wireless number.

cc. Land Mobile Radios (LMR) (non-tactical).

(1) *Usage.* LMR systems (non-tactical) provide wireless communications in support of the force protection, homeland security, and installation management mission of posts, camps, and stations (see also DA Pam 25–1–1, para 10–10).

(2) *DOIM as operator.* The installation DOIM is the single provider and operator of all LMR capabilities, as

approved by the CIO/G-6, at Army installations. LMR systems that are not operated by the DOIM are prohibited unless an exception is approved by the respective garrison-owning command.

(3) *Memorandums of Understanding.* MOUs that describe operational roles and responsibilities for all LMR services shared between the installation and outside agencies or other installations are required. A separate MOU will be developed and approved by the respective garrison and each outside agency or installation.

(4) *Resourcing.* The CIO/G–6 will notify Army installations of requirements for compliance with domestic and international laws regulating LMR usage. Installation DOIMs will identify all resource requirements for achieving compliance to their respective RCIO. The RCIOs will in-turn identify regional priorities for LMR investments to the CIO/G–6 based on the level of risk to the installation of non-compliance with these laws.

(5) *Frequency assignments.* Installations will coordinate individual migrations of frequency assignments through the supporting area frequency coordinator, with the Army Spectrum Management Office (ASMO). The ASMO, in turn, will coordinate these frequency assignments with DOD components and other Federal departments and agencies under current NTIA policy and procedures to minimize mutual interference and retain system integrity.

(6) *Waivers.* Requests for waivers for spectrum policies must be submitted to the ASMO. Requestors should contact the ASMO for additional technical guidance.

dd. VoIP and Voice over Secure IP (VoSIP). Organizations that have a requirement to use VoIP or VoSIP to perform their missions will implement solutions in accordance with DODl 8100.3 and CJCSI 6215.01. Organizations must use only authorized products listed on the JITC Web site: http://jitc.fhu.disa.mil/. This requirement applies to both VolP equipment and the associated local area network. Organizations with a requirement to implement VolP must first submit their request through the local installation DOIM. The request will then be processed through the appropriate RCIO and forwarded to the CIOIG–6, ATTN: SAIS–AOI for approval. Organizations not located on an installation with a DOIM will forward their requirement to the appropriate RCIO. The package submitted to CIO/G–6 must include a cost or operational benefit analysis of the proposed implementation, which reflects a benefit either in monetary terms or enhanced capability. VolP solutions that require a waiver to the CJCSl 6215.01 will be forwarded through ClO/G–6 to Joint Staff for final approval.

ee. Unofficial and pay-per-use Internet access and services offered on post. Unofficial and pay-per-use Internet access and services are MWR functions. When pay-per-use unofficial Internet services (for example, barracks Internet services or wireless hot-spot service) are to be provided, 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, Voice over IP, unofficial e-mail, video mail, and streaming audio/video. Paid and free unofficial Internet access and services are identified in AR 215–1. Access to DOIM 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 US 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 local national specifications when installed. When requested by MWR, DOIM frequency managers will direct that other unofficial users of these frequencies be terminated if it interferes with approved MWR implementation at the same frequency.

6–5. Long-haul and deployable communications

Long-haul telecommunications are defined in DODD 4640.13. This section provides Army policies on the use of long-haul communications, wide area networks, and deployable communications. (See DA Pam 25–1–1, para 10–7.)

a. DISN. DISN is DOD's integrated worldwide enterprise-level network for exchanging secure and non-secure data, voice, and video information.

(1) *Requirements.* All Army long-haul customers will use DISN service to satisfy Army long-haul and wide-area network transfer communications requirements. Requirements will be processed per DISA Circular (DISAC) 310–130–1 and the supporting Army activity's procedures. The policies above state that all long-haul telecommunications services shall be planned, designed, implemented, managed, and acquired by DISA. All requests for long haul service should be submitted directly to NETCOM/9th SC (A) NETC–EST-TT in order for NETCOM to complete the order through the DISA Direct Order Entry (DDOE) system. DISA is designated as the only entity authorized to order telecommunication services from Networx contracts for the Army. Army activities will continually assess the impact of mission and operational concepts on their long-haul communications requirements. DOIMs will validate operational requirements before requesting connection approval from NETCOM/9th SC (A) to ensure DISN is the best solution for the requirements by considering the bandwidth, security, connectivity, and other technical issues. DOIMs will ensure voice switching hardware and software are on the APL found at http://jitc.fhu.disa.mil/tssi/apl.html before procuring these items.

(2) *Responsibilities.* Commands, RCIOs, and other Army activities will—

(a) Review long-haul common-user transmission requirements and forward all requirements not needing combatant command, Joint Staff, or OSD approval to NETCOM/9th SC (A) for development of a technical solution, coordination, and implementation. Per DISA's criteria, systems requirements must be identified far enough in advance to ensure a timely acquisition of network components to satisfy the operational date.

(b) Review and submit, as delegated by the supported combatant commander, requirements for service with the information prescribed in DISAC 310–130–1.

(c) Program, budget, fund, and provide support for assigned portions of the DISN through the PPBE process, including approved contractor and foreign government systems.

(d) Provide sufficient local distribution capability to meet the combatant commanders' validated connectivity requirements. These systems must be capable of supporting the operational requirements of the Army as well as Joint task force contingencies.

(e) Ensure that information security, communications security, TEMPEST, physical security measures, and installation requirements conform to the Army and DISN security policy.

(f) Ensure that approved systems use DISN services to meet mission requirements and ensure compliance with the Army and DISN policy and procedures.

(g) Coordinate with the theater commander and DISA before submitting long-range requirements for DISN access within a geographic region of responsibility of a theater command. Conflicting views among the requesting activity, DISA, and the concerned combatant commander will be forwarded to the J–6, Joint Staff, for resolution.

(h) Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits per DISA's criteria and provide representatives, as required, to Joint- or DISA-chaired working groups on related topics.

(i) Provide requisite site support for DISN equipment located on their respective posts, installations, or the equivalent. Site support requirements will be specified by DISA in appropriate procedural documentation and coordinated with the services and defense agencies. Support required will include, but is not limited to, providing power, physical security, floor space, and on-site coordination for the DISN data networks points of presence located on their respective posts, installations, or equivalent.

(j) Manage DISN subnetworks when authorized by the Director, J–6, Joint Staff.

b. DSN. DSN is the DOD preferred means of providing voice communications for C2 in accordance with CJCSI 6215.01. DSN may be used to transmit unclassified facsimile traffic.

c. DRSN services—

(1) *Overall requirements.* The combatant commanders and Defense agencies coordinate the overall Joint requirements for DRSN services per CJCSI 6215.01. Army commanders are responsible for their designated portions of the DRSN. This may include, but is not limited to, providing O&M funds for the DRSN logistics support, sustainment, training, DRSN-related equipment, and special interface trunks required by the combatant command or supported command for which they are responsible.

(2) *Unique requirements.* Unique requirements will be forwarded through the Army command to HQDA, CIO/G–6, ATTN: SAIS–AOC, for coordination and validation. Guidance for submitting DRSN requests can be found in enclosure E of CJCSI 6215.01.

(3) *Certification.* Servicing Army commands will certify that funds are or are not available as part of the DRSN approval request. The funding review and forecast for certification will be coordinated through the chain of command to the CIO/G–6 prior to approval.

d. Networx. Networx is the preferred network for administrative long-distance voice communications (see para 6–4*a*).

e. Defense Messaging System (DMS).

(1) *Usage.* The DMS has been designated as the DOD record messaging system. The DMS may be implemented in all environments. Organizational messaging is defined as correspondence that is used to conduct the official business of the Army. As an organizational message system, DMS may be used to commit resources, direct action, clarify official positions, or issue official guidance. DMS migration will be accomplished through centralized fielding by the Army DMS PM. (See also DA PAM 25–1–1, paragraph 10–6*b*.)

(2) *Message size.* Attachments to DMS messages are limited to the maximum size specified in Allied Communication Publication (ACP) 123(A).

(3) *Privacy communications.* For information on the Privacy Communication System messaging, refer to ACP 127 US Suppl–1 (J), Communication Instructions Tape Relay Procedures http://www.jcs.mil/j6/cceb/acps/ACP127USSUP-P1J.pdf; and Defense Message System GENSER Security Markings Implementation Manual, which can be obtained through the DMS Asset Distribution System (https://dkwwwefgv001.roscc1.disa.mil/).

f. JCS-controlled mobile/transportable communications assets. JCS maintains control of mobile/transportable communications equipment and ensures it is kept in readiness for worldwide emergency/contingency communications for the operational and support needs of the JCS. All Army commands with requirements for JCS-controlled assets will submit requests in accordance with CJCSI 6110.01, Enclosure B.

g. Military telecommunications agreements.

(1) *International agreements.* Army activities will adhere to U.S.-ratified international standardization agreements (including NATO standardization agreements and ABCA Quadripartite standardization agreements) when designing or procuring telecommunications equipment. Exceptions may be requested through CIO/G–6 (SAIS–AOC) when unique

Army specifications are a major impediment to adoption of an otherwise cost-effective allied system. Army CIO/G–6 is the voting representative to the SATCOM Interoperability Standards Committee in support of NATO.

(2) *NATO communications.* Army activities will carry out assigned responsibilities contained in formally consummated memoranda of understanding or similar documents between the U.S. Government, NATO, and NATO nations, to include formal U.S. commitments made in support of NATO and NATO member communications plans, programs, and policy.

(3) *NATO facilities.* Whenever the Army requires telecommunications facilities, the available telecommunications facilities of NATO or member nations will be used to the maximum extent feasible, provided reliable communications for use can be assured and that such use is cost effective.

(4) *Unilateral communications.* When NATO and NATO member communications are nonexistent, inadequate, or not cost-effective for use, the U.S. will provide unilateral communications. These are wholly owned, operated, and maintained by the U.S. Government, or U.S. commercial enterprises, or a combination thereof, and will be used by the U.S. to provide minimum essential unilateral control of the U.S. forces and to complement NATO and NATO member nation communications.

(5) *Interoperability.* Interoperability will be achieved on a planned, step-by-step basis and efforts toward consolidated, collocated, interconnected, and interoperable systems will result in mutually supportive U.S., NATO, and NATO member-systems that satisfy NATO, other NATO members, and U.S. requirements.

h. Compatibility and interoperability of tactical C3I systems.

(1) *Tactical C3I.* The Army will develop, acquire, and deploy tactical C3I systems that meet operational needs of U.S. tactical forces and are interoperable with allied tactical and non-tactical C3I systems, including systems used in support of civil authorities.

(2) *Requirements.* The coordination and validation of requirements, to include required joint coordination, will be accomplished per AR 70–1 and AR 71–9.

(3) *Interfaces.* For the interfaces between tactical and non-tactical C3I systems that support joint or combined operations, the J–2, Joint Staff, assists in making defense intelligence communication acquisition requirements support military forces and in achieving joint and multinational interoperability. Intelligence warfighting requirements are examined for solutions and ensure compliance with DODDs and joint directives.

(4) *Joint approval.* The J–6, JS, is the approval authority for joint or combined communications system prior to initiation of system development. Established joint interface standards and operational procedures are standard practices for tactical Army C3I systems. Requirements for new Army-funded joint or combined tactical C3I systems will be validated by the CIO/G–6 prior to forwarding to the J–6, Joint Staff.

(5) *NATO agreements.* The basis for U.S. and Allied compatibility and interoperability of tactical C3I systems will be those agreements between the U.S., NATO countries or alliances as specified in requirements documents, and Allied standardization agreements.

(6) *Interoperability testing.* Interoperability testing and evaluation (T&E) of tactical C3I systems will be performed during the acquisition process. T&E will be conducted throughout the acquisition process via established system benchmarking or demonstrations to reduce acquisition risks and to estimate operational effectiveness and suitability of the system. Critical capabilities, test objectives, and evaluation criteria related to mission requirements will be established at the beginning of the acquisition process. Functional proponents and MATDEVs will use performance measurements to ascertain performance and results-based management of C3I systems. Refer to paragraph 3–8 of this publication and AR 73–1 for policy on interoperability testing.

i. Reduction and control of information during emergencies (MINIMIZE).

(1) *Worldwide MINIMIZE.* The authority to impose MINIMIZE worldwide and within a specified area is limited to the JCS. The JCS will release general instructions to all U.S. military activities concerned. There is no requirement for separate additional notifications.

(2) *MINIMIZE authority.* Authority to impose MINIMIZE is prescribed in the Allied Communications Publications 121 (G) Communication Instructions-General section IV. Policy concerning MINIMIZE is contained in chapter 3, Section VII, ACP 121, US Supplement 1.

(a) Authority to impose MINIMIZE is inherent in command and, therefore, is not limited unless denied by appropriate higher authority.

(b) MINIMIZE is normally confined to the command controlled by the imposing authority. If the need for reduction and control of messages originated outside of, but flowing into or through, the affected area is apparent or when it becomes apparent, assistance shall be requested through command channels from the command authorized to effect the required reduction and control. Until such assistance has been requested of and directed by the appropriate authority, communications and communications systems controlled by other than the initial imposing authority shall not be affected.

(3) *Continental United States (CONUS) MINIMIZE.* CONUS is a single area of command responsibility under the jurisdiction of the JCS.

(4) *Command MINIMIZE.* ACOMs and ASCCs are authorized to take the following actions:

(a) Impose MINIMIZE upon all or part of their respective areas of command responsibility.

(b) Impose MINIMIZE by releasing the appropriate general instructions to all concerned military activities and information transfer facilities.

(c) Request that the JCS or other commanders impose MINIMIZE on users in other areas originating traffic destined for addressees in their area of command responsibility.

(5) *Army Command and Army Service Component Command Minimize.*Army Command and Army Service Component Command commanders that impose MINIMIZE on originators of traffic destined for addressees within their areas of command responsibility will forward their recommendations for MINIMIZE and substantiating justification to the commander of the area in which they are located.

(6) *Subordinate command MINIMIZE.* Major subordinate commanders and installation commanders may also impose MINIMIZE when it is necessary to reduce the flow of information within their respective areas of responsibility. Local notification procedures will be established to inform users within the affected command of the imposition of MINIMIZE.

(7) *Justification.* When the imposition of MINIMIZE will affect users outside the command's area of responsibility, such as reducing the flow of information into the area, a request to impose MINIMIZE on a wider basis will be forwarded, through the chain of command, to the CIO/G–6 (SAIS–AOC). Substantiating justification will accompany the request.

(8) *Notification.* Army commanders will notify the commander of the unified or combatant command in which they are located when MINIMIZE is imposed on originators of traffic destined for addressees within their area of responsibility. Justification for the MINIMIZE will be provided.

(9) *Local procedures.* Army commands will establish procedures for notification of MINIMIZE for all organizations affected by the order.

6–6. Satellite communications systems

a. General. SATCOM includes those systems owned or leased and operated by the DOD that communicate to and/or receive communications from spacecraft and those commercial SATCOM services used by the DOD. SATCOM systems are an integral part of the DOD command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structure that includes the C4ISR architectures and systems of the combatant commands (COCOMs) and Defense agencies. Army SATCOM terminal systems include military-developed and acquired terminal systems (including Army-owned COTS terminals such as Inmarsat terminals and Iridium and SECTERA handsets). SATCOM systems are considered a constrained resource of the DOD. Access to SATCOM systems is based on JS-validated and prioritized requirements and approved priorities for day-to-day operations for the execution of operational plans and is directed by the JS and National Command Authority. (See also DA Pam 25–1–1, paragraph 10–9*c*.)

b. SATCOM requirements. The CJCSI 6250.01 establishes operational policy and procedures and provides guidance for the planning, management, employment, and use of SATCOM systems. The space segments of all SATCOM systems are controlled as joint assets to meet JS-approved requirements. Units must complete a Satellite Database (SDB) requirement in order to gain access to equipment and services of a SATCOM system. Units will submit the SDB requirement application via the telecommunications management system classified SATCOM toolkit or through the DISA Form 772. JS certification, through the JITC, of compliance with approved SATCOM technical standards is required before access to the space segment will be granted. Requirements for SATCOM connectivity and requests for access to a SATCOM system will be submitted per guidance in CJCSI 6250.01. Access is predicated on having a JS-approved requirement.

(1) *PPBE.* Army is assigned PPBE process responsibility for the payload and network control systems of the MILSATCOM System, the Wideband Global SATCOM (WGS), and the Advanced Wideband System/Transformational Communications architecture.

(2) *SATCOM earth terminals.* Army is designated as lead military department for the development and acquisition of ground SATCOM earth terminals (less Military Strategic and Tactical Relay System ground command post and GBS Primary Injection Point terminals).

(3) *Service requests.* All Army components requiring SATCOM service from DISA will submit a TR through DDOE. If the service cannot be provided by DISA, an OSD waiver is required to obtain the service from a vendor. Army activities requesting OSD waivers will submit them through NETCOM/9th SC (A)/ESTA.

c. Use of wideband MILSATCOM. The Army will procure and field only single and multi-band-capable wideband satellite systems with at least one of those bands being a wideband MILSATCOM frequency band (that is, X or Ka band).

(1) *Upgrading.* In addition, all fielded wideband satellite terminal systems will be required to upgrade to be capable of operating over MILSATCOM as soon as fiscally possible, but not later than 2012 when WGS achieves worldwide coverage. This will ensure the Army can take advantage of the capability provided by the WGS and reduce commercial transponder leasing costs.

(2) *Exceptions.* Exceptions to the use of wideband frequency bands will be considered on a case-by-case basis. Justifications for exceptions to policy will be included in the Operation Needs Statement and DD Form 1494 (Application for Equipment Frequency Allocation) submissions (see DA Pam 25–1–1, para 10–9*e*, for procedures).

(3) *Other SATCOM services.* This wideband MILSATCOM requirement does not include Army Combat Service Support SATCOM and Intelligence systems, as those systems are scheduled to migrate to the Warfighter Information Network-Tactical as the Army's objective network.

d. SATCOM standardization. Organizations requiring SATCOM communications must comply with Strategic Directive (SD) 714–1, which standardizes and consolidates Joint operations, management and control policies, processes, and procedures for the DOD gateways.

(1) *Requirement approval.* An SDB requirement must be completed and validated by the COCOM J3/J6 for approval by the JCS Joint SATCOM Panel. The process to accomplish this task is outlined in CJCSI 6250.01 and applies to all Defense Satellite Communications System (DSCS) and Commercial SATCOM requirements.

(2) *Validation.* Once an approved SDB is received for a DSCS super high frequency mission, the unit submits a terminal request with the SDB number, POC, and funding documentation through the COCOM J3 to USSTRATCOM J61, Offutt Air Force Base, Nebraska, for validation.

(3) *Engineer analysis.* USSTRATCOM will in-turn forward the request to DSCS Washington (Wash) which conducts an engineering analysis to determine the type of terminal required to support the mission or advises if there are adequate resources to support the mission.

(4) *Terminal request.* Upon DSCS Wash/USSTRATCOM validation, the terminal request will be forwarded to the JS J6Z. J6Z will forward the requirement to HQDA (DCS, G–3/5/7, CIO/G–6, and DCS, G–8) and the Services under a Joint Staffing Action (JSA) for their concurrence/non-concurrence. Upon receipt of JSA validation, the JS will approve.

e. NETCOM/9th SC (A) operations of MILSATCOM systems. NETCOM/9th SC (A) operates and maintains designated strategic MILSATCOM systems and terminals, the direct communications link, teleport systems and terminals, and fixed regional hub nodes.

f. Handheld and mobile/transportable satellite terminal equipment. Handheld and mobile satellite terminals are non-tactical transmission terminals that require satellite spectrum use approval and have a billed cost associated with transmission time.

g. International Maritime Satellite (Inmarsat). This technology is a commercial international satellite system, which provides global transportable SATCOM for commercial, emergency, and safety applications on land, at sea, and in the air. The use of Inmarsat terminals in any theater of operation will be guided by the policy of the theater combatant commanders. Primary C2 communications should be conducted via DISA/Joint/Combatant Commander/Army networks and devices, with Inmarsat filling voids when primary communications providers are not available and the transmission of such information is unclassified or appropriately protected to the level of the data sensitivity. Inmarsat must be used with a STU III, STE, or other NSA-approved device. (See DA Pam 25–1–1, paragraph 10–9*a*).

(1) *Broadband usage.* Inmarsat has launched a new generation of satellites, Inmarsat 4 (I–4), that offer a Broadband Global Area Network (BGAN). With light-weight terminals and higher data rates up to half a Megabit per second, I–4/BGAN will allow users to communicate and access existing and proposed applications more efficiently. DISA executed a modification to the current Inmarsat contract which allows procurement of I–4/BGAN services. Army Inmarsat users will migrate to I–4/BGAN services. New Inmarsat users will consider I–4/BGAN as their first choice when submitting Operational Needs Statements for Inmarsat service.

(2) *Procurement of Inmarsat equipment.* Army commands are responsible for funding Inmarsat terminal acquisition and airtime. Organizations/units will submit their requirements for approval to DCS, G–3/5/7, ATTN: DAMO-RQ. Organizations/units will submit a TR through DDOE to establish a DITCO service contract for I–3 Inmarsat systems, BGAN SIM card acquisition, and airtime activation. The procuring organization/unit is responsible for arranging the commissioning of Army Inmarsat terminals into satellite access operation by arrangement through NETCOM/9th SC (A)/ESTA-TT.

(3) *Operation of Inmarsat equipment.* Army commands/Army service component commands will ensure field operators configure Inmarsat units to the correct Inmarsat land-earth station. ACOMs/ASCCs may use Inmarsat terminals during deployments and exercises. Upon the establishment of communications by the supporting signal units, Inmarsat terminals will become a backup means for communications.

(4) *Equipment readiness.* Army commands/Army service component commands are responsible for testing Inmarsat terminals to ensure devices are in proper working order. Diagnostic tests will be performed in accordance with the operator's manual.

h. Iridium. Iridium is a unique handheld global satellite terminal system that connects into the DOD satellite gateway via DSN routine secure voice, Networx, International Long Distance, and Hawaii local and toll-free numbers. It has an associated O&M cost that must be reimbursed for its use. Monthly recurring/usage charges may be applied to cover associated O&M cost. (See DA PAM 25–1–1, paragraph 10–9*b*.)

(1) Army commands are responsible for funding Iridium handset acquisition and airtime.

(2) Organizations/units will submit an operational needs statement for approval through the Army command and supporting DOIM to DCS, G–3, ATTN: DAMO–RQ.

(3) Organizations/units will submit a TR through DDOE for acquisition and airtime.

i. Other Mobile Satellite Service Handheld Systems. DOD restricts the use of MSS providers other than Iridium for

unclassified purposes only, with the source and destination within the CONUS. Similarly, the use of Iridium handsets without the security sleeve, for unclassified operations in CONUS, is allowed without receipt of an OSD waiver.

j. Global positioning system (GPS)/precise positioning service (PPS).

(1) The development and procurement of all PPS, GPS user equipment and PPS security devices, including that for special applications, will be coordinated with the GPS Joint Program Office (JPO). (See DA Pam 25–1–1, paragraph 10–9*d*.) Army PPS users will employ PPS user equipment incorporating both selective availability and antispoofing features to support combat operations. The AAE submits waiver requests to OSD for use of Standard Positioning System user equipment in specific platforms or application categories that do not involve combat operations and do not require direct PPS accuracy.

(2) Except for Congressional exemptions (range instrumentation, advanced technology, mapping, Special Forces, and classified applications), the GPS JPO will develop and procure all DOD GPS common-user equipment. Waiver requests for special applications will be submitted to OSD through the AAE.

6–7. Army Web sites and services

a. General.

(1) *Format conventions.* The Army CIO/G–6 is responsible for promulgating policies, procedures, and format conventions for Army Web sites and services.

(2) *Use of AKO/DKO.* Official Army Web sites may exist on either public or non-public (private) Web sites. The AKO/DKO portal is the primary source for collaboration and coordination of Army's non-public information. The use of net-centric communications and AKO/DKO supports execution of Army missions through information sharing and saves resources currently expended on traditional means of communication. Any organization desiring Web capabilities that would duplicate services already available on AKO/DKO must request a waiver from the CIO/G–6, ATTN: SAIS–GKM, prior to purchasing this capability. Waiver requests must demonstrate coordination with the AKO/DKO Program Office.

(3) *Web domain registry.* NETCOM 9th/SC (A) will manage the "army.mil" Web site assignment of subdomains and the Web domain registration process. The Web domain registry will include all the Web domain information of "army.mil" Web sites at the third level domain as well as any commercial Web sites being used. Army organizations desiring subdomains must register their domain through this process.

(4) Coordination through the DOIM. Organizations requesting Web domains will coordinate their requests through the supporting DOIM to apply for any new Internet protocol addresses. DOIMs will complete the application through the NETCOM/9th SC (A) OIA&C. See also DA Pam para 8–1*f*.

(5) *Use of army.mil Web domain.* All Army public and non-public Web sites must be located on an "army.mil" domain unless the CIO/G–6 waives that requirement. See also paragraph*b* for policy concerning use of .mil domains, required waivers, and exceptions.

(6) *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, US Army Reserves, Army National Guard, ACOMs, ASCCs, DRUs, PEOs, PMs, service schools or centers, installations, division-level units, and special service organizations will establish third-tier 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.

(7) *Use of IP restriction.* Public Web sites are on the Internet (World Wide Web) and are considered unrestricted. A Web site which relies only on an Internet protocol (IP) restriction to control access is considered a public Web site.

(8) *Web management policy.* Army Web site managers/maintainers must comply with the Web management policy in this regulation and the DOD Web site administration policy located at http://www.defenselink.mil/webmasters and subsequent DOD guidance and direction.

(9) *Web content.* Management and utilization of public and non-public Web sites must be consistent with Army and Defense policy on official and authorized use of telecommunications. See paragraphs 6–1,*e* and *f* above.

(10) *FTP.* File Transfer Protocol sites in the public domain are not authorized and will not be used in the place of authorized public Web sites.

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

(12) *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.

(13) *Assignment of Web master/maintainer.* Army organizations will assign a Web master/maintainer for each of their Web sites/pages.

(a) Army organizations will provide their Web masters/maintainers sufficient resources and training on both technical and content matters. Resources are available at the Army Web master's homepage: http://www.army.mil/webmasters/.

(b) On-line training is available at https://iatraining.us.army.mil/_usermgmt/login.htm and http://www.disa.mil/handbook/handbook_v1.6.doc.

(c) Web masters/maintainers will have technical control over the site's content and will ensure the site conforms to Defense and Army policies, standards, and conventions.

(14) *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/sec508/508standards.htm. Exceptions should be referred to the Staff Judge Advocate for legal review. (See also paragraph 6–7*a*(2) on information access.)

(15) *Private Web sites.* Activities will establish organizational private Web sites for collaboration and coordination purposes. Organizational Web site managers will install access-control mechanisms, as required. (See para 6–7*a* (2) above for waiver requirements.)

b. Required Use of Army.Mil Domain.

(1) *Use of army.mil.* Per DODI 8410.01, organizations must use "army.mil" domain as their second-level domain name for the Unclassified-but-Sensitive Internet Protocol Router Network (NIPRNet) and "army.smil.mil" for the Secret Internet Protocol Router Network (SIPRNet) unless a waiver has been granted by the CIO/G–6 and, in turn, the DOD CIO. Requests for a waiver must explain the rationale for the use of any domain other than army.mil on a temporary or permanent basis.

(2) *Exception.* The following are exceptions to the "army.mil" policy and do not require waivers:

(a) Army Reserve Officer Training Units that do not fund or operate Internet systems, but use, instead, the domains of their hosting organizations or the organizations that support their Internet communication needs.

(b) US Military Academy, which is authorized to use an "edu" domain.

(c) MWR activities, AAFES operations, and other NAF instrumentalities, which are authorized to use commercial domains.

(d) Army recruiting Web sites in the public domain, which may be hosted and served in a commercial Web domain.

(3) *Special needs.* Examples of special needs or requirements that may be considered and approved for other than the Army.mil domain are as follows:

(a) Inability of GIG assets to support the operations as documented by a GIG waiver.

(b) An international program for which an Army organization is the lead agency representing the United States; the Web site may require a "gov" domain.

(c) A public-private partnership information system or service in which most of the content is non-government, but where the government shares data with a private entity.

(d) Organizations requiring use of "dod.mil" domain because they are designated DOD executive agents or single managers for specified programs.

(e) Temporary Web site (six months or less) used to directly support crisis/disaster, law enforcement, intelligence, counter intelligence, or information warfare operations.

(f) Specialized services on contracted commercial systems not connected to the NIPRNet or SIPRNet and not reliant on access-control mechanisms used in the ".mil" domain. (Generic services such as Web site hosting and e-mail services do not constitute specialized services.)

(4) *Waivers.* Requests for waivers to the required use of the "army.mil" domain, signed by colonel or civilian equivalent, must be submitted by the Web site owner's HQDA element or parent command through Headquarters, Department of the Army CIO/G–6 (SAIS–GKP), 107 Army Pentagon, Washington, DC 20310–0107, to Principal Deputy DOD CIO. Signed memo will be scanned and forwarded by e-mail to: armycio@hqda.army.mil.

(5) *Waiver justification.* Requests for non-army.mil domains must be accompanied by the completed templates from enclosures 6 and 7 in the DODI 8410.01. Minimum justification will include—

(a) Purpose of the Web site.

(b) Army or DOD sponsor.

(c) Authority (statute or regulation) to disseminate/exchange this information.

(d) Time period in which this Web site will be used.

(e) Reason why an Internet domain other than "army.mil" is needed. (Explanations will normally address cost and expedience.)

(f) If non-public, why AKO/DKO or other .mil site cannot be used. (Explanation will include coordination with AKO/DKO and other server administrators to confirm that other .mil solutions are not achievable.)

(g) Confirmation that there will be no association on the Web site with the name of the private provider, no advertising, and no commercial trademarks or symbols.

(h) Access controls and overall security to be applied. (If PKI with AKO/DKO Single Sign-On (AKO/DKO SSO) is not used for access, explain the reason. Refer to paragraph*e* on commercial certificates.)

(i) Description of any personally identifiable information concerning a military service member, family member, or

other individuals that will be collected and maintained, a justification for why this information must be collected, and explanation of how it will be managed and safeguarded.

c. Army Public Web Site Management.

(1) *Guidance.* The Army CIO/G–6 promulgates policies, procedures, and format conventions for public Web sites in this regulation and the DA Pam 25–1–1, chapter 8. This guidance, in addition to any updated policy, is posted on the CIO/G–6 Web site at http://www.army.mil/ciog6/references/webmaster/policy.html.

(2) *Registration.* In order to facilitate the public in locating government information resources, organizations must register their public Web sites (for example, http://www.netcom.army.mil) with the Army Homepage Web master at http://www.army.mil. Army organizations' Web maintainers must update this information as changes occur.

(3) *Posting.* Only official Army information that is releasable and of value to the public may be posted on Army public Web sites. Official information of interest to Army employees will be posted on AKO/DKO. Army commanders/organizational heads will ensure that the PAO and other appropriate designee(s) (for example, command counsel, force protection, intelligence, and so on) review and clear Web content and format prior to posting to the Internet. Information contained on publicly accessible Web sites is subject to the policies and clearance procedures prescribed in AR 360–1, chapter 5, for the release of information to the public. Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the Internet. (See also paragraph 5–10.)

(4) Web site reviews. 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 herein 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 management control checklist items at appendix C, paragraph C–4. In addition, Army organizations using the Internet will not post the following types of information on Army's publicly accessible Web sites:

a. FOIA-exempt information.

b. Records currently and properly classified in the interest of national security.

c. Records related solely to internal personnel rules and practices that are not meant for public release.

d. Restricted or limited distribution information.

e. Records protected by another law that specifically exempts the information from public release. This includes information protected by copyright.

f. Trade secrets and commercial or financial information obtained from a private source which would cause substantial competitive harm to the source if disclosed.

g. Internal records that are deliberative in nature and are part of the decision-making process that contain opinions and recommendations. This exemption includes draft documents, draft publications, or pre-decisional information of any kind.

h. Records which, if released, would result in a clearly unwarranted invasion of personal privacy.

i. Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties-such as general officers and senior executives, PAOs, or other personnel designated as official command spokespersons-is permitted. In addition, command Web sites may publish the name, rank, and duty station of military personnel in photo captions and news stories. Point of contact information on posted memoranda is also excluded from this restriction.

j. Investigatory records or information compiled for law enforcement purposes.

k. Web logs, video logs, or chat rooms.

(5) Privacy and security. Web masters/maintainers will apply appropriate privacy and security policies to respect visitors' privacy.

a. Web sites will display a privacy and security notice in a prominent location on at least the first page of all major sections of each Web site.

b. Each privacy and security notice must clearly and concisely inform visitors to the site what information the activity collects about individuals, why it is collected, and how it will be used. For an example, see the Defenselink Web site (official Web site of DOD), which states, "For management purposes, statistical summary information or other non-user identifying information may be gathered for the purposes of assessing usefulness of information, determining technical design specifications, and identifying system performance or problem areas."

c. 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 identifying information on public Web sites without the express permission of the user is prohibited. Requests for exceptions must be forwarded to the Army CIO/G–6.

d. Third-party cookie generation will be disabled.

(6) Web content. Web site owners/maintainers will ensure that—

a. Web servers are IAVM compliant and placed behind a reverse proxy server or implement an alternative security procedure. Reverse proxy servers must be configured in a way that does not cache secure sockets layer (SSL) traffic.

b. Web site content is accurate, current, and provides reliable data in compliance with information quality guidelines at paragraph 1–12.

(7) Army commands and activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web sites. Guidelines should consider the information needs of mission-related requirements and public communications and community relations objectives.

a. No compensation of any kind may be accepted in exchange for a link placed on an organization's publicly accessible official Army Web site.

b. Listings of Web links on Army Web pages must separate external Web links from Government and military links.

c. When external links to non-Government Web sites are included, the following disclaimer must appear on the page(s) listing external links or through an intermediate "exit notice" page: "The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this Web site."

(8) Web site owners notified by the AWRAC of Web site violations will make immediate corrections or block the Web site or link until corrections can be made. (See paragraph 5–10 for additional information.)

d. AKO/DKO and AKO-S.

(1) *Use of AKO/DKO.* AKO/DKO (www.us.army.mil) and AKO-S are the enterprise portals supporting unclassified and classified Army web sites. Activities will leverage AKO/DKO and AKO-S to the maximum extent possible to develop knowledge networks and portals inside AKO/DKO. Private Web sites separate from AKO/DKO should be established only when AKO/DKO cannot support the requirement. The use of AKO/DKO and AKO-S enables optimal sharing of Army information and knowledge resources across the entire Army enterprise. Army activities will maximize their use of AKO/DKO resources, features, and tools to reduce the need for investment in the same types of IT resources.

(2) *Authentication of access.* AKO/DKO is the single authoritative source for authenticating user access to Army Web-enabled ISs and Web servers that serve users with DOD IP addresses. Existing Army portals or Web servers with authentication services that duplicate AKO/DKO services will migrate to AKO/DKO authentication unless waived by CIO/G–6. Army Web-enabled business applications are required to be linked from the AKO/DKO portal. The initial minimum standard is a URL link on the Army portal to the application. The objective standard is to use the AKO/DKO directory services for authentication as well as a URL link on the Army portal.

(3) *Administration.* For organizational space on the AKO/DKO portal, each Army organization will assign a top-level administrator for their primary organizational presence, and, where needed, assign delegated administrators to manage the content within subordinate organizations. Army organizations will provide administrators sufficient resources and support.

(4) *Content control.* Organizations will ensure their AKO/DKO site content posting procedures conforms to Defense- and Armywide Web site policies. Content that is made available to all AKO/DKO users and groups, that is, "Unrestricted" content, should be treated as publicly accessible and subject to Web guidelines for PAO review. Organizations should establish procedures for content providers to place information on the site and ensure that administrators assign security and access controls requested by content providers. Content owners are required to establish the appropriate mechanisms to protect sensitive information from being accessed by unauthorized individuals.

(5) *Logon.* All AKO/DKO account users are responsible for the security of their AKO/DKO credentials (that is, user name and password) and content that they create on the portal. CAC logon is preferable to user name and password logon.

(6) *Posting.* AKO/DKO users will conform to AKO/DKO posting procedures and policy on the use of official and authorized telecommunications. See paragraphs 6–1*d*, *e*, and *f*.

(7) *Security.* Users that fail to properly secure their AKO/DKO credentials and content on the AKO/DKO portal will be subject to nonjudicial or judicial action under the Uniform Code of Military Justice. See Summary page of this publication.

(8) *AKO records.* E-mail and other files on AKO/DKO that are determined to be records will be managed per chapter 8 and AR 25–400–2.

e. Other Private Web Sites (Intranets and Extranets).

(1) *Hosting.* Army organizations are authorized to host private Web sites when AKO/DKO resources cannot support the functional requirement (para 6–7*d*). See also paragraph 6–7*b* for Web domain restrictions.

(2) *Authentication.* All unclassified 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 encryption certificates are loaded. Use of Internet Protocol 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/9th SC (A) TNOSC.

(3) *Web application authentication.* All Intranet Web applications will use AKO SSO or AKO SSO with CAC for user access, unless waived by NETCOM/9th SC (A). Legacy applications currently using AKO/DKO Lightweight

Directory Access Protocol to authenticate clients must migrate to SSO capable platforms. For more information on how to use AKO/DKO directory authentication and AKO SSO, visit the AKO/DKO Authentication Center and SSO Homepage at AKO Home, Quick Links, AKO Tips & Training, and Single Sign-On Home.

(4) Use of PKI. Web applications must be PKI-enabled.

(5) *Exceptions.* The following type of Web server is exempt from using CAC/PKI or other forms of encryption: any unclassified Army Web server providing non-sensitive and publicly releasable information resources categorized as a private Web server only because it limits access to a particular audience only for the purpose of preserving copyright protection of the contained information sources, facilitating its own development, or restricting access to link(s) with limited access site(s) (and not the information resources).

(6) *Extranets authentication.* Unclassified Extranets (private Web sites used for exchanging non-public 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 (http://iase.disa.mil/common/index.html).

6–8. Information technology support for military construction

Information technology requirements must be identified and funded in all military construction (MILCON) so that the resulting building has a built-in IT infrastructure that satisfies the occupants' requirements on the beneficial occupancy date. (See DA Pam 25–1–1 paragraph 7–10.)

a. Planning, designing, and monitoring construction. The supporting DOIM will provide oversight of the IT support for MILCON. The DOIM must maintain a close and continuous coordination with the Directorate of Public Works to ensure a complete awareness of all IT functional requirements, to include mission-related and base support, for inclusion in the USACE statement of work for construction. If this expertise is not available, the DOIM should request assistance from the using organization in developing the IT functional requirements to support the facility. Upon contract award, a task officer with IT expertise will monitor contractor performance and provide approval/disapproval to the common operating environment contracting officer's representative.

b. Requirements for floor space intended for IT systems. The supporting DOIM will identify all proposed floor space intended for IT systems to the RCIO. The RCIO will review the proposed requirements for consistency with single DOIM server consolidation and APC migration timelines. The CIO/G–6 will coordinate with the occupant and the U.S. Army Information Systems Engineering Command (USAISEC) as appropriate to validate the required floor space needed for IT systems.

c. Cost estimates and funding. Department of Public Works will ensure the DOIM 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 DOIMs will ensure that IT cost estimates for validated IT requirements are identified for each component supporting MILCON facilities. The RCIO will validate and approve the DOIM input to the DD Form 1391 prior to submission. The USAISEC must certify all DD Form 1391s to IMCOM before the respective Project Review Board in accordance with AR 420–1, paragraph 4–4*v* and 4–20*a*. IT funding and installation responsibilities will be identified for inclusion to the DD Form 1391 (FY, MILCON Project Data) per AR 420–1, paragraph 4–23. 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. Inter-Service support agreements (ISAs) 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.

(1) LANs are the preferred solution to satisfy data requirements and will be installed during the construction of a facility.

(2) Existing metallic cabling will be used as long as it is capable of providing the required service(s). New cable runs, optical fiber or combined fiber, and twisted pair cable must be installed for both the outside cable plant and building premises. This includes cable from the main distribution frame, through intermediate distribution frames, and to the communications distribution room. Army MILCON that provides copper only to the outlet will provide additional raceway space to accommodate future fiber optic cable installation, for both premise wiring and outside cable plant. Fiber optic cable will be installed to the outlet during construction if the user/proponent has a current valid requirement for fiber optic connectivity.

Chapter 7
Visual Information

7–1. General

Visual information (VI) is that element of IT that addresses the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery and multimedia, with or without sound, linear or nonlinear, for the purpose of conveying information. VI includes the exchange of ideas, data, and information regardless of formats and technologies used (see DODD 5040.3).

a. Mission. The VI mission is to provide the President, Secretary of Defense, JS, military departments, and Army commanders with COMCAM and record documentation, multimedia/VI products, and services to satisfy official requirements. These requirements may include, but are not limited to, support for C2, training, education, logistics, medical, personnel, special operations, engineers, public affairs, and intelligence to effectively convey accurate information to the warfighter, decision-makers, and supporting organizations.

b. Exclusions. The following are excluded from the VI provisions of this chapter, except as otherwise noted:

(1) All VTC capabilities and/or facilities. For VTC policy, see chapter 6 of this regulation.

(2) Photomechanical reproduction, cartography, x-ray, and microfilm and microfiche production.

(3) Products collected exclusively for surveillance, reconnaissance, intelligence, or psychological operations and VI equipment integrated in a reconnaissance-collecting vehicle.

(4) Multimedia/VI productions on the technical, procedural, or management aspects of DOD cryptological operations.

(5) Facilities, services, and products operated or maintained by AFRTS. Products or productions acquired and distributed exclusively for AFRTS overseas use.

(6) Commercial entertainment productions and equipment acquired and distributed by the AAFES and the Navy Motion Picture Service.

(7) Systems embedded in training devices, simulators/simulations, instrumentation systems, weapons systems, medical systems, or language labs for which the primary purpose is not VI.

(8) Equipment and products acquired with NAF.

(9) Organizations using still camera equipment for the purpose of generating identification or security badges.

(10) At the discretion of the VI manager, individual VI activities and their equipment and services that are 100 percent funded by RDT&E and used solely to support programmed and funded RDT&E missions and not common-support VI requirements. RDT&E activities are not excluded from the VI Documentation Program (see para 7–10).

(11) Non-VI activities using COTS office business graphic software in an office environment.

(12) Nurse call/paging systems, binoculars, fixed outdoor public address systems, bugle call systems, silk screen equipment, outdoor sign makers, and security surveillance systems.

(13) USACE products and services that are funded by civil appropriations and used solely to support civil works-funded and non-DOD agency missions.

(14) Multimedia products developed within the printing and publications policy and procedures guidelines.

(15) Library materials and equipment acquired for use in Army libraries.

(16) Multimedia/VI productions that are produced to support the Army recruiting efforts.

c. Exception. If a product that would otherwise be excluded from this chapter is used in a multimedia/VI production, the production and all materials used are subject to the policies in this chapter.

7–2. Visual information Combat Camera

Combat Camera (COMCAM) imagery is used to assist battlespace decision-making and is valuable for frontline commanders. Commanders can depend on COMCAM teams to help exploit the power of horizontal information flow, speed up the decision-making cycle, and facilitate execution at lower levels. COMCAM also provides historical documentation of ongoing military operations and supports strategic communication objectives by integrating and synchronizing the acquisition and distribution of still and motion imagery.

a. The CIO/G–6 is the proponent for COMCAM. The Army VI Management Office (SAIS–AOI) serves as the focal point for the program.

b. NETCOM/9th SC (A) organizes and operates COMCAM teams through the 55th Combat Camera Company to provide visual documentation of operational contingencies, exercises, joint operations, and relief activities in response to major disaster and other peacetime engagements.

c. Army VI COMCAM teams will be maintained to provide rapid VI support to combatant commanders for military operations, emergencies, and field exercises. CIO/G–6 and FORSCOM will ensure that all contingency and war plans include COMCAM requirements in their operation annexes. (See DODI 5040.4.)

d. COMCAM teams will provide still and motion imagery coverage of force deployments and events before, during, and after military engagements.

e. FORSCOM is responsible for COMCAM mission taskings. Requirements for COMCAM support will be identified to FORSCOM and copy furnished to NETCOM/9th SC (A).

f. Army COMCAM teams will be tasked to participate in DOD joint exercises along with COMCAM teams from other services. Only the CJCS and combatant commanders have the authority to task joint service COMCAM teams. (Also see DODI 5040.04 and FM 6–02.40.)

g. Materiel requirements for COMCAM will be documented and approved per AR 70–1 and AR 71–9. VI authorization to TOE and TDA units will be documented per AR 71–32.

h. COMCAM will submit imagery for historical documentation to meet the requirements prescribed in the CFR 36.

7–3. Visual information responsibilities

a. Assistant Secretary of Defense (Public Affairs) (ASD(PA)) Defense VI (DVI) assigns various responsibilities to the military departments to provide VI support to more than one DOD component.

(1) Army productions will be acquired per the Federal Acquisition Regulation (FAR) 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.

(2) Army Multimedia and Visual Information Directorate (AMVID) will provide a central capability to rent, lease, procure, or produce multimedia/VI productions in support of Army, DOD, other military departments, and other Government agency requirements as requested. AMVID and the Enterprise Multimedia Visual Information Service Center (E/MVISC) are the only authorized Army activities to issue production procurement contracts exceeding the $10,000 limit (to include man-hours, equipment rental, administrative expenses, and any other operating cost) for support services (see para 7–7*a*(11)(*b*)). Contact AMVID/Production Acquisition Division, http://www.hqda.army.mil/amvid, for assistance with production cost estimate. AMVID will also provide support to OSD, JS, other Army organizations, and other Federal agencies within the Pentagon reservation and the NCR. AMVID is responsible for the Army's imagery accessioning.

(3) The E/MVISC will provide products and services classified as "above baseline" or mission per the CIO/G–6 List of Directorate of Information Management (DOIM) Service Level Agreement (SLA) /Operational Level Agreement C4IM services. All M/VI personnel will comply with the C4IM common-user baseline services document. These 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 E/MVISC for production or approval for local installation production. The E/MVISC will provide in-house production of multimedia/VI in support of Army, DOD, other military departments, and other Government agency requirements. Contact: 2715–C McMahon Street, Fort Eustis, VA 23604–5253; Commercial: 757–878–3761; www.eustis.army.mil/tasc and/or Ft Lewis (E/MVISC), B1401 W. 6th St. MS 97, Fort Lewis, WA 98433–9500; 253–966-1187; lewisdoimvi.info@conus.army.mil.

(4) The Department of the Army Multimedia Visual Information Production Distribution Program (DAMVIPDP) supports the development, replication and distribution of training videos to support HQDA approved programs of instruction. To request DAMVIPDP funding, contact US Army Training Support Center, Fort Eustis, VA 23604. Alternatively, visit http://www.atsc.army.mil/ or call 1–800–ASK–ATSC (1–800–275–2872).

b. The CIO/G–6 Visual Information Management Office is responsible for managing the Army's VI activities and coordinating with ASD (PA) on VI reporting requirements. The HQDA CIO/G–6 (SAIS–AOI) office will—

(1) Assign a production identification number (PIN) to non-local productions.

(2) Assign the DOD Visual Information Activity Number (DVIAN).

(3) Manage the Army portion of the Defense Automated VI System (DAVIS).

(4) Manage the VI Systems Program (VISP).

(5) Manage and execute the VI Award Program.

c. U.S. Training and Doctrine Command school proponents and FOA visual information managers will—

(1) Search the DAVIS before completion of DD Form 1995.

(2) Develop a six-year VI systems acquisition plan and submit the investment portion of the plan and annual updates to CIO/G–6 (VI) for POM development.

d. Local VI managers will—

(1) Validate, consolidate, and submit VI investment system production (VISP) requirements to HQDA CIO/G–6 (SAIS–AOI) for validation, prioritization, and funding when requested by HQDA CIO/G–6.

(2) Approve and/or validate VI production multimedia requirements, maintain production registers, and submit requirements for annual DA Multimedia/Visual Information Production and Distribution Program (DAMVIPDP).

(3) Annually review, validate, approve as authorized and forward requests through the Defense Visual Information (DVI) Web site (http://dodimagery.afis.osd.mil/) to create or modify a VI Activity Profile. Complete DD Form 2858 (Visual Information Facilities) for the establishment, expansion, or disestablishment of VI activities.

(4) Conduct commercial activity reviews for assigned VI functions (T–807–Visual Information) per AR 5–20.

(5) Serve as the representative to the Army VI Steering Committee.

(6) Manage VI non-tactical documentation submissions to the VIDOC program.

7–4. Visual information activities

a. The Enterprise Multimedia Visual Information Service Center supports the realignment of VI resources, functions, and facilities for the transforming institutional Army. The E/MVISC will be symmetrical in design and connected to an Armywide network. Each installation multi-media/VI (M/VI) activity will be connected to the supporting E/MVISC for support from a single location.

b. A VI activity performs or provides any product or service listed in paras 7–7 and 7–8. No organization or individual will perform, provide, or contract these products or services without authorization unless specifically excluded. (See exclusions in para 7–1*b*.)

c. Visual information activities are classified as industrial operations (General Functional Area T–807) and are subject to OMB Circular No. A–76 studies, except for VI management, combat, and combat support (COMCAM) elements. Curtailment of commercial activities is appropriate to reestablish combat and combat support elements or rotational positions to support war plans.

d. Local VI activities submit requirements through a DOD Web site at http://dodimagery.afis.osd.mil/ using DD Form 2858. CIO/G–6 (SAIS–AOI) will assign the DVIAN. (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.

e. All installation DOIMs, in coordination with VI managers, will plan, program, and budget for all authorized VI requirements.

(1) When funding permits, VI activities will be staffed and equipped to operate at average projected workloads. Installation VI managers will establish a standard level of support documents that identify the customers and resourced capabilities. Requirements above this standard level of support will be satisfied on a reimbursable basis in accordance with current Army reimbursable policy or will be referred to the Activity VI manager for support. Army off-post customers operating under "shop smart" will not reimburse for military personnel file photographs, as required by AR 640–30.

(2) Visual information activities may be authorized to fabricate VI aids, displays, and exhibits.

(3) Visual information activities will establish and maintain a list of current charges for all reimbursable products and services. Fee-for-service or industrially funded VI activities will recover the full cost of support.

f. Media loans will be recorded on DA Form 4103 (Visual Information Product Loan Order). A DA Form 3903, Multi-media/Visual Information (M/VI) Work Order, will be used to identify and capture all work associated with a customer request for products and services. These forms are available on the Army Publishing Directorate (APD) Web site (http://www.apd.army.mil/).

7–5. Visual information operations

a. Visual information support will be limited to events or activities that are related to official missions and functions. The use of VI products, equipment, or facilities for other than official purposes, such as loaning equipment to local and state governments or nonprofit organizations meeting on Government property, will be at the discretion of the local commander and in accordance with AR 700–131 and AR 735–5.

b. Priorities for VI support will be established with consideration given to mission, timeliness, cost effectiveness, quality and quantity of products, and services available.

c. Visual information activities will not expand or accept permanent additional workloads that exceed their existing capability without a change in authorization.

d. Each VI activity will publish standing operating procedures (SOPs) which will be included as part of the customer SLA document.

e. Procedures, reports, and formats for the management and operation of VI activities are contained in DA Pam 25–91. VI prescribed forms and reports are listed in appendix A, section III.

f. Visual information activities with a unit identification code may maintain a dedicated property book of VI equipment and systems.

g. At the beginning of each quarter, installation VI Managers will collect and consolidate data for input into Army's IT Metrics Program. See also paragraph 3–7*i*. The installation VI Manager will coordinate with the DOIM office, as the central IT Metrics data collection point, for data deadline information and consolidation of input.

7–6. Equipment and systems

a. Definition. Visual information equipment and systems are items of a nonexpendable or durable nature that are capable of continuing or repetitive use. These items are used for recording, producing, reproducing, processing, broadcasting, editing, distributing, exhibiting and storing VI products. A VI system exists when a number of components (items) are interconnected and designed primarily to operate together. When items that could otherwise be called non-VI equipment are an integral part of a VI system (existing or under development), they will be managed as part of

that VI system. All hardware and software listed under Federal Stock Classification 70 that have a dedicated purpose of preparing or presenting VI material will be validated, approved, and managed as VI equipment by the appropriate level. When copiers or duplicators capable of producing single or multicolor process copies in a single pass, regardless of speed, are used in support of VI, prior approval to procure must be obtained from the appropriate level of VI management (Reference AR 25–30.).

b. Funding requirements. Visual information COTS investment items are DA-controlled with a cost threshold established by Congress. VI systems and equipment requirements costing in excess of the OPA threshold will be validated by the requesting FOA VI manager and coordinated with the DOIM prior to forwarding to HQDA, CIO/G–6 (SAIS–AOI). These requirements will be prioritized and funded (MDEP MU1M) by the CIO/G–6. Television-Audio Support Activity (T-ASA), an OSD organization, is the item commodity manager for the acquisition of commercially available VI investment equipment. COTS nontactical VI equipment and systems costing $50,000 or more will be procured by the T-ASA. Installations and FOA VI managers may provide supplemental investment funds for the acquisition of CIO/G–6-approved requirements. Local procurement authority may be granted by T-ASA. Expense items of equipment costing less than $50,000 may be procured locally upon approval of the DOIM. This authority may not be delegated further.

c. Resourcing. Visual information managers will plan for VI equipment to meet their current and projected needs per the Army VI strategy. Requirements for investment equipment will be developed and forwarded annually by each VI manager in a consolidated six-year plan. This plan is the basis for establishing annual funding increments for equipment replacement. VI managers will also submit investment VI equipment requirements for inclusion in the POM submissions. Visual information activity managers will plan for VI expense and investment equipment through installation resource management channels as part of their annual operating budget.

d. U.S. Army Installation Command (IMCOM) will conduct a data call to the garrisons and provide requirements to HQDA CIO/G–6 for IMCOM installations. For non-IMCOM installations, data will be collected by the appropriate command.

(1) Requirements for photography, television, audio, graphic art, electronic imaging, and broadcast radio and television equipment and systems will be submitted for VI management approval and will subsequently be documented on the appropriate authorization document (TDA or CTA) per AR 71–32 and AR 710–2. All requirements for VI items (excluding expendables and consumables) with an end item cost over $25,000 will be documented on DA Form 5695 (Information Management Requirement Project Document (requirement control symbol (RCS): CSIM–46)), available on the APD Web site. (See DA Pam 25–91 for instruction on form completion.)

(a) Type classified items: CIO/G–6 will validate requests for authorization of VI equipment and systems prior to documentation in a CTA, TDA, or TOE/MTOE to ensure compliance with DODI 5040.02. Per AR 710–2, users/owners are responsible for property book accountability of authorized VI equipment.

(b) Investment VI equipment requirements for Government-owned, contractor-operated VI activities that use Government-furnished equipment will be acquired through the VISP, and, consistent with the terms of the contract, will only support contractor services provided to the Government.

(2) Installation VI managers may designate specific nonproduction, end-user VI equipment that is subject to high-volume, continuous use, to be authorized for procurement, ownership, and operation by organizations normally supported by the authorized VI activity. Examples include consumer-grade video cameras, video/data projectors, viewgraph projectors, 35-mm projectors, self-developing cameras, Digital Video Disc (DVD) players/recorders, TVs, or portable projection screens. The following guidelines will be observed when exercising this option:

(a) Only expense-funded VI equipment costing under $25,000 per item/system may be considered for end-user ownership.

(b) The user/owner will ensure that all equipment meets interoperability, DISR, and VI architecture standards. User/owners will maintain their own equipment. (Visual information activities will not maintain this equipment.)

(c) Common support VI activities may continue to provide VI equipment for loan on a limited basis to support requirements. User/owners will not acquire, lease, or rent professional quality VI production equipment.

(d) User/owners must adhere to Federal copyright and records management laws. Record documentation acquired by on-duty Government employees or contractors on the behalf of Government must be submitted to their local support VI manager for accessioning.

(3) The total procurement cost will determine if a purchase is an expense or an investment item when adding, replacing, or modifying components to an existing system. However, VI managers should anticipate training costs when making purchases of VI equipment, and these costs may be included in the total procurement cost depending upon the terms of the contract.

(4) Installation VI managers must establish annual review procedures to validate VI equipment and repair part allowances and inventories. They will also ensure that obsolete or under-utilized equipment and repair parts are redistributed where needed or turned in for disposal. VI managers may procure repair parts locally.

(5) Maintenance of VI equipment will be performed and managed in accordance with AR 750–1, chapter 5, section VIII. Preventive maintenance on VI equipment will be performed in accordance with manufacturers' prescribed scheduled maintenance.

e. Certification of assets.

(1) The Army must certify VI equipment and systems with network or wireless interface capability as DISR-compliant prior to acquisition.

(2) The CIO/G–6 is the delegation authority for certifying VI assets between $250,000 (or the OPA threshold) and $2.5 million. The installation DOIM processes the request for equipment and systems between $250,000 and $900,000 through the VISP for the CIO/G–6 certification. Proof of certification exists when a HQDA VISP acquisition priority number is assigned to a specific VI requirement.

(3) Equipment and systems under $250,000 (or the OPA threshold, whichever is higher) are certified by the DOIM or delegated to the installation VI manager. Certification authority may be delegated to the lowest level that assures positive and effective controls and ensures compliance with the DISR. Written certification must be provided to the contracting officer prior to procurement for VI equipment and systems under $250,000.

f. The Visual Information Systems Program provides for the annual identification, funding, and acquisition of requirements for COTS VI investment (DA controlled) equipment and systems. Table of Distribution and Allowances VI activities will use this equipment to record, produce, reproduce, distribute, or present VI products. Examples are still and motion media systems (analog and digital), computer graphic equipment, and conference room presentation systems. Department of the Army-controlled equipment/systems are investment items above the threshold established by Congress. CIO/G–6 is the functional proponent for the VISP. Project management and engineering is the responsibility of T-ASA. (See also DA Pam 25-91.) The following equipment will not be purchased through the VISP:

(1) Visual information equipment used exclusively for RDT&E.

(2) Medical peculiar VI items such as medical life support and patient monitoring systems, Medical Care Support Equipment items (radiological graphic processors), medical information display systems, and so on.

(3) Permanently-installed public address systems (including bugle-call systems) at installations, which are handled as real property or property in place.

(4) Television observation/surveillance and remote viewing systems.

(5) Cable distribution systems external to the actual front-end production and playback equipment.

(6) Intercom systems external to front-end equipment for transmission of feed, except those designated specifically to control studio productions.

(7) Visual information equipment items that are part of information system requirements for all MILCON projects.

(8) Manual or electronic typesetters, copiers, and laser printers used for printing and publishing.

(9) Installed presentation systems in classrooms or conference rooms.

g. Investment VI equipment and systems are normally funded with OPA-2 dollars. Operations and Maintenance, Army funds support expense items.

h. Funding other than procurement dollars. VI activities that are supported by funding other than procurement dollars (for example, Army Industrial Funds, civil works, intelligence, and so on) will procure VI equipment with those resources that support their operation. FOA VI managers will ensure that only authorized VI activities with established DVIANs purchase DISR-compliant VI equipment.

7–7. Products

a. Multimedia/VI productions. Multimedia/VI productions are a combination of motion media with sound in a self-contained complete presentation, developed according to a plan or script for conveying information to, or communicating with, an audience. When multimedia/VI productions meet the criteria stated below, they will be managed per the DAMVIPDP.

(1) The delivery of multimedia/VI productions includes, but is not limited to, solid state memory cards, hard disk, removable magnetic or optical disk, digital video disc (DVD), and the Internet. Multimedia/VI productions are usually displayed electronically or optically.

(2) Multimedia productions may include combinations of text and/or other VI products such as motion video, graphics, still photography, animation, or audio. Multimedia/VI productions include informational products (for example, recruiting, public, or command information) or electronic publications. Multimedia/VI productions will be used when cost-effective and appropriate to support mission requirements. Wherever possible, COTS or existing productions will be used vice creating a new one.

(3) Productions containing predominantly textual information are considered electronic publications, not multimedia productions, and are governed by printing and publishing policies.

(4) The recording, duplicating, and/or use of copyrighted material in a VI production is prohibited by law (Title 17 USC, Copyrights) unless prior permission from the copyright owner is obtained in writing. (Also see paragraph 7–12*d*.)

(5) The following VI products are exempt from the provisions of this section:

(a) Graphic art, electronic and/or digital images, still photographs, motion picture photography, and video and audio recordings not used in multimedia/VI productions.

(b) Visual information report content that is obsolete within a year does not require life cycle management. Examples include VI reports (technical, intelligence, and maintenance reports), video reports, and videos of briefings,

seminars, conferences, classroom instructions, or commanders' messages to their troops that are for short-term immediate use.

(c) Visual information products resulting from criminal investigations and other legal evidentiary procedures.

(d) Television and radio spot announcements, public service announcements, and news clips.

(e) Documentation or productions created for the purpose of communicating clinical, histopathological, or other professional medical information to members of the civilian health science community and are not a part of the DAMVIPDP.

(6) All multimedia/VI production requirements will be processed per DODI 5040.07 using DD Form 1995 (Visual Information (VI) Production Request and Report) (RCS DD–PA (AR)–1381). See DA Pam 25–91 for instructions. Multimedia/VI productions will be identified as one of two types listed below—

(a) Local productions. Local productions support the needs of a local installation and its area of responsibility with no dissemination of the production outside the area.

1. Local productions will be reviewed annually for currency.

2. Total cost will not exceed $10,000 (to include man-hours, equipment rental, administrative expenses, and any other operating cost) and incur no direct out-of-pocket expenses. Total number of replicated copies will not exceed 25.

3. The DAVIS/Defense Instructional Technology Information System (DITIS) will be searched by subject and the results maintained in the official production record throughout its life cycle. Data entry into DAVIS/DITIS is mandatory.

4. Local productions will not be created to support human resource development or activities that are applicable for Armywide use, including human relations, chaplains, safety, medical topics (excluding medical seminars, briefings, continuing education, and medical board and society updates), military police, and other similar activities.

5. A production authorization number (PAN) will be assigned to each local production. (Reference DA Pam 25–91, chap 6.)

6. Activity VI managers will maintain a PAN register for all local inhouse produced productions. The inhouse production register will be maintained on file by the installation VI manager for current fiscal year plus two additional years (FY+2).

(b) Non-local productions. These productions are for multi-installation, FOA, Army, or DOD-wide use.

1. These productions, regardless of cost or format (for example, videotape or multimedia), will be certified by the CIO/G–6 using DD Form 1995.

2. Non-local productions will be assigned a PIN. A PIN register or log will be maintained to ensure control and accountability of non-local multimedia/VI productions. (See DA Pam 25–91 for format.) Non-local productions will be assigned a PIN by HQDA CIO/G–6 (SAIS–AOI).

3. Joint VI Service Distribution Activity (JVISDA) distributes non-local productions.

4. A subject search in DAVIS/DITIS is required. Search results will be maintained in the official production record throughout its life cycle. Data entry into the DAVIS/DITIS is mandatory using DD Form 1995.

5. Non-local multimedia/VI productions (inhouse and COTS) will be reviewed by the Office of Primary Responsibility (OPR) for obsolescence within five years of their initial distribution and every three years thereafter. Multimedia/VI productions are obsolete when they no longer reflect current information and will be removed from the inventory. Obsolete multimedia/VI productions may be declared historical when they no longer reflect current policies and procedures, but accurately reflect past events that are considered historically significant (see DA Pam 25–91).

6. Office of Primary Responsibility and/or VI managers will go online to initiate and complete Section I of the DD Form 1995 (http://dodimagery.afis.osd.mil/) - Order/Initiate VI Production. This section will include production costs. The HQDA CIO/G–6 (SAIS–AOI) will validate the DD Form 1995 and complete Section II. That includes assigning a PIN to the production. The form is returned to the requesting activity to proceed with the production. The contracting activity or Production Activity completes Section III of the form. The Distribution Activity completes Section IV of the form. This process is done by e-mail. Note: Activity proponent must complete Section I, DD Form 1995 fields or blocks to include productions cost. CIO/G–6 (SAIS–AOI) will not certify the Form 1995 without complete information (for assistance with production cost estimate, contact AMVID/Production Acquisition Division).

7. Captioning for hearing-impaired: OPRs are responsible for ensuring that their multimedia/VI productions comply with both Section 508 of the Rehabilitation Act of 1973 and DOD guidance. (See also paragraph 6–1*p* of this publication.)

8. The functional proponent, who manages the resources for the area to be supported, will validate VI production requirements. The functional proponent will evaluate the production objective and confirm that it is a legitimate requirement in support of an authorized program or mission, does not duplicate an existing production, and is the best method of presentation. In making this determination, the functional proponent will consider these factors: communication objective; doctrinal accuracy; target audience; production costs; user costs; life span of the information to be conveyed; frequency of use; immediacy of requirement; necessity for periodic updating; distribution format; method, level, and cost of distribution; and compatibility with other existing communication programs.

9. Multimedia/VI productions will be acquired in the most cost-effective manner. The Army will use the Federal

Uniform Audiovisual Contracting System for competitive procurement of new multimedia/VI productions as prescribed by DODI 5040.07. The training video will comprise less that 25 percent of the cost of the overall effort and will be incidental to the overall effort and not the primary requirement.

a. When the total production is contracted at 100 percent (excluding replication and distribution), the production will be assigned to the designated Army contracting activity for production. In instances where the effort is less than 100 percent, the requiring activity may contract in the most cost effective manner to complete the project using commercial or government assets assigned to the Information Management Command (IMCOM).

b. Visual information managers, AMVID activities, and procurement officers will ensure that all applicable FAR rights and data clauses are included in contracts acquiring multimedia/VI productions or services to ensure the Army owns all rights to the productions and master materials. The Army will not be required to pay royalties, recurring license or run-time fees, use tax, or similar additional payments for any production or associated materials developed for the Army.

10. The VI production activity (for inhouse production) or the AMVID VI contracting office (for contracted productions) will obtain a legal review and public release clearance prior to production distribution. Legal review and public clearance documents will be maintained throughout the life cycle of the production.

11. Exceptions to VI production policy are—

a. When recruiting, multimedia/VI productions are integral to an overall advertising agency contract.

b. Purchasing production services to augment inhouse capabilities when this method of acquisition is the most cost-effective. Production support services, such as narrations, scriptwriting, and graphics, will not exceed $10,000.

c. When COTS proprietary productions are purchased, leased, or rented.

12. Prior to commitment of production funds for a product whose intended audience is the public, a copy of the treatment or script will be submitted, with legal determination, to Public Affairs requesting public exhibition authority. A separate clearance from Army Public Affairs is required for sale, rental, or lease to the public or foreign countries. All VI productions will be cleared for public release upon completion except when restricted by security classification, production, or when the production contains copyrighted material.

13. Reproduction of any Army production in whole or in part is prohibited without the approval of the proponent, VI manager, JVISDA, or CIO/G–6. Non-local multimedia/VI productions will not be distributed until JVISDA receives the master and production folder. JVISDA will replicate and make initial replication of all non-local multimedia/VI productions. Requests for additional copies can be electronically submitted through DAVIS/DITIS.

14. The sale of multimedia/VI productions under the Foreign Military Sales Program is covered in AR 12–8. Requests for multimedia/VI productions from or on behalf of foreign sources may be approved, provided the following is met—

a. Requests for release of multimedia/VI productions for loan or viewing by foreign military audiences will be forwarded to JVISDA for necessary administrative clearance. Release of classified information will be conducted per AR 380–10.

b. Requests for purchase of unclassified media by foreign civilian sources will be routed through JVISDA to the U.S. Army Security Assistance Command for clearance.

c. If release to a foreign audience is questionable because of production content, the Deputy Under Secretary of the Army will make the final determination.

15. Actions to adopt multimedia/VI productions of other U.S. Government agencies (non-DOD) for Army use will be coordinated and certified in the same manner as non-local multimedia/VI productions. (See paragraph 7–7*a*.)

16. Audio/video playback or broadcast equipment on which classified information will be transmitted must be installed in accordance with the provisions of AR 25–2 and Federal Standard 222.

a. Procedures for transmitting classified information are contained in AR 25–2 and AR 380–5.

b. Each classified video/audio recording will be identified at the beginning and end with the appropriate security classification.

c. Classified material containers will display labels with the appropriate security classification of the contents.

d. Each classified recording must be degaussed or destroyed, except when VI production (copies only, not masters) containing classified information has not been removed from the operational area or library. These copies may be destroyed without having a certificate of destruction prepared. A witness must be present to verify destruction.

17. Requests to translate or rescore new non-local multimedia/VI productions into a foreign language will be processed in the same manner as all other non-local productions. Requests for rescoring or translating of existing multimedia/VI productions will be approved by CIO/G–6 only if the requestor is responsible for all costs.

18. Productions cleared by Army Public Affairs will be offered for sale to the public and foreign Governments and nationals through the National Audiovisual Center (NAC). Requests for purchase information will be directed to the National Technical Information Service/NAC, 5285 Port Royal Road, Springfield, VA 22161.

19. All multimedia/VI productions will be validated by the functional proponent and cleared for public release prior to placement on a Web site for viewing or downloading.

20. Current authorized distribution format for official Army multimedia/VI productions primarily are DVD and Compact Disc-Read Only Memory (CD-ROM).

b. Video/audio documentation. Recordings of specific types of official events as they occur (for example, briefings, seminars, and Very Important Person visits) are authorized. Generally these recordings are not edited and are normally provided to the customer in their raw form or may be incorporated into a VI production. However, unusual and compelling situations may transpire where minor edits are needed. VI activities will discuss possible retention of these recordings as record material with the customer. (Also see paragraphs 7–9*c* and 7–11.)

(1) Images.

(a) Imaging, whether chemically, digitally, or manually produced, is a still or moving pictorial representation of a person, place, thing, idea, or concept, either real or abstract, to convey information. Graphic material used in multimedia/VI productions or video transmissions will adhere to the standard aspect ratio safe area in a horizontal delivery format.

(b) The alteration of official imagery by any means for any purposes other than to establish the image as the most accurate reproduction of a person, event, or object is prohibited. (Also see DODI 5040.5 and DA Pam 25–91.)

(c) Photographic and video postproduction enhancement (includes animation, digital simulation, graphics, and special effects used for dramatic or narrative effect in education, recruiting, safety and training illustrations, publications, or productions) is authorized under the following conditions:

1. The enhancement does not misrepresent the subject of the original image.

2. It is clearly and readily apparent from the context of the image or accompanying text that the enhanced image is not intended to be an accurate representation of any actual event.

(d) Use, duplication, and electronic alteration of commercially obtained electronic images will be in accordance with applicable copyrights and licenses.

(e) Only authorized VI activities may process official military personnel file photographs and electronically submit the DA Photograph Management Information System. (See also AR 640–30 and DA Pam 25–91.)

(2) *Video reports.* Recordings of official events as they occur (for example, meetings, conferences, seminars, workshops, lower level changes of command, parades, classroom instruction, and similar types of activities) are authorized. These reports may be enhanced through minor editing, titling, narration, and/or adding a music score prior to delivery to the customer. These types of reports will be accomplished as a low priority service.

c. Use of digitized text. life cycle management of multimedia products containing only digitized text is governed by printing and publications guidelines.

7–8. Services

a. Customer self-help. Visual information activities will provide customer self-help support for the production of simple products (for example, briefing charts, sign-out boards, flyers, or flip charts).

b. Consultation. Visual information activities will provide customer consultation services in support of official requirements for customer and professionally developed VI products and services.

c. Ready access file. Visual information activities will develop a consolidated electronic source of imagery that is accessible by official customers. CIO/G–6 and FOA VI managers will ensure that accessibility to this imagery is provided to the widest audience possible.

d. Presentation support services. When required, VI activities will provide or facilitate the provision of support to official events that require the setup, use, operation, and/or breakdown of VI equipment/systems. This includes events such as briefings, ceremonies, presentations, and so on.

e. Defense Automated Visual Information System. The Defense Automated Visual Information System (DAVIS) is a DOD-wide automated catalog system for management of VI products and interactive multimedia instruction (IMI) material (includes production, procurement, inventory, distribution, production status, and archival control of multimedia/VI productions and IMI materials). The DAVIS is accessible at Web site http://dodimagery.afis.osd.mil.

f. Broadcast services.

(1) *Cable television.* The VI activity will operate only the command channel(s) provided as part of the Cable television (CATV) franchise agreement. See chapter 6 of this regulation for CATV policy.

(2) *Closed Circuit Television.* The VI activity will operate installation Closed Circuit Television (CCTV) systems.

g. Media library services. Authorized VI activities may provide a central library (physical or digital) of distributed and local multimedia/VI productions and imagery.

7–9. Visual information records management

a. 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 per General Records Schedule 21, DODI 5040.6, this regulation, and DA Pam 25–91. For VI housekeeping files, refer to AR 25–400–2.

b. Activity VI managers will maintain a system for numbering individual product items based on DODI 5040.6 requirements. Still photographs, motion picture footage, video recordings (excluding those assigned a PAN or PIN), and audio recordings, if retained for future use, will be assigned a VI record identification number (VIRIN). A

description of the required VIRIN elements is provided in DA Pam 25–91. All VI material retained for future use will be captioned (DD Form 2537 (Visual Information Caption Sheet)) per procedures outlined in DA Pam 25–91. DD Form 2537 is available on the Army Publishing Division Web site.

c. For contractor-produced VI records, the contract will specify the Army's legal title and control of all such VI media and related documentation.

d. Because of their extreme vulnerability to damage, VI records will be handled in accordance with DODI 5040.6 and associated manuals.

e. Visual information managers will maintain continuous custody of permanent or unscheduled VI records prior to their retirement or submission for accessioning to the Joint Combat Camera Center (JCCC) or Defense Visual Information Center (DVIC).

f. If different versions of multimedia/VI productions (such as short and long versions, closed captioned, and foreign-language) are prepared, an unaltered copy of each version will be maintained and forwarded through the authorized JVISDA to the DVIC.

g. Visual information record documentation will be forwarded for accessioning daily or as soon as possible to the JCCC or DVIC.

h. Non-local multimedia/VI productions upon completion will be forwarded with their production folder to the JVISDA. Local multimedia/VI productions and their production folders selected for retention, as record material will also be forwarded to JVISDA for submission to the DVIC.

7–10. Visual information documentation program

Visual information documentation (VIDOC) provides a visual record of significant Army events and activities. This information is acquired for operational, training, and historical purposes (see 36 CFR 1232.1 and DODI 5040.6). OSD, CJCS, HQDA, and field commands use VIDOC information for C2, management presentations, and reports. Doctrinal, combat, materiel, and training developers use this material for analysis, reports, and briefings in support of their programs. Public affairs offices use their products to keep Army personnel informed and for release to the news media. The VIDOC program includes both tactical and nontactical documentation.

a. Tactical documentation. Record VIDOC is obtained by COMCAM teams during theater Army and Joint wartime operations, contingencies, exercises, or humanitarian operations. COMCAM teams will electronically forward imagery, with embedded captions, to the JCCC (jccc@hqda.afis.osd.mil) (703–693–5699/DSN 223–5699) for distribution to operational decision-makers and other customers via videotape, prints, or the Web site http://dodimagery.afis.osd.mil. COMCAM teams will provide original source material through the JCCC for accessioning into the DVIC. (See DA Pam 25–91.)

b. Non-tactical documentation.

(1) Non-tactical (infrastructure) documentation is record documentation of technical, operational, and historical events as they occur during peacetime. This documentation provides information about people, places, and things as well as processes in the fields of medicine, science, logistics, RDT&E, and other historical events. (See DA Pam 25–91.)

(2) All Army VI activities will participate in the Army Documentation Program by making daily, or as soon as possible, submissions of record VIDOC to the JCCC or DVIC for accessioning. The capturing and submission of record VIDOC will be considered high priority by all VI activities.

(3) Direct Reporting Units and local VI activities will submit historically significant VIDOC products directly to the CAP. Combat camera VIDOC products will be submitted through the JCCC for accessioning.

(4) Non-tactical record documentation includes linear and digital video, photographic imagery, graphic artwork (including recruiting and safety posters/artwork), or audiotape. To meet minimum submission requirements, VI activities will document and submit imagery of one or more of the following:

(a) Readiness posture of units.

(b) Significant military operations, campaigns, exercises, or maneuvers.

(c) Programs and projects that have an impact on national or Army policy and, therefore, must be retained.

(d) Significant events related to construction of major systems, facilities, and installations within theater of operations.

(e) Army participation in disaster relief, civil disturbances control environmental protection, and related subjects of national attention or significance.

(f) Construction of major systems, facilities, and installations.

(g) Depictions of the President of the United States or Family members.

(h) Significant military events, such as base closures/realignments, activation, deactivation, or deployment of a division or larger unit; a promotion to brigadier general or higher rank; a change of command of a division or larger unit; or the award of the Medal of Honor or other similar events.

(i) Outstanding examples of military life (for example, images of soldiers at work, using recently fielded items of

new equipment, in unusual or extreme climates, physical training, enjoying life as a military family, or other similar examples depicting today's Army).

c. Original VI material not meeting the above criteria will be destroyed by the VI activity no later than two years after the date of recording; earlier destruction is authorized.

d. Use of chain-of-command photographs is a command decision. Photographs of the President, Secretary of Defense, SECARMY, and the CSA may be obtained by local VI activities from JVISDA.

7–11. Restrictions and controls for visual information production and distribution

a. Recording events. Recording information by audio or videotape will be limited to official events or activities that are related to military missions and functions. Civilian activities and social events are not normally considered appropriate subjects for recordings. The DOIM and/or garrison commander must approve official requests for these types of recordings.

b. Use of multimedia/VI productions. Multimedia/VI productions will not be used to promote organizations and commands, promote sales of commercial products or private industries, influence pending legislation, or provide forums for opinions on broad subjects (see DODD 5040.3). Multimedia/VI production content will not be incompatible or inconsistent with Army policies or doctrine; discriminate against or stereotype individuals on the basis of gender, race, disability, creed, nationality, age, religion, national origin, or sexual orientation; or weaken or cast doubt on the credibility of the Army or DOD.

c. Prohibited recordings. Title 18 USC Chapter 25 prohibits the photo-optical and electronic recording of the items listed below. Offenders are subject to fines and/or punishment. All personnel assigned to make VI recordings will be informed of these restrictions. When in doubt of recording legality, the Regulatory and Intellectual Property Division, U.S. Army Legal Services Agency, will make final determination. Prohibited items include—

(1) Photographing money, genuine or counterfeit, foreign or domestic, or any portion thereof. However, such photography is authorized in black and white for philatelic, numismatic, educational, or historical purposes; for publicity in connection with sales and campaigns for U.S. Bonds; or for other newsworthy purposes (excludes advertising purposes) provided such photographs are less than three-quarters or more than one and one-half the size (in linear dimension) of the money photographed. The negatives (original recording material) and plates used must be destroyed after the final use. The term "money," for purposes of this regulation, refers to notes, drafts, bonds, certificates, uncancelled stamps, and monetary securities in any form (reference 31 CFR, Subtitle B, Chapter IV).

(2) Government transportation requests.

(3) Passport and immigration or citizenship documents.

(4) A badge or identification card prescribed by agencies of the U.S. Government for use by an officer or employee (18 USC 701).

(5) Selective service registration card.

(6) Foreign Government, bank, or corporation obligations.

(7) Property titles when regulated, restricted, or prohibited by the issuing state.

d. Copyright material. Recording and/or use of copyrighted material in the development of any VI product is prohibited by law (17 USC) without written permission from the copyright owner. Evidence of this consent will be maintained throughout the life cycle of the product. "Fair use" doctrine (for educational purposes) rarely applies to the military departments, and written permission will be obtained. Ownership or possession of copyrighted material does not constitute the permission to use or duplicate. When the copyright status is unclear, consult with the local VI manager or judge advocate general before proceeding. Prevention of copyright infringements is the responsibility of all individuals, and violators are subject to prosecution at all levels of involvement.

e. Modification of VI productions. The editing or modifying of any Army VI production, either in-house or by commercial contract, may have legal encumbrances that limit their use. Therefore, completed and distributed official productions or copies may not be cut or otherwise modified without prior approval by the functional proponent or CIO/G–6.

f. Broadcast recordings. Off-air public information broadcasts (audio or video) may be recorded by Army activities under the following conditions:

(1) The information will have an impact on the role of the Army in performing its mission.

(2) The Army organization that requires the information submits an official request for the program to be recorded.

(3) The information recorded will be destroyed 60 days after the recording unless the unit or installation commander determines that the information has permanent value. Permission of the copyright holder must be obtained in writing if the recording is held longer than 60 days. Commanders of units or activities that provide this recording service will ensure that:

(a) Excerpts are not edited or copied from the original recording.

(b) Recorded information is not presented out of context.

(c) Viewing audiences are limited to DOD personnel who require the information.

g. Use of recorded information. DOD personnel will not use recorded information as an instructional aid or for

general viewing, without the written permission of the copyright owner. If consent of the copyright owner cannot be obtained prior to use of the recorded information due to time constraints, written permission from copyright owner will be obtained prior to duplication or distribution. Off-air broadcasts may be recorded and used without permission of the copyright owner when the viewing of the recording is for the following purposes:

(1) Law enforcement investigations.

(2) National security investigations.

(3) Civil emergencies, when necessary to accomplish an Army mission.

h. Personnel and equipment.

(1) Army personnel on official VI assignments are not permitted to engage in VI recordings for personal retention or for any other purposes not directly related to official Army activities. This prohibition does not apply during off-duty status. If personally owned equipment or supplies (such as cameras, film, videotape, and graphic arts material) are used during an official assignment, either by choice or agreement, the images becomes Army recorded property and will be turned into an authorized VI activity. Army personnel on official assignments have no personal rights to sell or distribute this type of imagery.

(2) Government personnel will not perform VI assignments that subject them to health or safety hazards not normally encountered in their regular duties.

i. Releases. Releases are required for the use of personnel, equipment, property, and so on prior to their inclusion in motion media, audio and video recordings, drawings, electronic imagery, and other VI products. These releases will be required whether the product is for internal DOD use or release to the press, public, or individuals. For policies governing these releases, see DODI 5040.07, AR 25–55, AR 340–21, AR 380–5, DA Pam 25–91, and AR 360–1.

j. Disposition. Army VI products will not be withheld for personal purposes, or disposed of in any manner not covered in this regulation, without the written consent of an official who is authorized by law, regulation, or competent orders to permit such withholding, reproduction, or disposition.

k. Public exhibition clearance. The local PA or other designated representative at the lowest possible level will review all unclassified imagery for possible public release unless otherwise directed by Office of the Chief, Public Affairs or higher authority. All multimedia/VI productions will be reviewed for public exhibition by the PAO prior to distribution (see DODI 5040.07). VI products produced by the Army (whether in-house or by contract) and cleared for public exhibition become part of the public domain. These products, upon completion, will not have legal encumbrances such as copyright, patent, personal property, or performance restrictions. Any contract for the production of VI products requires that the contractor assign all interest in the work, to include copyright, to the Government.

(1) If the review reveals that legal encumbrances exist, the product will not be cleared for release until these encumbrances have been removed. Public clearance must be granted for any VI product (such as still or motion media productions, stock footage, or electronic images) prior to release to the public or placement on a Web site.

(2) Army productions that have been cleared for public release may be presented on AFRTS stations. Authorization for use of this material is the responsibility of the local AFRTS commander based on AFRTS regulations and criteria established for the host country involved through coordination with the U.S. Embassy. AFRTS stations will not broadcast any VI production not cleared for public release.

l. Legal reviews. All completed multimedia/VI production will be reviewed by the local judge advocate prior to distribution. Any U.S. civilian organization may borrow Army VI products that have been cleared for public exhibition. An official request from Army/DOD agencies for Army products has priority over civilian requests for the same product. Loans to U.S. civilian organizations are subject to the following conditions:

(1) Editing or cutting of Army VI products (productions or footage), in whole or in part, by or for organizations is prohibited. The borrower will be required to prepare and sign a letter of indemnification to the U.S. Army stating that they will not use (or authorize others to use) the subject products for any purposes other than as a public service. Civil penalties may be imposed for violating the FOIA (AR 25–55), and civil and criminal penalties may be imposed for violating the Privacy Act (AR 340–21).

(2) No admission fees or fees of any sort may be charged in connection with showing of the production or use of equipment.

(3) All production copies will be loaned for temporary periods and will have a specific return date.

(4) Failure to comply with the conditions listed above or to return the material in good condition will provide a basis to deny a subsequent loan of multimedia/VI productions to the individual or organization concerned.

Chapter 8
Records Management Policy

Note: Per DA General Order 2006–01, the records management function transferred from the DCS, G–1, to the AASA. Performance of the missions and functions will continue to be subject to the oversight of the CIO/G–6.

8–1. 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.

8–2. Management concept

a. The Federal Records Act (44 USC Chapter 31) requires the head of each Federal Agency to maintain a continuing program for the economical and efficient management of the records of the agency.

b. The Records Management Program.

(1) Establishes the most efficient, economical, and technologically advanced methods to ensure creation of only information essential for conducting operations and preserving that information as records.

(2) Establishes effective controls over the creation, organization, maintenance, use, and disposition of Army record information.

(3) Provides for the most expeditious and accurate distribution of record information at a minimum cost by applying advanced technology and eliminating all but essential processing procedures.

(4) Ensures that permanently valuable information is preserved and all other record information is retained, reviewed, and disposed of systematically. Refer to AR 25–400–2.

(5) Defines the records management policy for electronically stored Army information.

(6) Includes the following Records Management subprograms: Official Mail, Correspondence Management, Rulemaking, Office Symbols, Management Information Control Program, Abbreviations, Brevity Codes, Acronyms, and Compilation of Army Addresses.

c. Within the Federal Government, records are considered to be any of the following if they are made or received by any DA entity under Federal law or in connection with the transaction of public business and preserved— or are appropriate for preservation by DA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of DA or because of the informational value of the data in them:

(1) All documents, books, papers, maps, photographs, and graphic art.

(2) Record information stored on machine-readable media. These include magnetic media (for example hard disks, tapes, and/or diskettes), optical recording media (for example, laser disk, optical disk, optical card, optical tape, compact disc (CD), and/or DVD), all electronic formats (office automation software— for example, word processing, spreadsheet and/or presentation software), e-mail, Web sites, ISs, NSS, databases, and printouts .

(3) Record information stored on film slides, aperture cards, roll microfilm, microfiche, videotape, overhead transparencies, and motion picture films.

(4) Audio and video recordings (set forth in DODI 5040.6 and chap 7).

(5) Any other documentary materials regardless of physical form or characteristics.

d. The following are not included within the statutory definition of the word "record" per DOD 5400.7R and AR 25–55:

(1) Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference, and stocks of publications and processed documents. Extra copies of such materials should be kept to a minimum.

(2) Objects or articles — such as structures, furniture, paintings, sculptures, three-dimensional models, vehicles, and equipment — regardless of their historical value or value as evidence.

(3) Commercially exploitable resources, including but not limited to—

(a) Maps, charts, map compilation manuscripts, map research materials, and data, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA.

(b) Computer software, if not created or used as primary sources of information about organizations, policies, functions, decisions, or procedures of DA. This does not include the underlying data processed and produced by such software, which may in some instances be stored with the software.

(4) Unaltered publications and processed documents, such as regulations, manuals, maps, charts, and related geographical materials, which are available to the public through an established distribution system, with or without charges.

(5) Intangible information, such as an individual’s memory or oral communication.

(6) Personal records of an individual not subject to agency creation or retention requirements that are created and maintained primarily for the convenience of an agency employee and not distributed to other agency employees for their official use.

(7) Information stored within a computer for which there is no existing computer software program to extract the information or a printout of the information.

e. Records management officials duties—

(1) Army proponent records management duties are specified in paragraph 2–8 under AASA responsibilities.

(2) The Director, U.S. Army Records Management and Declassification Agency (RMDA) has operational responsibility for records management and its associated programs as defined in paragraph 8–5.

(3) ACOM, ASCC, and DRU RAs have command/unit-wide responsibilities for ensuring the creation and preservation of official mission records throughout subordinate units and activities. RAs will be appointed in writing and registered as an RA in the ARIMS (see Web site at https://www.arims.army.mil for registration instructions). Copies of written appointments will be sent to the U.S. Army Records Management and Declassification Agency, ATTN: AAHSRDRR, 7701 Telegraph Road, Room 102, Alexandria, VA 22315–3860. Aside from references included in AR 25–400–2, para 1–4; chapters 2 and 8 of this publication; and DA Pam 25–403, paras 1–6*a* and 6–4*e*, RAs must—

(a) Provide policy interpretation, procedural guidance, and oversight of mission-unique records management programs.

(b) Ensure availability of records management training for all command/unit personnel.

(c) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings.

(d) Advise staff and system development personnel on the requirement for integration of records management functions at the concept development stage and coordinate at each milestone.

(e) Ensure that records management requirements are documented and included in systems acquisition as appropriate.

(f) Keep abreast of and/or implement new IT for access storage, retrieval, and disposition of information.

(g) Ensure records management factors are considered for respective C4/IT acquisitions regardless of acquisition category.

(h) Ensure compliance with the DA FOIA Program, the Army Privacy Program, and EO 12958.

(i) Ensure compliance with and enforcement of DA policies and rules governing management of information requirements under the Management Information Control System.

(j) Maintain liaison with publication, forms, and reports management officials to achieve a minimum production in types and numbers of copies of documents and reports required.

(k) Provide technical assistance to the VI RMs as required.

(4) The FOA, staff support agency, separately authorized activity, and tenant and satellite organization RMs will—

(a) Be appointed in writing and registered as an RM in the Army Records Information Management System (ARIMS) (see Web site at para 8–2*e*(3) for registration instructions). Copies of written appointments will be sent to the address in para 8–2*e*(3). Aside from references included in AR 25–400–2, para 1–4, and DA Pam 25–403, para 1–6*b*, RMs must—

(b) When not served by an installation records holding area (RHA), index records to be turned in by the organization's offices into the ARIMS Records Input Processing Subsystem.

(c) Ensure availability of training for records management personnel.

(d) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings to the absolute minimum required.

(e) Provide technical assistance to VI RM.

(5) The IMCOM will provide program coordination to the regional records manager as required.

(6) Regional-level RM will

(a) Be appointed in writing and be registered as an RM in ARIMS (see Web site at https://www.arims.army.mil for registration instructions). Copies of written appointments will be sent to the U.S. Army RMDA address in para 8–2*e*(3).

(b) Provide functional management and oversight of the records management program and its subprograms for the installations in their respective regions in accordance with this regulation and AR 25–400–2, AR 25–55, AR 340–21, AR 25–50, AR 25–58, AR 335–15, AR 25–59, and AR 25–51.

(7) Installation level RMs serve on the installation staff and have installation-wide responsibilities. They will—

(a) Be appointed in writing and be registered as an RM in ARIMS. (See Web site above for registration instructions.) Copies of written appointments will be sent to the U.S. Army RMDA address in para 8–2*e*(3).

(b) Approve office record lists for sub-units.

(c) Serve as local authority for records management procedures/issues.

(d) Manage, oversee, and direct the installation records management program and its subprograms.

(e) Survey and appraise the installations records management program at least once every three years and prescribe and ensure that necessary corrective action is taken.

(f) Manage and provide staff direction for operation of the RHA to include

1. Ensuring that RHA managers (RHAMs) are designated for all established and approved RHAs and that they are registered as a RHAM in ARIMS. (See Web site at https://www.arims.army.mil for registration instructions.)

2. Ensuring that records are properly arranged and packed before movement from the RHA to a records center.

3. Maintaining liaison and coordinating the transfer, retirement, and retrieval of records with the Federal Records Centers and local National Archives and Records Administration (NARA) offices.

4. Indexing records turned in by installation offices and tenant offices into the ARIMS Records Input Processing System.

5. Ensuring that records management factors are considered for all installation level IT/C4 and intelligence acquisitions.

6. Ensuring availability of training for records management personnel.

7. Maintaining liaison with and providing advice and assistance to security managers in developing and executing a program to reduce classified records holding to the absolute minimum required.

8. Providing technical assistance to VI RMs as required.

9. Records coordinators will be designated at sub-elements as necessary for program execution and will be registered as RCs in ARIMS (see Web site at http://www.arims.army.mil for registration instructions). For more information on the function of RCs, reference DA Pam 25–403, para 1–6*c*.

10. Action officers at all levels of command create official records on behalf of the Army. The records management responsibilities of action officers are listed in DA Pam 25–403, para 1–6*c*.

8–3. Life cycle management of records

Aside from those mentioned in paras 1–1*e*, 3–4*a*, and 4–1*c*(3) of AR 25–400–2, the objectives in the life cycle management of records are as follows:

a. 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, chaps 5, 6, and 7, on how to maintain official records). Create only the minimum records essential and adequate to support, sustain, and document the following:

(1) Military operations in time of peace, war, and operations other than war (for example, contingency operations and humanitarian, peacekeeping, and nation building missions).

(2) The conduct of all other activities of the Army's official business.

b. Control the quantity and quality of records produced by the Army.

c. 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 prevent the creation of unnecessary records.

d. Simplify the activities, systems, and processes of record creation, maintenance, and use.

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

f. Establish and maintain such other systems or techniques as the Archivist of the United States, in consultation with the Archivist of the Army, finds necessary.

g. Employ modern technologies and cost effective alternatives for storage, retrieval, and use of records.

h. Ensure records are preserved in a manner and on media that meet all legal and archival requirements.

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

j. Ensure the periodic evaluation of the records management activities relating to the adequacy of documentation, maintenance and use, and records disposition, at all levels, through the IRM review process.

8–4. Tenets

In executing the mission, objectives, and associated programs, Army activities will conform to the following program tenets:

a. Simplify recordkeeping methods.

b. Minimize the burden on commanders, soldiers, and civilian and contractor personnel.

c. Establish proactive control over operational records.

d. Centralize record collection when deployed in theater.

e. Digitize once with multiple access.

f. Ensure appropriate command emphasis.

g. Incorporate records management requirements into training.

8–5. Major sub-programs

a. Army recordkeeping systems management. The objectives of Army recordkeeping systems management are to cost-effectively organize Army records stored on any medium so needed records can be found rapidly; to ensure that records are complete, accurate, authentic, reliable, and trustworthy; to facilitate the selection and retention of records of enduring value; and to accomplish the prompt disposition of unscheduled records in accordance with NARA-approved disposition schedules. RMDA is the only Army activity authorized to schedule the disposition of records with NARA. (See AR 25–400–2.)

(1) *Army Records Information Management System.* The ARIMS process sets forth the policy and procedures for the systematic identification, maintenance, retirement, and destruction of Army record information on any medium (paper,

microforms, electronic, or any other). It is the Army's enterprisewide system for capturing and maintaining long-term (over six years) electronic records. It provides for the establishment and operation of central and overseas command RHAs, and furnishes the only legal authority for destruction of nonpermanent Army records by organizational elements.

(2) *Systems Administrators.* Systems Administrators will ensure that e-mail and Web file servers are backed up for a period of time no less than 90 days in an off-site secure storage facility. This includes Web content on Army public and private Web sites. Backup tapes are to be used for security and contingency planning only and are not to be used for records retention purposes.

b. Official mail and distribution management. Official mail and distribution management provides rapid handling and accurate delivery of official mail throughout the Army at minimum cost. (See AR 25–51.)

c. Office symbols. The office symbol program provides policy for the use and construction of office symbols throughout DA and establishes a requirement that all DA office symbols be maintained on the RMDA Web site at https://www2.arims.army.mil/aao. (See AR 25–59.)

d. Correspondence management. The correspondence management program provides for the preparation and management of correspondence in a standardized, economical, and efficient manner. (See AR 25–50.)

e. Army Addresses. The Army Addresses program consists of a Web-based consolidated address listing of ACOMs, ASCCs, and DRUs. It includes office symbols and official mailing addresses and allows users to access and search the database for specific organizations and to submit requested changes to the address database electronically. Army addresses are located at https://www2.arims.army.mil/aao. (See DA Pam 25–50.)

f. Rulemaking. The rulemaking program satisfies the legal requirement for the Army to publish Army regulations or other issuances and notices that have a substantial and continuing impact on the public in the Federal Register (44 USC Chapter 15). (See AR 25–58).

g. Freedom of Information Act program management. The FOIA program implements the DOD policy that requires its activities to conduct business in an open manner and to provide the public a maximum amount of accurate and timely information concerning its activities, consistent with legitimate public and private interests of the American people. (See AR 25–55.)

h. Privacy Act Program management. The Privacy Act Program provides a comprehensive framework regulating how DA collects, maintains, uses, or disseminates personal information on individuals. The program provides balance between information requirements of the Department and privacy interests and concerns of the individual. (See AR 340–21 and DA Pam 25–51.)

i. Management Information Control Office. The HQDA Management Information Control Office (MICO) objectives are to establish policy, procedures, and standards for IM control and prescribe responsibilities for the management and control of external and internal Army information requirements. These objectives include interpreting and implementing existing Army reports control policy, statutes, and external guidance (OMB, GSA, and DOD); implementing Army information control policy goals and objectives; and assigning RCSs. The MICO will evaluate proposed, new, or revised public information requirements; prepare the Annual Information Collection Budget; and plan and coordinate periodic reviews of public information requirements. (See AR 335–15.)

j. Vital records. This program provides for the selection and protection of records required for the Army to conduct its business under other than normal operating conditions, to resume normal business afterward, and to identify and protect important records dealing with the legal and financial rights of the Army and persons directly affected by actions of the Army. It also provides policies and guidance for emergency preparedness, contingency planning, assessing damage, and implementing disaster recovery procedures. See DA Pam 25–403, para 2–4, for guidance on vital records.

(1) *Emergency operating records.* These are records essential to the continued functioning and reconstitution of an organization before, during, and after a national security emergency or under emergency or disaster conditions. These records include such groups as emergency plans and mobilization plans and programs. Reference AR 50–03; DA Pam 25–1–1, chapter 2; and DA Pam 25–403, paragraph 2–4*a*, for more information on emergency operating records. (See also para 6–1*b* of this publication.)

(2) *Rights and interests records.* These records include medical records, personnel action records, certain records from operational deployments, and other records delineated in DA Pam 25–403, para 2–4*b*.

k. Authorized abbreviations, brevity codes, and acronyms. This program prescribes authorized abbreviations, brevity codes and acronyms procedures for their use within the Army. Program objectives are to standardize abbreviations, brevity codes, and acronyms used within DOD and between DOD elements and NATO countries and to assist in reaching a mutual or common definition and meaning of terminology between DOD elements, and between DOD elements and NATO member countries. (See also AR 25–52.)

l. Management of records of defunct Army commands and organizations. This subprogram manages records from Army organizations that no longer exist. Such records are in the physical custody of a Federal Records Repository but are still under Army control until legal authority is transferred to the National Archives. Refer to DA Pam 25–403, paragraphs 2–9 and 9–5 for more information on managing records of a defunct command.

m. Oversight records administration of Joint/Multi-Service/DOD. These are records that have been transferred into a

Federal Records Repository and for which the DOD has designated the Army as executive agency for record administration until legal authority is transferred to the National Archives.

n. Archivist of the Army. The AASA is the Archivist of the Army and is responsible for the executive coordination and interface with the Archivist of the United States. The Army Archivist may delegate specific responsibilities for achieving the records management mission. The recipients of such delegation are effectively assistant archivists of the Army. The Archivist of the Army promotes cooperation with the Archivist of the United States in applying standards, procedures, techniques, and schedules designed to improve management of records, safeguard the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value. The Director, RMDA, takes final action to offer records to NARA.

o. Defense Visual Information Center. The DVIC is the only authorized VI record center for OSD and the military components. Official record material is submitted to the DVIC through the JVISDA or through the CAP. (See also para 7–10.)

p. Joint Services Records Research Center Program. The program meets current and future Army requirements by locating, analyzing, and extracting pertinent data from unit records created during U.S. military operations past and present. The program provides expertise in the identification and interpretation of pertinent U.S. Army combat unit records for the purpose of verifying the claims of veterans, supporting scientific and epidemiological studies, and creating and maintaining databases associated with the total military combat experience.

q. Army Declassification Activity. The Army Declassification Activity (ADA) oversees the Army's implementation of Section 3.3 (Automatic Declassification) of EO 12958 and is responsible for reviewing all 25-year old permanent historical Army records for declassification, exemption, exclusion, or referral to other federal agencies. It conducts other special declassification reviews and makes declassification decisions on records of defunct ACOMs and organizations.

8–6. General policies

a. Personal records pertain solely to an individual's private affairs (see DA Pam 25–403, para 2–3). 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. Back-channel 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.

b. A Government official may accumulate extra copies of records. When deposited in a recognized research institution, these reference files or by-name collections often serve the broader interests of historiography. 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, paragraph.

c. 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.

d. Records identified below may not be removed from the control of the Federal Government for personal retention or donation to any institution unless approval is obtained from the Archivist of the United States:

(1) The official record copy of any document.

(2) Security classified documents.

(3) Restricted data or formerly restricted data documents (AR 380–5).

(4) Diaries that contain official schedules of meetings, appointments, field trips, or other official activities. These are official records and will be so maintained.

(5) Copies of records containing information exempted from public release under the nine exemptions of the FOIA or the Privacy Act (PA).

(6) Any record, including any normally non-record copy, whose absence creates a gap in the files or impairs the logical sequence of essential documentation.

(7) Records required to transact the official business of the Army and any document that assists in the decision-making process.

e. Commanders and agency heads will safeguard official records and properly dispose of them per 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

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

(2) There are criminal penalties for the unlawful removal or destruction of Federal records and for 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.

(3) 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 their potential capture by the enemy is prejudicial to the interests of the U.S.. If emergency destruction is performed, the government official will compile a list of records and a list of records destroyed, their inclusive dates, and the date destroyed. This information will be forwarded through channels to the address provided in para 8–2*e*(3) as expeditiously as theater or operational conditions permit.

8–7. Record media

a. 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 for long-term records that best serve the operational needs of the Army and meet statutory scheduling requirements must be selected. These decisions are vital considerations in the design stage of information life cycle management.

b. Army records, regardless of media or format, must follow the disposition instructions identified in AR 25–400–2 and comply with the security requirements of AR 25–2. All electronic information generated by or contained in an IS or any office IT source or created during the conduct of electronic business/electronic commerce must be considered. This requirement applies to information contained in any enterprise information system, e-mail, command-unique systems, and systems maintained in the office environment. The retention schedules of records contained within ISs will be systematically established at Milestone A.

c. When other than paper is the record copy

(1) The medium selected must have the durability to meet the test of time established by the ARIMS RRSA, such as the retention period for information contained in the system, individual microform or database. AR 25–400–2 provides policy for the systematic identification, maintenance, retirement, and destruction of Army record information. The longest retention schedule will apply where more than one ARIMS files series in contained in the record, systems of records, or database. Electronic records management automated ISs will comply with DOD 5015.2 STD.

(2) Digital Rights Management (DRM) restrictions such as those that assign rights to future users to take subsequent actions on protected content (for example, opening, printing, editing, copying, or forwarding the content) will not be used on Army records and systems. As part of the transfer process, ARIMS will routinely scan records during their transfer for DRM protected content. If such content is encountered, the records will be rejected and returned to the originating organization for removal of the DRM protected content. Additionally, permanent records of DA (and all other Federal agencies) containing DRM protected content are not acceptable for deposit in the National Archives.

(3) The ability to retrieve record information economically and efficiently must be maintained for the length of time that the information remains in the Army's legal custody. Army records retired to Federal Records Centers remain in Army legal custody even though they are in the physical custody of NARA. Formal accessioning into the National Archives of the U.S., however, transfers legal custody from the Army to the Archivist of the United States.

(4) Federal Records Centers have storage facilities for records stored in machine-readable and microform media; however, they do not possess servicing capability. The retiring activity for servicing, testing, manipulation, or data processing must be able to retrieve records in these media.

(5) Information retained as the record copy on other than paper must meet all legal requirements imposed on the records of the Federal Government and must adequately protect the rights and interests of the Army and any individual members, Family members, employees, or citizens that it affects.

(6) Visual information original materials are retained in their original format.

(7) When the record copy from an IS is converted to a microform document, the longest retention of any ARIMS record series contained in the microform will determine the technical specifications of the film to be used.

d. The Archivist of the United States has proprietary interest in the permanent records of DA (and all other Federal agencies). This covers the entire life cycle from creation until eventual deposit in the National Archives. This proprietary interest includes both the informational contents of the records and the recording and storage media.

(1) Prior to converting a permanent series of records to microform, a specific determination must be solicited from the Archivist of the United States. In some instances, the filmed documents are not acceptable for deposit in the National Archives, and the original media must be provided.

(2) Agencies may use optical media for storage and retrieval of permanent records while the records remain in an agency's legal custody. However, permanent records may not be destroyed after copying onto optical media without NARA's approval. Requests should be sent to the RMDA address at para 8–2*e*(3).

e. Due to personal health risks, agencies will not destroy optical media (CDs or DVDs) by burning, pulverizing, or shredding. Optical media will be stored pending development of final disposition instructions. If the volume of stored optical media becomes a storage or security concern, the manufacturer should be contacted to seek assurance that the

product does not contain toxic substances. With manufacturer assurance relating to specific disk products, excess optical media may be smelted.

f. Visual information digital still and motion images are excluded from this paragraph. Visual information products are managed under the provisions of DODI 5040.6, chapter 7 of this regulation, and DA Pam 25–91.

Chapter 9
Publications and Printing

9–1. Management concept

The AASA is the functional proponent for the policy, management, and execution of the APP. The APP consists of the major subprograms for managing publishing, printing, and forms. Major subprograms of the APP and related policies and responsibilities are described in AR 25–30. The APP—

a. Includes all levels of publishing (including printing and duplicating) in the Army.

b. Provides support for creating, preparing, coordinating, printing, distributing, and managing publications.

c. Provides support for maximizing the use of electronic publishing and electronic forms.

9–2. Central configuration 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.

a. Electronic publishing support includes the following:

(1) Maintaining the Army Continuous Acquisition and Lifecycle Support (CALS) Standard Generalized Markup Language (SGML) Registry and the Army CALS SGML Library.

(2) Maintaining the central official online repository for administrative publications, forms, and publications index at http://www.apd.army.mil and on AKO/DKO. The repository also contains hyperlinks to the official publication Web sites for departmental publications other than administrative.

(3) Ensuring that electronic publications maintained in the central official online repository are DISR-compliant.

b. APD manages the two official Web sites for Armywide administrative publications and forms. Those activities desiring to provide Internet access to departmental publications and forms on a Web site must establish electronic links to the approved official publications and forms as listed in the official repository instead of publishing a duplicate publication.

c. HQDA proponents and Army commands will staff unclassified draft publications and forms electronically by posting to AKO/DKO or AKO-S. E-mail notifications will include the link to AKO/DKO instead of attaching files for review. Access to draft documents on a Web site must be limited to those activities involved in the staffing and review of the publication or form. Draft publications will not be displayed on public access Web sites.

d. Draft publications are for information and planning purposes only and will not be used for implementation or compliance. Proponents will include the words "DRAFT – NOT FOR IMPLEMENTATION" across the top of each page of the draft (including electronic drafts).

9–3. Statutory restrictions for publications

Refer to AR 25–30, paragraph 2–1 for policy on restrictions in publishing, printing, and distribution of materials.

9–4. Statutory requirements for printing

All printing and duplicating work is subject to statutory requirements. AR 25–30 prescribes these requirements, including those governing the following special areas:

a. Propriety of material.

b. Product configuration.

c. Requirements for certifications.

d. Printing of items such as classbooks and yearbooks, calling and business cards, invitations, personalized items, official telephone directories, calendars, and newspapers.

e. Advertising.

f. Printing requirements included in contracts for equipment and services or in grants.

g. Initial publication by private publishers.

h. Recognition of agencies or individuals.

i. Reproduction of items such as licenses; certificates of citizenship or naturalization; U.S. Government or foreign Government obligations, certificates, currency, passports, bonds, and the like; certificates of deposit, coupons, and such; and official badges, identification cards, or insignia.

j. Use of color and illustrations.

k. Copyrighted materials.

9–5. Requisitioning printing

a. All Army printing and duplicating (including CD-ROM replication) will be prescribed in accordance with policies in AR 25–30, chapter 7, section III.

b. When determining whether in-house or commercial resources will be used, effectiveness and economic printing options will be considered in accomplishing mission objectives.

c. 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.

d. 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.

Appendix A
Reference

Section I
Required Publications

AR 25–2
Information Assurance (Cited in paras 1–7*b*, 1–8*c*, 2–15*g*, 2–25*a*, 4–9*h*, 5–1, 5–2, 5–2*b*, 5–3*d*, 5–4*c*, 5–6*c*, 5–7, 6–1*g*, 6–1*i*, 6–4*q*, 6–4*u*, 6–4*z*, 7–7*a*.)

AR 25–30
The Army Publishing Program (Cited in paras 7–6*a*, 9–1, 9–3, 9–4, 9–5*a*.)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in paras 1–7*b*, 7–11*i*, 7–11*l*, 8–2*d*, 8–2*e*, 8–5*g*.)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in paras 2–12*f*, 2–16*g*, 6–4*m*, 6–7*d*, 7–9*a*, 8–2*b*, 8–2*e*, 8–3, 8–3*a*, 8–5*a*, 8–6*e*, 8–7*a*, 8–7*c*.)

AR 70–1
Army Acquisition Policy (Cited in paras 2–6, 2–15*c*, 3–2*b*, 3–8*a*, 3–8*b*, 3–8*c*, 6–1*n*, 6–5*g*, 7–2*g*.)

AR 71–9
Materiel Requirements (Cited in paras 2–15*c*, 3–5*f*, 3–6*a*, 3–7*d*, 6–5*g*, 7–2*g*.)

AR 73–1
Test and Evaluation Policy (Cited in paras 3–8*d*, 6–5*g*.)

AR 215–1
Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities (Cited in paras 6–1*n*, 6–4*o*, 6–4*s*, 6–4*dd*.)

AR 215–4
Nonappropriated Fund Contracting (Cited in paras 6–1*n*, 6–4*o*, 6–4*s*.)

AR 340–21
The Army Privacy Program (Cited in paras 1–7*b*, 7–11*i*, 7–11*l*, 8–2*e*, 8–5*h*, 8–6*e*.)

AR 360–1
The Army Public Affairs Program (Cited in para 6–4*s*.)

AR 380–53
Information Systems Security Monitoring (Cited in para 6–4*q*.)

DA Pam 25–1–1
Information Technology Support and Services (Cited in paras 1–8*b*, 1–9, 1–12*b*, 2–2*a*, 2–15*h*, 3–2*a*, 3–3*a*, 3–3*d*, 3–7*j*, 3–10, 3–11*a*, 4–1*f*, 4–3, 5–10, 6–1*a*, 6–1*d*, 6–1*i*, 6–1*k*, 6–1*o*, 6–1*p*, 6–1*q*, 6–2*a*, 6–2*b*, 6–2*c*, 6–2*d*, 6–2*i*, 6–2*j*, 6–3*a*, 6–4*c*, 6–4*e*, 6–4*g*, 6–4*m*, 6–4*p*, 6–4*r*, 6–4*cc*, 6–5, 6–5*d*, 6–6*a*, 6–6*c*, 6–6*g*, 6–6*h*, 6–6*j*, 6–7*c*, 6–8, 8–5*j*.)

DA Pam 25–91
Visual Information Procedures (Cited in paras 7–5*e*, 7–6*d*, 7–6*f*, 7–7*a*, 7–7*b*, 7–9*a*, 7–9*b*, 7–10*a*, 7–10*b*, 7–11*i*, 8–7*f*.)

DOD 5500.7–R
Joint Ethics Regulation (JER) (Available at http://www.dtic.mil/whs/directives.) (Cited in para 1–8*c*.)

DODD 8115.1
Information Technology Portfolio Management (Cited in paras 3–3, 3–3*a*(3).)

DODI 1015.14
Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources (Available at http://dtic.mil/whs/directives.) (Cited in para 6–1*n*.)

DODI 5000.2
Base and Long-Haul Telecommunications Equipment and Services (Cited in para 6–6*a*(1).)

DODI 5040.02
Visual Information (VI) (Cited in paras 7–1, 7–6*d*(1), 7–11*b*.)

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.

AR 5–11
Management of Army Models and Simulations

AR 5–12
Army management of the Electromagnetic Spectrum

AR 5–20
Commercial Activities Program

AR 5–22
The Army Proponent System

AR 12–8
Operations and Procedures

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 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 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–40 (O)
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (U)

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

AR 381–14 (C)
Technical Counterintelligence (TCI) (U)

AR 500–3
Army Continuity of Operations (COOP) Program

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 Personnel Files

AR 700–127
Integrated Logistics Support

AR 700–131
Loan and Lease of Army Material

AR 700–142
Materiel Release, Fielding, and Transfer

AR 710–2
Supply Policy Below the National Level

AR 735–5
Policies and Procedures for Property Accountability

AR 750–1
Army Materiel Maintenance Policy

ACP 123(A)
Common Messaging Strategy and Procedures (Available at http://www.jcs.mil/j6/cceb/acps/Acp123a.pdf.)

ACP 127 US Suppl–1 (J)
Communication InstructionsTape Relay Procedures (Available at http://www.jcs.mil/j6/cceb/acps/ACP127USSUP1J.pdf.)

Chairman, JCS (CJCS) Instruction (CJCSI) 3170.01
Joint Capabilities Integration and Development System

CJCSI 6110.01
CJCS-Controlled Tactical Communications Assets

CJCSI 6212.01
Interoperability and Supportability of Information Technology and National Security Systems

CJCSI 6215.01
Policy for DoD Voice Networks with Real Time Services (RTS)

CJCSI 6250.01
Satellite Communications

CTA 50–909
Field and Garrison Furnishings and Equipment

DA General Order 2002–03
Assignment of Functions and Responsibilities within Headquarters, Department of the Army

DA PAM 25–30
Consolidated Index of Army Publications and Blank Forms

DA PAM 25–40
Army Publishing: Action Officers Guide

DA PAM 25–50
Compilation of Army Addresses

DA PAM 25–51
The Army Privacy Program-System of Records Notices and Exemption Rules

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

DCID 6/3
Protecting Sensitive Compartmented Information Within Information Systems. (Available at http://www.us.army.mil/portal/portal_home.jhtml.)

Defense Message System GENSER Message Security Classification, Categories, and Marking Phrase Requirements
(Available at http://www.fas.org/sgp/othergov/dod/genser.pdf.)

Defense Supplement to the Federal Acquisition Regulations Subpart 208.74
Enterprise Software Agreements (Available at http://www.acq.osd.mil/dpap/dfars/index.htm.)

Defense Finance and Accounting Service – Indianapolis Regulation 37–1
Finance and Accounting Policy Implementation (Available at http://www.asafm.army.mil/budget/di/di.asp.)

DISAC 310–130–1
Submission of Telecommunications Service Requests (Available at Web site https://www.disadirect.disa.mil/products/ejad/310-130-5/dc3101305.asp.)

DFAS–IN Manual 37–100–FY
Army Management Structure (AMS) (Available at https://dfas4dod.dfas.mil.)

DOD 4160.21–M
Defense Materiel Disposition Manual

DOD 5015.2–STD
Design Criteria Standard for Electronic Records Management Software Applications

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) (Information Technology/National Security Systems)

DODD 1015.2
Military Morale, Welfare, and Recreation (MWR)

DODD 1035.1
Telework Policy for Department of Defense

DODD 3020.26
Defense Continuity Programs

DODD 4630.5
Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

DODD 4640.7
DOD Telecommunications System (DTS) in the National Capital Region (NCR)

DODD 4640.13
Management of Base and Long-Haul Telecommunications Equipment and Services

DODD5040.3
DOD Joint Visual Information Services

DODD 5230.9
Clearance of DOD Information for Public Release

DODD 5400.11
DOD Privacy Program

DODD 8000.01
Management of DOD Information Resources and Information Technology

DODD 8500.01
Information Assurance (IA)

DODI 1000.15
Private Organizations on DOD Installations

DODI 1015.12
Lodging Program Resource Management

DODI 4000.19
Interservice and Intragovernmental Support

DODI 4630.8
Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) (Cited in para 4–2.)

DODI 4640.14
Base and Long-Haul Telecommunications Equipment and Services

DODI 5040.4
Joint Combat Camera (COMCAM) Program.

DODI 5040.5
Alteration of Official DOD Imagery

DODI 5040.6
Life-Cycle Management of DOD Visual Information (VI)

DODI 5040.07
Visual Information (VI) Production Procedures

DODI 5335.1
Telecommunications Services in the National Capital Region (NCR)

DODI 8100.03
Department of Defense (DOD) Voice Networks

DODI 8410.01
Internet Domain Name Use and Approval

DODI 8510.1
DOD Information Assurance Certification and Accreditation Process (DIACAP) (Available at http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf)

DODI 8551.1
Ports, Protocols, and Services (PPSM)

DODI 8560.01
Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing

DRMS Instruction 4160.14, Volume IV
Policy and Procedures In Disposal Operations for Property Accounting (Available at http://www.drms.dla.mil/publications/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

Federal Acquisition Regulation
Government Printing and Binding Regulations (Available at http://www.arnet.gov/far/)

FM 6–02–40
Visual Information Operations

General Records Schedule 21
Audiovisual Records, Transmittal No. 8, December 1998 (Available at http://www.archives.gov/records-mgmt/index.html.)

Homeland Security Presidential Directive/HSPD 12
Policy for a Common Identification Standard for Federal Employees and Contractors

Joint Publication 1–02
Department of Defense Dictionary of Military and Associated Terms (Available at http://www.dtic.mil/doctrine/s_index.html.)

Joint Travel Regulations
(Available at http://secureapp2.hqda.pentagon.mil/perdiem/.)

OMB Cir A–11
Preparation, Submission, and Execution of the Budget (Available at http://www.whitehouse.gov/omb/circulars/index.html.)

OMB Cir A–76
Performance of Commercial Activities (Available at http://www.whitehouse.gov/omb/circulars/index.html.)

OMB Cir A–130
Management of Federal Information Resources

P.L. 107–314
Bob Stump National Defense Authorization Act for Fiscal Section Year 2003

SB 700–20 (EM 0007 FEDLOG)
Army Adopted/Other Items Selected for Authorizations/List of Reportable Items (Available at https://liw.logsa.army.mil/.)

36 CFR Chapter 7
Chapter 7, Library of Congress (Available at http://www.gpoaccess.gov/cfr/index.html.)

5 USC 552
Freedom of Information Act (Available at http://www.gpoaccess.gov/uscode/index.html.)

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/bss/.)

5 USC 552a
The Privacy Act

10 USC 1588(f)
Authority to accept certain voluntary services

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 Chapter 96 (P.L. 106–229
Electronic Signatures in Global and National Commerce Act (also known as the "E-Sign Act")

17 USC 101, 501
Copyrights

18 USC 701
Official Badges, Identification Cards, Other Insignia

29 USC 794d (Section 508 of the Rehabilitation Act Amendments of 1998, as amended by Section 2405 of the FY 2001 Military Appropriations Act (P.L. 105–220) (Available at http://www.gpoaccess.gov/uscode/index.html.))
Electronic and Information Technology

40 USC 762 (P.L. 100–542
Telecommunications Accessibility Enhancement Act of 1988

Title 40 USC Subtitle III (Clinger–Cohen Act (CCA))
Information Technology Management

44 USC, Chapter 15
Federal Register and Code of Federal Regulations (http://www.archives.gov/about/laws/cfr.html.)

44 USC, Chapters 29, 31, and 33 (Federal Records Management Act and Amendments)
Federal Records Management

44 USC, Chapter 35 (Paperwork Reduction Act and Amendments)
Coordination of Federal Information Policy

44 USC, Chapter 36 (Management and Promotion of Electronic Government (E–Gov) Services Act)
Management and Promotion of Electronic Government Services

47 USC, Chapter 5 Section 225
Telecommunications services for hearing-impaired and speech-impaired individuals

47 USC, Chapter 5, Section 611
Closed-captioning of public service announcements

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

Section III

Except where otherwise indicated below, the following forms are available as follows: DA forms are available on the AEL CD-ROM (EM 0001) and the APD Web site (http://www.apd.army.mil); DD forms are available from the OSD Web site (http://www.dior.whs.mil); and SF forms are available from the GSA Web site (http://www.gsa.gov).

DA Form 3903
Multi-media/Visual Information Work Order (Prescribed in para 7–4*f*)

DA Form 4103
Visual Information Product Loan Order (Prescribed in para 7–4*f*)

DA Form 5695
Information Management Requirement/Project Document (Prescribed in para 7–6*d*(1))

DA Form 5697
Army Visual Information Activity Authorization Record (Prescribed in para 7–3*d*)

DD Form 1367
Commercial Communications Work Order (Prescribed in para 6–4*c*)

DD Form 1995
Visual Information (VI) Production Request and Report (Prescribed in paras 7–3*c* and 7–7*a*)

DD Form 2537
Visual Information Caption Sheet (Prescribed in para 7–9*b*)

DD Form 2858
Visual Information Facilities (Prescribed in para 7–3*d*)

SF 258
Agreement to Transfer Records to the National Archives of the United States (Prescribed in para 8–5*l*)

Section IV
Referenced Forms

DA Form 11–2–R
Management Control Evaluation Certification Statement

DD Form 1391
FY ____ Military Construction Project Data

Appendix B
Telecommunications Services Authorized for Specific Activities

B–1. U.S. Army National Guard
Installation voice and data services may be provided to off-post U.S. Army National Guard (ARNG) units, activities, and detachments on a reimbursable basis with funding from the ARNG. On-post voice and data services to ARNG units, activities, and detachments will be provided as common use IT services with funding provided per the current Army reimbursement policy for common use IT services. (See ASA(FM&C) Web site: http://www.asafm.army.mil/pubs/pubs.asp.)

B–2. U.S. Army Reserve
Installation voice and data services may be provided to on-post and off-post U.S. Army Reserve (USAR) units and activities on a reimbursable basis with funding from the USAR. When such services are provided, funding will be in accordance with the current Army reimbursement policy for common use IT services. (See ASA(FM&C) Web site: http://www.asafm.army.mil/pubs/pubs.asp.)

B–3. Reserve Officer Training Corps
Local voice and data services for senior and junior Reserve Officer Training Corps (ROTC) detachments are normally provided by the supported educational institution. Services beyond those provided by the educational institution may be provided by the supporting DOIM on a reimbursable basis. The requesting ROTC detachments are responsible for ensuring that funding is available through their chain of command. All available services, including Networx and equivalent service, should be considered prior to approving commercial service.

B–4. Army Morale, Welfare, and Recreation programs and Nonappropriated activities
The Army policy for providing telecommunications services to Army MWR operations is defined within AR 215–1. Official electronic communications services to include telephone (Class A–2), network services, VTC, NIPRNet, and Internet are authorized when used for executive control and essential command supervision (ECECS) and C2/management functions. Access to other data services may be provided if the capacity exists and it does not inhibit Army C2 functions. If the existing telecommunications and network systems do not have the capacity to allow MWR traffic, RCIOs and DOIMs will include it in future system upgrades.

a. All MWR directly-operated activities will be provided Class A–2 telephone service and data transfer services, such as administrative, sales, and service within the confines of this paragraph.

b. Morale, Welfare, Recreation commercially-contracted concessions will use commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

B–5. Defense Commissary Agency
Official common user telephone and data services are authorized for use by commissary store activities when essential

to commissary management. Management functions include statistical data gathering and reporting, personnel management, official telecommunications with other Army installations and Government agencies, and procuring contractual services.

a. Class A–3 and C telephone services are provided to CONUS commissary officers, their assistants, and administrative control sections.

b. Class A–4 telephone service is authorized for use by cashiers for the purpose of official telecommunications with the local banking facilities for check collection.

c. Class A–4 telephone service is installed in locations where only cashier personnel have access to the service.

d. Class C telephone service is authorized for managers of meat departments, produce departments, grocery departments, warehouses, and associated commissary annexes. This service is provided on a reimbursable basis only in the office of the department warehouse and annex managers.

e. At installations where the commissary officer is not authorized to contract for voice and data service, the DOIM may provide support for the requirement. In such cases, a host/tenant agreement is executed. Depending on the source of reimbursement, this agreement may be between the DOIM and the commissary officer or the area commissary field director.

f. Official common user communications services are authorized on a nonreimbursable basis for use by commissary stores overseas, including Alaska, Puerto Rico, and Hawaii.

g. If the existing telecommunications and network systems do not have the capacity or would otherwise be adversely impacted by DeCA traffic, ACOMs and DOIMs will plan to accommodate such traffic in future system upgrades or otherwise provide right-of-way access and support for the separate acquisition of commercial voice and data telecommunications services for DeCA facilities.

B–6. Army and Air Force Exchange Service

Army and Air Force Exchange Service (AAFES) HQ, exchange regions, area exchanges, exchange managers, main store managers, and military clothing sales store operations will be authorized Class A–2 official telephone service in CONUS and OCONUS on a nonreimbursable basis for official business (that is, command management functions). Access to commercial circuits for the conduct of AAFES business will be on a reimbursable basis at Government rates whenever possible. Access to data services, networks, or cable plant will be provided by the installation to accomplish command management functions that require data transfer. These services are on an as-needed basis, provided the capacity exists and it does not inhibit Army C2 functions. All AAFES directly operated activities are authorized Class C telephone service and data transfer services, such as administrative, sales, and service within the confines of this paragraph. AAFES' commercially-contracted concessions will use commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

B–7. Contractors

a. Contractors providing resale services related to NAFI operations will use commercial telephone service when available. Class B service may be provided if commercial service is not available. Contractors normally will be provided only proximity access to intra-post Class C service necessary for coordinating local support and for fire and safety reasons. Contractors normally will not be provided access to data services and networks for the conduct of official business unless stipulated as a provision of their contract.

b. Contractors providing APF type of support may receive official telephone service. The contracting officer determines if such service is advantageous to the Government and is mission essential. Authorized service must be specified in the contract as Government furnished.

c. When official telephone service is authorized, Class A and/or Class C service may be provided, as determined by the DOIM, contracting officer, or contracting officer's representative for specific contracts. DOIMs will charge the contractor public tariff rates for supplemental services. These services include facilities such as key equipment, special switchboards, private lines, and FX lines for the exclusive use of the contractor. In the absence of tariff rates, or excessive rates, the installation commander determines equitable charges based on the actual cost of providing the services.

d. When the Army furnishes long-distance service from Class B–2 telephones to contractors on a reimbursable basis, the contractor will pay all actual charges and all taxes. Army activities do not provide official Government telephone calling cards to contractors. The procedures for authorizing, controlling, and recording long-distance service also apply to official collect telephone calls that contractor personnel place or receive.

e. The agency funding the contract reimburses the host installation for telephone charges that the contractor incurs. CJCSI 6215.01 provides guidance on when U.S. civilian contractor personnel can use the DSN.

B–8. Field operating activities/Direct Reporting Units

Field operating activities (FOAs) and Direct Reporting Units (DRUs) located on an Army installation, or stationed nearby with agreement, may be provided the following telephone services:

a. Class A–1 service, when performing a military function, to include medical.

b. Class A–2 service, when performing a civil works function.

c. A mix of Class A–1 and A–2 service when performing both a military and civil works function. The mix of service type is mutually determined at the local level.

d. Access to data services and networks is provided when the capacity exists and it does not inhibit Army C2 functions already on the network.

B–9. Department of Defense Dependent Schools

Provide Class A–2 and Class C telephone service to Government-operated school facilities for military Family members on an Army installation. Access to other voice and data services is dependent upon local agreements.

B–10. American Red Cross

Provide official voice and data service without reimbursement if ARC personnel supplement MWR functions. The ARC must use separate, unofficial voice and data service to conduct unofficial business.

B–11. Army lodging temporary duty facilities

The Comptroller General has ruled, "Where sufficient official need exists for a telephone not in private quarters, appropriated funds may be used, regardless of the incidental personal benefit to the occupant." (See also DODI 1015.12, enclosure 4.) Therefore, the following guidelines are provided for official telephone service in Army transient facilities. RCIOs/DOIMs will—

a. Set controls to ensure that the Army does not pay for unofficial or personal toll calls with appropriated funds, establish controls through system hardware and software configurations if possible, and set up direct toll billing procedures for transient residents.

b. Authorize direct access from transient billets to DSN and the local calling area, when necessary. Appropriated funds must not be used to pay message unit charges accrued for unofficial or personal individual calls to the local area.

c. Implement the requirements detailed in the Telephone Operator Consumer Service Improvement Act (47 USC 226).

B–12. Official telephone service for hospitalized active duty military personnel

A hospital room is the duty location for hospitalized personnel. If capacity exists in the installation telephone infrastructure, Class C telephone service must be provided. The installation DOIM has authority to approve a higher class of service or special features.

B–13. Private telephone service for hospital patients

Upon request, the hospital administrator will coordinate infrastructure with the installation DOIM for the local telephone company to provide private unofficial telephone service to hospital patients. A contractual agreement for commercial service is solely between the patient and the commercial company providing the service. Local telephone companies will reimburse the installation DOIM for any infrastructure used to support private unofficial telephone service to patients. When the Government provides Class B service, the patient must pay the recurring cost plus the cost of individual toll calls.

B–14. Nonprofit organizations

The commander or appropriate DA civilian supervisor who is the head of an organization within an Army component may authorize support to certain nonprofit organizations in a manner consistent with the provisions of DOD 5500.7-R. Nonprofit organizations do not pay service charges for Class A or C telephone service on an Army installation when performing a function related to, or furthering, a Federal Government objective or one that is in the interest of public health and welfare. Nonprofit organizations will reimburse the installation for all long-distance telephone services. DSN access will not be authorized. Access to data services and networks may be furnished provided the capacity exists and it does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

B–15. Government employee labor unions

Class B–2 rates for telephone service apply to government employee labor unions. Only reimbursable long-distance telephone services may be provided. Labor unions are not authorized DSN access. However, access to these and other voice and data services is dependent upon local collective bargaining agreements.

B–16. Public schools

Public schools normally use commercial voice and data service on Army installations. If commercial service is unavailable, the school reimburses the Government for the cost of Class B services. Access to data services and networks may be furnished provided the capacity exists and it does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

B–17. Civilian post offices on military installations

Reimbursable voice and data service will be provided to on-base civilian post offices, branches, or stations when requested. The extent of services is dependent upon local agreements.

B–18. Soldiers in the barracks

All private telephone service for Soldiers in the barracks will be through the AAFES contract. Other organizations are not authorized to establish telephone service for Soldiers in the barracks. Access to other voice and data services is dependent upon local agreements.

B–19. Army Community Service Volunteers and Army family support groups

Army Community Service (ACS) volunteers and Army Family support groups are authorized to place calls or use e-mail using official Government communications networks (for example, DSN and Networx) through local operations centers or installation telephone operators as long as such communications support the APF command support functions. Refer to AR 25–2 for requirements on access to computer systems. Access to data services and networks may be furnished provided the capacity exists and does not reduce the effectiveness of security or operational functions of the network. The extent of services will be based upon local agreements.

Appendix C
Management Control Evaluation Checklist

C–1. Function

The functions covered by this checklist are the administration of Army IM/IT organizations. They include 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, and installations in evaluating the key management controls outlined below; it is not intended to cover all controls.

C–3. Instructions

Answers must be based on the actual testing of management 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 management 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–R (Management Control Evaluation Certification Statement).

C–4. Test questions

a. Responsibilities (chap 2). Have C4/IT plans, programs, and requirements been coordinated with the appropriate IM/IT managers? (All)

b. Chief of Information Office (CIO) 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, DRU)

(2) Has the installation clearly established a DOIM who has the sole responsibility of implementing the installation's IM/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, DRU)

(4) Does the organization have a strategic plan that is linked to its mission? Is it periodically updated? (ACOM, ASCC, DRU)

(5) Has a forum been established to develop and implement C4/IT procedures, requirements, and priorities? (ASCC, DRU)

(6) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (HQDA, ACOM, ASCC, 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, DRU)

(8) Does the process support core/priority mission functions? (HQDA, ACOM, ASCC, DRU, FOA)

(9) Can the process be eliminated? (HQDA, ACOM, ASCC, 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, 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, DRU)

(12) Are exceptions to the IT investment screening process clearly documented? (HQDA, ACOM, ASCC, 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, DRU)

(14) Are IT investment decisions made a part of the organization's integrated capital planning process or are IT projects separated out? (HQDA, ACOM, ASCC, DRU)

(15) Does the organization have a process in place to conduct periodic reviews (inhouse or via outside consultant/expert) of its current IT investment portfolio to assess alignment with mission needs, priorities, strategic direction, or major process reengineering? (HQDA, ACOM, ASCC, DRU)

(16) Does the organization have a process for documenting and disseminating results of this review? (HQDA, ACOM, ASCC, DRU)

(17) Are process analysis and improvements for warfighter processes documented in the initial capabilities document using the DOTMLPF requirements methodology as defined by the Army requirements generation process in AR 71–9? (HQDA, ACOM, ASCC, DRU)

(18) Have webification status and future webification 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 organizational mission before execution of that investment? (HQDA, ACOM, ASCC, DRU, PEO, PM)

(21) Have IT investments been synchronized to overall DOD/Army mission priorities? (HQDA, ACOM, ASCC, DRU, PEO, PM)

(22) Are performance measures linked to management-level goals, objectives, and measures? (All)

(23) Are requirements being developed in consonance 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, ACOM)

(24) Are non-IT programmed purchases in excess of the $25,000 threshold for Operation and Maintenance, Army funds and in excess of the $100,000 threshold for Research, Development, Test and Evaluation funds being executed using the AKM Goal 1 Waiver process? (All)

(25) Are all AKM Goal 1 Waivers being submitted in accordance with DA Pam 25–1–1, chapter 2–6? (All)

c. Army Enterprise Architecture (chap 4). (All, as applicable)

(1) Has the organization developed the appropriate architectures for the Army Knowledge EA that support the DOTMLPF components as mapped to the Net-Centric Operations and Warfare Reference Model?

(2) Has the organization developed the appropriate architectures for the Battle Command Architecture that support 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 that 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 lifecycle management, materiel supply and service management, real property and installations life cycle, human resources management, and financial management?

d. Information Assurance (chap 5). (Applies to HQDA, ACOM, ASCC, DRU, separate reporting activity, region, installation, and unit.)

(1) Has an IA program been established at all levels?

(2) At each level, have the appropriate IA personnel been appointed?

(3) Are Information Assurance Vulnerability Management (IAVM) messages being acted upon and reported in a timely fashion?

(4) Are all ISs and networks accredited and certified? When a new IS is created, does it meet all accreditation and certification standards?

(5) Have the appropriate software controls been implemented to protect system software from compromise, subversion, and/or tampering?

(6) Is only approved software being used on Army networks and standalone workstations?

(7) Are databases that contain classified defense information protected to the highest security classification of any identifiable database element?

(8) Are developers of Army systems that include software using appropriate security features in the initial concept exploration phase of the life cycle system development model? Is the software being independently tested and verified prior to release for operation?

(9) Are developers of Army systems employing IA and security requirements in the design, development, and acquisition of the system, software, and/or physical environment of the system?

(10) Have all personnel received the appropriate level of training necessary to perform their designated IA responsibilities?

(11) Are proper password control and procedures being implemented within commands? Are minimum requirements of accountability, access control, least privilege, and data integrity being met?

(12) Are appropriate measures to secure all communications devices to the level of security classification of the information to be transmitted over such communication equipment being met?

(13) Has an effective risk management program been established by the commander? Has a periodic review of the risk management program taken place in the recent past?

e. C4/IT support and services (chap 6).

(1) Is a process in place for acquiring IT and ensuring all required licensing and registration are accomplished? (DOIM)

(2) Is the DOIM the single organization responsible for the oversight and management of installation IT? (DOIM)

(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 verified by the users 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 Thin Client Concept? (DOIM)

(7) Is an accurate inventory being maintained and validated annually for IT equipment? (DOIM, IMO)

(8) Are COOPs and procedures documented, distributed, and tested at least annually? (ACOM, DOIM)

(9) Has guidance been provided to ensure all software is checked for viruses before being loaded? (DOIM)

(10) Are existing capabilities and/or assets considered prior to upgrading, improving, or implementing LANs? (RCIO, DOIM)

(11) Are uneconomical IT service contracts identified and terminated? (All)

(12) Has the DOIM coordinated the acquisition of licenses with the CHESS office prior to entering into an agreement with a COTS vendor? (DOIM)

(13) Are spare capacity and functional expansion on IT being considered and/or used when new requirements are identified? (All)

(14) Has the DOIM reported its server consolidation status for all its Army tenants to the Army CIO/G–6? (DOIM)

(15) Are measures being taken to ensure that hard drives are disposed of properly? (DOIM)

(16) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (RCIO, DOIM)

(17) Has guidance been provided to review and revalidate cellular telephones and pagers every two years? (RCIO, DOIM)

(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? (DOIM)

(19) Is there a requirement for cellular phones and pagers to be recorded in the property book? (DOIM)

(20) Has the DOIM implemented accountable billing procedures? (DOIM)

(21) Have maintenance and support strategies been devised to minimize overall systems life cycle cost at an acceptable level of risk? (PEO, PM, ACOM)

(22) Have program managers, project managers, and IT MATDEVs coordinated their system architectures and fielding plans with the gaining commands, DRUs, RCIOs, and installation DOIMs prior to fielding systems? (PEO, PM)

(23) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (RCIO, DOIM, IMO)

(24) Are private sector service providers made aware that written assurance of compliance with software copyright laws may be required? (RCIO, DOIM, IMO)

(25) Are existing portals being migrated to AKO/DKO and AKO–S? (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 for external links notice for 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 personally identifiable information about Web visitors? (All)

(31) Is each Web site made accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act? (All)

(32) Is 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 account 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. - 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. - FOUO.

(b) Operations, plans, and training. - Operational orders and plans. - Mission-specific training. - Exercise and simulations activity. - Exercise, deployment, or training schedules. - Unit relocation/deployment. - 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/or e-mail by unit personnel (personal or official business). - Availability of secure communications. - Hypertext links with other agencies or units. - Family support plans. - Bulletin board postings/ messages between soldiers and family members.

(d) Logistics/maintenance. - Supply and equipment orders/deliveries. - Transportation plans. - Mapping, imagery, and special documentation support. - Maintenance and logistics requirements. - 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. - Lists of personnel.

(35) Are existing infrastructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA, ACOM)

(36) Is the fully qualified domain name (for example, http://www.us.army.mil or http://apd.army.mil) for Army sites registered with the Government Information Locator Service at http://sites.defenselink.mil/ and the contact information updated annually?

(37) Are the Web servers IAVA compliant and placed behind a reverse proxy server?

f. Visual Information (chap 7).

(1) Does the mission guidance include 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 RCIO's purview have a DVI Authorization Number (DVIAN)? (HQDA)

(5) Does the VI manager approve all VI equipment required by AR 25–1, chapter 7? (HQDA)

(6) Is VI policy being followed for multimedia/VI productions? (For example, DD Form 1995 is used, funds identified up front, PAN registers maintained, DAVIS searches conducted, service support contracts awarded for less than 50 percent of the total production cost, non-local DAVIS 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 include an SOP? (installation)

g. Records management (chap 8).

(1) Is a records management program established in your organization? (All)

(2) Has a records official been appointed to manage the internal records of the organization and its subelements? (All)

(3) Are RMs included in the planning process for new or replacement automated systems? (All)

(4) Are records management reviews of agencies and commands conducted at least once every three years? (All)

(5) Have instructions been issued specifying the degree of protection to be afforded to records stored and used electronically in accordance with classification, releasability, FOIA, and Privacy Act? (All)

(6) Are procedures in place to ensure software and equipment are available to read electronic records throughout their retention period? (All)

(7) Do all information collections from the public, affecting 10 or more individuals, have OMB approval? (All)

(8) Do the documents have special management or archiving requirements? (All)

h. Publishing and printing management (chap 9).

(1) Are policy publications issued as regulations? (HQDA)

(2) Are higher-echelon forms used in lieu of creating local forms for the same purpose? (All)

(3) Is a program established to encourage the design and use of electronically generated forms? (HQDA)

(4) Are Armywide forms for electronic generation approved by the functional proponent and APD? (HQDA)

(5) Is field printing coordinated through DAPS and the printing officer? (All)

C–5. Supersession

This checklist replaces the checklist for the administration of Army IM and IT previously published in AR 25–1, dated 15 July 2005.

C–6. Comments

Help make this a better tool for evaluating management controls. Submit comments to CIO/G–6 (SAIS–GKP), 107 Army Pentagon, Washington, D.C. 20310–0107.

Appendix D
Army IT PfM MA/Domain Leads

Figure D–1 lists the Army IT PfM MA and Domain Leads. Reference paras 3–3, 3–4, and 3–11 for the functions of MA and Domain Leads and their role in IT PfM. DOD equivalent MAs are identified in DODD 8115.1 and DODI 8115.02.

Warfighting Mission Area	Lead: DCS, G-3/5/7	
	Battlespace Awareness Domain	DCS, G-2
	Force Application Domain	DCS, G-8
	Force Protection Domain	DCS, G-8
	Logistics Domain	DCS, G-4
	Net-Centric Domain	CIO/G-6
	Force Management Domain	DCS, G-3/5/7
	Training Domain	DCS, G-3/5/7
	Command and Control Domain	DCS, G-3/5/7
Business Mission Area	Lead: USA (DUSA)	
	Acquisition Domain	Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA(AL&T))
	Financial Management Domain	Assistant Secretary of the Army (Financial Management & Comptroller) (ASA(FM&C))
	Human Capital Management Domain	Assistant Secretary of the Army (Manpower & Reserve Affairs)
	Logistics Domain	DCS, G-4
	Installations & Environment Domain	ACSIM
EIEMA	Lead: CIO/G-6	
	Communications Domain	CIO/G-6
	Computing Infrastructure Domain	CIO/G-6
	Core Enterprise Services Domain	CIO/G-6
	IA Domain	CIO/G-6

Figure D–1. Army IT PfM MA/Domain Leads

Appendix E
Sample DISR Waiver Request

This sample waiver (fig E–1) is an example of a request that must be submitted to request Army waivers to DISR standards. The CIO/G–6 coordinates the requests and the U.S. Army Research, Development and Engineering Command's Communications–Electronics Research, Development, and Engineering Center Army Systems Engineering Office provides a technical review and risk assessment/impact analysis. Waiver requests are reviewed for mitigation of potential negative impacts on cost, schedule, or performance. Reference para 4–2 of this publication for the complete waiver request policy and process.

Army CIO/G-6
DOD IT Standards Registry (DISR) Waiver Request

System Name and Acronym:
System Description:

System deployment date:
Proposed non-mandated IT standard title and description:
Has a DISR Change Request (CR) been submitted for this standard? Y ☐ N ☐
If yes, what was the outcome?
Is there a DoD mandated standard supporting this or a similar capability?: Y ☐ N ☐
If Yes, identify standard DISR number and title:
Justification and rationale for waiving requirements to use the aforementioned mandated standard:

Are any upgrades or replacements planned for the system?: Y ☐ N ☐
If so, (1) when and to (2) what degree?:

Is the system planned for retirement?: Y ☐ N ☐
If so, when?:

Acquisition Category: Mission Critical/Mission Essential ACAT ☐ Non-ACAT ☐ Other ☐
If Other, please specify: _____

Attached TV-1 Supports which JCIDS Document Type: CDD ☐ CPD ☐ Not Applicable ☐

JCIDS Document Stage: I ☐ II ☐ III ☐ Not Applicable ☐
JCIDS Document Title:_____

Does this waiver request support a C4 Information Support Plan or Information Support Plan submission?: Y ☐ N ☐
Other document: _____

Acquisition Milestone: A ☐ B ☐ C ☐ Not Applicable ☐

Organization Requesting Waiver:

POC (Name / Office Symbol / Phone Number / Email):

PM (Name / Office Symbol / Phone Number / Email):

PEO (Name / Office Symbol / Phone Number / Email):

Figure E–1. Sample DISR Waiver Request

PEO Technical Director (Signature):

_____ _____

Name/Title Date

Attach **Transition Plan** associated with this waiver which addresses:
1. When the system will be brought into compliance with DISR mandates.
2. How the system will be brought into compliance with DISR mandates.

Attach **Risk Assessment** associated with this waiver which addresses:
Interoperability impacts -
If waiver is granted
If waiver is not granted
Names and acronyms of all systems interfacing with program requesting waiver.
Impacts to program requesting waiver (if waiver is not granted):
Cost
Schedule
Performance
Operational limitations
Information Security

Notes:

Submit waiver request to:
Army CIO/G-6
107 Army Pentagon, Rm 1A267
ATTN: Enterprise Architecture Div. (SAIS-AOE)
Washington, DC 20310-0107

Provide a copy to:
Headquarters, Communications Electronics
Research Development & Engineering Center
ATTN: ASEO (AMSRD-CER-SE
Fort Monmouth, NJ

Figure E–1. Sample DISR Waiver Request—Continued

Glossary

Section I
Abbreviations

AAE
Army Acquisition Executive

AAFES
Army and Air Force Exchange Service

AASA
Administrative Assistant to the Secretary of the Army

ABCA
American, British, Canadian, Australian

ACAT
acquisition category

ACOM
Army Command

ACP
Allied Communications Publication

ACS
Army Community Service

ACSIM
Assistant Chief of Staff for Installation Management

ADA
Army Declassification Activity

ADS
Authoritative Data Source

AEA
Army Enterprise Architecture

AEI
Army Enterprise Infrastructure

AEL
Army Electronic Library

AENIA
Army Enterprise Network Operations Integrated Architecture

AFIP
Armed Forces Institute of Pathology

AFRTS
Armed Forces Radio and Television Service

AGNOSC
Army Global Network Operations Security Center

AIC
Army Interoperability Certification

AKM
Army Knowledge Management

AKO/DKO
Army Knowledge Online/Defense Knowledge Online

AKO–S
Army Knowledge Online–Secret

AMC
United States Army Materiel Command

AMP
Army Modernization Plan

AMVID
Army Multimedia & Visual Information Directorate

ANCDMP
Army Net-Centric Data Management Program

APC
Area Processing Center

APD
Army Publishing Directorate

APF
appropriated fund(s)

APL
approved product list

APMS
Army Portfolio Management Solution

APMS–AITR
Army Portfolio Management Solution–Army Information Technology Registry

APP
Army Publishing Program

AR
Army Regulation

ARC
American Red Cross

ARIMS (formerly MARKS)
Army Records Information Management System

ARNG
Army National Guard

AROC
Army Requirements Oversight Council

ARSTAF
Army Staff

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

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

ASCC
Army Service Component Command

ASD(PA)
Assistant Secretary of Defense (Public Affairs)

ASD(NII)
Assistant Secretary of Defense for Networks & Information Integration

ASMO
Army Spectrum Management Office

ATTN
Attention

AVID
Army Visual Information Directorate

AWRAC
Army Web Risk Assessment Cell

BASECOM
Base Communications

BEA
Business Enterprise Architecture

BMA
Business Mission Area

BES
Budget Estimate Submission

BGAN
Broadband Global Area Network

BPA
Blanket Purchase Agreement

C2
command and control

C3I
command, control, communications, and intelligence

C4
command, control, communications, and computers

C4IM
command, control, communications, computers and information management

C4ISR
command, control, communications, computers, intelligence, surveillance, and reconnaissance

C4/IT
command, control, communications, computers, and information technology

CAC
Common Access Card

CALS
continuous acquisition and lifecycle support

CAP
Component Accessioning Point

CATV
cable television

CCA
Clinger-Cohen Act

CCTV
closed circuit television

CD
compact disc

CDAd
Component Data Administrator

CD-ROM
compact disc-read only memory

CFR
Code of Federal Regulations

CHESS
Computer Hardware, Enterprise Software, and Solutions

CIK
Crypto Ignition Key

CIO
Chief Information Officer

CJCS
Chairman, Joint Chief of Staff

CJCSI
Chairman, Joint Chief of Staff Instruction

CLS
Common Levels of Support

CMO
Collaboration Management Office

COCOM
Combatant Command

COIs
Communities of Interest

COIDAds
Communities of Interest Data Administrators

COMCAM
combat camera

COMSEC
Communications Security

CoN
Certificate of Networthiness

CONUS
continental United States

COOP
Continuity of Operations Plan

CoP
Community of Practice

COTS
commercial off-the-shelf

CP–34
Career Program 34

CPIM
Capital Planning and Investment Management

CR
change request

CSA
Chief of Staff, Army

CTA
common table of allowances

CTSF
Central Technical Support Facility

DA
Department of the Army

DAA
Designated Accrediting Authority

DAB
Defense Acquisition Board

DAPS
Defense Automated Printing Service

DAMVIPDP
DA Multimedia/Visual Information Production and Distribution Program

DAVIS
Defense Automated Visual Information System

DBMS
Database Management Systems

DBSMC
Defense Business System Management Committee

DCID
Director of Central Intelligence Directive

DCS
Deputy Chief of Staff

DDOE
Defense Information Systems Agency Direct Order Entry

DeCA
Defense Commissary Agency

DFAR
Department of Defense Federal Acquisition Regulation

DIACAP
Department of Defense Information Assurance Certification and Accreditation Process

DISA
Defense Information Systems Agency

DISAC
Defense Information Systems Agency Circular

DISN
Defense Information Systems Network

DISR
Defense Information Systems Registry

DITIS
Defense Instructional Technology Information System

DLA
Defense Logistics Agency

DMRD
Defense Management Resource Decision

DMS
Defense Message System

DOD
Department of Defense

DODAF
Department of Defense Architecture Framework

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DOIM
Director of Information Management

DOTMLPF
doctrine, organization, training, materiel, leadership and education, personnel, and facilities

DPP
Data Performance Plan

DPPS
Data Performance Plan System

DRMS
Defense Reutilization and Marketing System

DRSN
Defense Red Switch Network

DRU
Direct Reporting Unit

DSAWG
Defense Information Systems Network Accreditation Working Group

DSCS
Defense Satellite Communications System

DSN
Defense Switched Networks

DUSA
Deputy Under Secretary of the Army

DVD
digital video disc

DVI
Defense Visual Information

DVIAN
Department of Defense Visual Information Activity Number

DVIC
Defense Visual Information Center

DVS
Defense Video Services

EA
enterprise architecture

e-Army
electronic Army

e-mail
electronic mail

EB
executive board

ECECS
executive control and essential command supervision

E-Gov
electronic government

EID
enterprise identifier

EIE
Enterprise Information Environment

EIEMA
Enterprise Information Environment Mission Area

EIT
electronic and information technology

ELA
enterprise license agreement

EO
Executive Order

E/MVISC
Enterprise Multi-media Visual Information Service Center

ERP
enterprise resource planning

ESA
enterprise software agreement

ESI
enterprise software initiative

ESTA
enterprise systems technology activity

FAR
Federal Acquisition Regulation

Fax
facsimile

FISMA
Federal Information Security Management Act

FMWRC
U.S. Army Family and Morale, Welfare and Recreation Command

FOA
Field Operating Agency

FOIA
Freedom of Information Act

FORSCOM
United States Army Forces Command

FOUO
For Official Use Only

FX
Foreign Exchange

FY
fiscal year

FYDP
Future Year Defense Program

GBS
Global Broadcast Service

GETS
Government Emergency Telecommunication Service

GIG
Global Information Grid

GNOSC
Global Network Operations and Security Center

GOTS
Government Off-the-Shelf

GPO
Government Printing Office

GPS
Global Positioning System

GSA
General Services Administration

HIPAA
Health Insurance Portability and Accountability Act of 1996

HMW
Health, Morale, and Welfare

HQ
headquarters

HQDA
Headquarters, Department of the Army

HQIM
Headquarters, Department of the Army Information Manager

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol Secure

IA
information assurance

IAM
Information Assurance Manager

IAPM
Information Assurance Program Manager

IASO
Information Assurance Security Officer

IAVA
Information Assurance Vulnerability Alert

IAVM
Information Assurance Vulnerability Management

IESS
Information Exchange Standards Specifications

ILS
integrated logistics support

IM
information management

IMCOM
Installation Management Command

IMI
interactive multimedia instruction

IMO
Information Management Officer

Inmarsat
International Maritime Satellite

INSCOM
United States Army Intelligence and Security Command

IP
internet protocol

IPN
installation processing node

IPv4
Internet Protocol version 4

IPv6
Internet Protocol version 6

IRB
Investment Review Board

IRM
Information Resources Management

IS
information system

ISA
Inter-Service Support Agreement

ISO
International Standards Organization

ISP
Internet Service Provider

IT
information technology

ITM
Information Technology Management

JCCC
Joint Combat Camera Center

JCIDS
Joint Capabilities Integration and Development System

JCS
Joint Chiefs of Staff

JITC
Joint Interoperability Test Command

JP
Joint Publication

JPO
Joint Program Office

JS
Joint Staff

JSA
Joint Staffing Action

JTF
Joint Task Force

JVISDA
Joint Visual Information Services Distribution Activity

JWICS
Joint Worldwide Intelligence Communications System

KM
Knowledge Management

LAN
local area network

LandWarNet
land warrior network

LMR
land mobile radio

LWN
LandWarNet

MA
mission area

MARS
Military Affiliate Radio System

MATDEV
Materiel Developer

MB
megabytes

MCEB
Military Communications-Electronics Board

MDEP
Management Decision Evaluation Package

MEDCOM
United States Army Medical Command

MFP
Materiel Fielding Plan

MH
military holdover

MHz
megahertz

MICO
Management Information Control Office

MILCON
military construction

MILSATCOM
Military Satellite Communications

MIP
Military Intelligence Program

MSC
Major Subordinate Command

MSS
mobile satellite services

MTOE
modified table of organization and equipment

M/VI
Multimedia/Visual Information

MWR
Morale, Welfare, and Recreation

NAC
National Audiovisual Center

NAF
nonappropriated fund(s)

NAFI
Nonappropriated Fund Instrumentalities

NARA
National Archives and Records Administration

NATO
North Atlantic Treaty Organization

NCR
National Capital Region

NETCOM/9th SC (A)
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)

NetOps
Network Operations

NIP
National Intelligence Program

NIPRNet
non-secure internet protocol router network

NR-KPP
net-ready key performance parameters

NSA
National Security Agency

NSS
National Security Systems

NTIA
National Telecommunications and Information Association

OA
Operational Architecture

OAASA
Office of the Administrative Assistant to the Secretary of the Army

OIA&C
Office of Information Assurance and Compliance

O&M
operation and maintenance

OCONUS
outside of the continental United States

OCSA
Office of the Chief of Staff, Army

OMB
Office of Management and Budget

OPA
other procurement, Army

OPR
office of primary responsibility

OSD
Office of the Secretary of Defense

OV
operational view

P.L.
Public Law

PA
Public Affairs

Pam
Pamphlet

PAN
Production Authorization Number

PAO
Public Affairs Officer

PC
Personal Computer

PDA
Personal Digital Assistant

PEG
Program Evaluation Group

PEO
Program Executive Officer

PfM
Portfolio Management

PIA
Privacy Impact Assessment

PIN
Personal/Production Identification Number

PKI
Public Key Infrastructure

PM
Program/Project/Product Manager

POC
point of contact

POM
Program Objective Memorandum

PPBE
planning, programming, budgeting, and execution

PPS
Precise Positioning Service

PPSS
Postproduction Software Support

PSN
Public Switch Network

RA
Records Administrator

RC
Records Coordinator

RCIO
Regional Chief Information Officer

RCS
Requirements Control Symbol

RDT&E
research, development, test, and evaluation

RHA
records holding area

RHAM
records holding area manager

RM
Records Managers

RMDA
Records Management and Declassification Agency

ROTC
Reserve Officer Training Corps

RSC
Regional Support Center

SA
Systems Architecture

SAP
Special Access Program

SATCOM
Satellite Communications

SB
Supply Bulletin

SC(A)
Signal Command (Army)

SCI
Sensitive Compartmented Information

SDB
Satellite Database

SECARMY
Secretary of the Army

SGML
Standard Generalized Markup Language

SIPRNet
Secret Internet Protocol Router Network

SLA
Service Level Agreement

SMS
Strategic Management System

SNAP
System Network Approval Process

SSL
Secure Socket Layer

SSO
single sign on

STARC
State Area Command

STE
secure telephone equipment

STU-III
Secure Telephone Unit, Type III

SV
system view

T&E
test and evaluation

T-ASA
Television-Audio Support Activity

TA
Technical Architecture

TAP
The Army Plan

TDA
table of distribution and allowances

TDY
temporary duty

TISP
Tailored Information Support Plan

TR
telecommunication request

TJAG
The Judge Advocate General

TNOSC
Theater Network Operations and Security Center

TOE
table of organization and equipment

TRADOC
U.S. Army Training and Doctrine Command

TV
technical view (architecture)

UFR
unfunded requirement

URL
Uniform Resource Locator

USACE
United States Army Corps of Engineers

USAISEC
United States Army Information Systems Engineering Command

USAR
U.S. Army Reserve

RMDA
U.S. Army Records Management and Declassification Agency

USC
United States Code

USSTRATCOM
United States Strategic Command

VI
visual Information

VIDOC
Visual Information Documentation

VIRIN
Visual Information Record Identification Number

VISP
Visual Information Systems Program

VOIP
Voice over Internet Protocol

VOSIP
Voice over Secure Internet Protocol

VTC
video teleconference

W3C
World Wide Web Consortium

WMA
Warfighting Mission Area

WPS
Wireless Priority Service

WWW
World Wide Web

XML
Extensible Markup Language

Section II
Terms

Access control mechanism
This permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform.

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 e-mail. An application should be considered a system for the purpose of reporting to the Army Information Technology Registry unless it is part of a larger system already being reported.

Architecture
See Enterprise Architecture and Army Enterprise Architecture.

Army Business Enterprise Architecture (ABEA)
The framework of the business processes and organizations that support the Army's warfighters.

Army Enterprise Architecture (AEA)
See 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 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 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 NARA approved schedules.

Army Visual Information Steering Committee
A committee chaired by CIO/G–6 that develops recommendations for the CIO/G–6 in regards to Army VI planning, policy, programming, systems, standards, architecture, procedures, organizational structure, COMCAM, combat and training development, doctrine, and other related issues.

Army Web Risk Assessment Cell
A team of IA personnel that conduct ongoing operational security and threat assessments of Army publicly accessible Web sites to ensure compliance with DOD and Army policy and best practices.

Army Web site
A collection of HTML pages, graphics, images, video and audio, databases or other media assets at a Uniform Resource Locator (URL) which is made available for distribution and/or 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 TV, 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, 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 (ADS)
An ADS is a data structure and value domain set that is readily available to provide common domains of data values to different databases.

Automation
Conversion of a procedure, process, or equipment to automatic operation. When allied to telecommunications facilities,

automation may include the conversion to automatic operation of the message processing at an exchange or remote terminal.

Bandwidth
The maximum rate at which an amount of data can be sent through a given transmission channel.

Base case system
A system that has been fielded and certified through the intra-Army interoperability process.

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.

Binning
The IT portfolio management phase that assigns IT investments to the governing Army IT MA or domain portfolio. The intent of the binning phase is to place Army IT investments within the appropriate IT Portfolio according to the capabilities that the system provides.

Broadcast
The transmission of radio, television, and data signals through the air waves or fiber optic cable.

Business Enterprise Architecture (BEA)
The EA for the DOD's business information infrastructure and 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 our warfighters through ensuring accurate, reliable, timely and compliant information across the DOD.

Business/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.)

Business process re-engineering
The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance such as cost, quality, service, and speed. Re-engineering is part of what is necessary in the radical change of processes. (DODD 8000.01.)

C4IM Services List
The source document that defines the Army Enterprise Baseline and Mission Information Technology (IT) services provided and/or supported by the DOIM. This list of service definitions is the foundation for the development and publishing of the LandWarNet (LWN) Services Catalog. The C4IM Services listed as "Baseline" are core/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 (cell phones, pagers, personal digital assistants, and so forth) and are grounded by the business processes that enable mission execution in a more efficient/effective manner.

Cable television (CATV) system
A facility consisting of a set of closed transmission paths and associated signal generation, reception, and control equipment that is designated to provide cable service that includes both audio and video programming and that is provided to multiple subscribers.

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 that requirement.

Capital Planning and Investment Management (CPIM)
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.

Class A (official) telephone service
Telephone service authorized for the transaction of official business of the Government on DOD/military installations; requires access to commercial telephone company central office and toll trunks for the proper conduct of official business.

Class B (unofficial) telephone service
Telephone service installed on or in the immediate vicinity of a DOD/military installation served through a military Private Branch Exchange or Central Exchange system through which the conduct of personal or unofficial business is authorized. This telephone service has access to commercial telephone company central office and toll trunks.

Class C (official-restricted) telephone service
Telephone service authorized for the transaction of official business of the Government on a DOD/military installation and without access to Telephone Company central office or toll trunks.

Class D (official-special) telephone service
Telephone service installed on military installations for official business of the Government and restricted to special classes of service, such as fire alarm, guard alarm, and crash alarm.

Closed circuit television (CCTV)
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 employed by a commander in planning, directing, coordinating, and controlling forces and operations in 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 that is essential to plan, direct, and control operations conducted by assigned resources.

Command, control, communications and computer (C4) systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications, and computers.

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 (COMSEC)
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 (COIs)
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 shared vocabulary for the information they exchange.

Community of practice (CoP)
A CoP is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice. 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 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 three-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 CATV franchisee for initial hookup, reconnection, or relocation of equipment necessary to transmit the CATV signal from the distribution cable to a subscriber's receiver.

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 (HTML) information flowing back and forth between the user's computer and the servers. They allow user-side customization of Web information. Normally, cookies will 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 formalized manner which is 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 built on standard semantics and structures 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 the 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 (DPP)
An organized and structured approach to the specification and collection of enterprise artifacts in support of COI objectives that 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 (DPPS)
A centralized repository for enterprisewide storing, viewing, and reusing architectures, data models, business rules, and other artifacts associated with functional Army systems.

Data standards
Metadata expressed as ADSs, IESSs, EIDs, and XML used to guide all data exchanges including those with legacy systems.

Data synchronization
Policies and procedures that govern consistency, accuracy, reliability, and timeliness of data used and generated by the Army. It addresses data planning, storage, scheduling, maintenance, and exchange among authorized users.

Defense Automated Visual Information System (DAVIS)
DOD-wide automated catalog system for management of VI products and multimedia material (includes production, procurement, inventory, distribution, production status, and archival control of multimedia/VI productions and materials). The DAVIS will be searched prior to any start of a new VI production to determine if a suitable product already exists. Armed Forces Information Service/DVI is the database manager and provides policy guidance concerning the operation of DAVIS functions. The Web site is http://dodimagery.afis.osd.mil.

Defense Telephone System
A centrally managed system that, in accordance with its charter, provides telephone service to all the DOD activities in the area.

Degauss
A procedure that reduces the magnetic flux of a medium to virtually zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.

Department of Army Multimedia/Visual Information Production and Distribution Program (DAMVIPDP)
Provides for the annual identification, funding, and acquisition of multimedia/VI production and distribution requirements. All Army organizations identify their requirements for multimedia/VI productions and forward their requests to their supporting regional/FOA VI manager for validation. Regional/FOA VI managers forward valid requirements to CIO/G–6 for validation.

Digital signature
The product of an asymmetric cryptographic system that is created when the owner of the private signing key uses that key to create a unique mark (the signature) on an electronic document or file. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who they claim to be.

Direct reporting unit (DRU)
An operational command that reports to and is under the direct supervision of an HQDA element. A DRU executes its unique mission based on policy established by its HQDA principal.

Disk
As applied to information management, disc and disk are synonymous. Flat, circular information system media used to record, store, manipulate, and retrieve data and information. Examples of discs are phonograph records, videodisks, computer disks, floppy disks, optical disks, and compact disks.

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.

DOD Information Technology Standards Registry (DISR)
DISR is a joint effort to identify and mandate IT standards for use in acquisition/development of DOD systems. It focuses on the interoperability and standardization of information technology and support to net-centric operations and warfare.

Domain
An area of common operational and functional requirements. Currently, there are four domains: C3I; weapon systems; modeling and simulation; and sustainment.

Electronic business (e-business)
A means of performing enterprise activities that involves the use of electronic technologies, including such techniques as facsimile, e-mail, WWW software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

Electronic Government (E-Government)
The use by Government of Web-based Internet applications and other information technologies, combined with processes that implement these technologies, to (A) enhance the 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 (e-mail)
An information dissemination and retrieval service accessed through distributed user workstations normally provided through office automation initiative.

Electronic recordkeeping
The operation of recordkeeping systems requiring a machine interface for the human use of records. Examples of record media include magnetic tapes, disks and drums, video files, and optical disks.

Electronic signature
A generic term encompassing both noncryptographic and cryptographic methods of authenticating identity. Noncryptographic methods include PIN or password, smart card, digitized signature, and biometrics. Cryptographic methods include shared symmetric key cryptography, and public/private key (asymmetric) cryptography-digital signatures.

Enterprise Multimedia and Visual Information Service Center (E/MVISC)
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
The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise Architecture (EA)
A strategic information asset base, which defines the mission, the 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 (44 USC 3601).

Enterprise identifier (EID)
A 64-bit information identification tag (key) that remains unique across an enterprise. Each EID is composed of a 32-bit EID seed followed by a 32-bit sequence determined by the EID server.

Enterprise Information Environment (EIE)
The common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or that 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 of, and delivery of information on the GIG.

Environment
The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.

Executive control and essential command supervision (ECECS)
Those managerial staff functions and positions located above the direct program managerial and operational level of individual MWR programs that support planning, organizing, directing, coordinating, and controlling the overall operations of MWR programs. ECECS consists of program, fiscal, logistical, and other managerial functions that are required by DODD 1015.2 to ensure oversight. AR 215–1 provides clarification of ECECS with respect to Army MWR programs and activities as those functions and positions that support planning, organizing, directing, coordinating, and controlling the overall operations of MWR programs. ECECS consists of program, fiscal, logistical, and other managerial fiduciary functions that are required to ensure oversight of Government appropriated and NAF MWR assets.

eXtensible Markup Language (XML)
A tagging language used to describe and annotate data so it 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 interbusiness 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.

Federated Architecture
An approach for EA development that is composed of a set of a coherent but distinct entity or architectures; the architectures of separate members of the federation. The members of the federation participate to produce interoperable, 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, 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 (GIG)
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.

Government Performance and Results Act (P.L. 103–62)
A law that creates a long-term goal-setting process to improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction.

Graphic arts
Relates to the design, creation, and preparation of two- or three-dimensional visual products. Includes charts, graphics, posters, and visual materials for brochures, covers, television, motion pictures, printed publications, display, presentations, and exhibits prepared manually, by machine, or by computer.

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
The meaning that a human assigns to data by means of the known conventions used in their representations (see JP 1–02). Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights.

Information Assurance Vulnerability Alerts (IAVA)
Positive control mechanism that pushes alerts and advisories on IA security vulnerabilities to IA personnel. IAVA also requires the tracking of response and compliance to the messages.

Information exchange requirement
Substantive content, format, throughput requirements, and classification level.

Information exchange standards specification (IESS)
A narrowly scoped data model to facilitate data exchange and interoperability between COIs.

Information management
Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information Management Office/Officer (IMO)
The office/individual responsible to the respective commander/director/chief for coordinating service definition, management oversight, advice, planning, and funding coordination of all IT/IM requirements (business and mission) for the organization. The IMO assists the commander/director/chief in exercising responsibility to effectively manage the organization's IT/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 (IRM)
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 acquisition and use of automatic data processing, telecommunications, and other IT.

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

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

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

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

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

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

Integrity (of information)
Assurance of protection from unauthorized change.

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

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

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

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

IPv6-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.

IPv6-Enabled
IPv6-Capable systems or products with the IPv6 functionality turned on - implying that IPv6 packets can be properly processed by that system or product/component.

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.

Intra-Army interoperability certification
Confirmation 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.

Intranet
A computer network that functions like the Internet, using Web browser software to access and process the information that employees need, and located on computers within the organization/enterprise. A firewall is usually used to block access from outside the intranet. Intranets are private Web sites.

IT Architecture
An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic and IRM goals.

IT capital planning and investment control
An end-to-end integrative process that frames and manages the life cycle of an IT investment. Its purpose is to maximize the value and assess and manage the risks of the IT acquisitions of the Army. The process includes the selection, management, and evaluation of IT investments.

IT investment portfolio
A collection of IT investments that represents the best balance of costs, benefits, and risks and is designed to improve the overall organizational performance and maximize mission performance.

IT management process
An end-to-end integrated process that includes the information management/information technology (IM/IT) business planning, business/functional process improvement, capital investment planning and investment control ITM and oversight, acquisition of C4/IT, fielding and prioritization.

IT support agreement
An agreement to provide recurring IT support, the basis for reimbursement (if any) for each category of support, the billing and payment process, and other terms and conditions of the agreement.

Knowledge-based Force
An organization whose processes, tools, and technologies are focused on exploiting the enterprise's knowledge assets to achieve mission-critical objectives.

LandWarNet (LWN)
Combination of infrastructure and services across the Army. It provides for processing, storing, and transporting information over a seamless network.

Land Mobile Radio (LMR) Systems
Antennas, consoles, switches, repeaters, handheld radios, vehicular mounted radios, and associated components of non-tactical radio frequency systems that operate in the bands 138-150.8 megahertz (MHz), 162-174 MHz, 380-399.9 MHz, and 406.1-420 MHz.

Life cycle
The total phases through which an item progresses from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

Machine readable
Data and information storage media requiring the use of one or more information system component(s) for translation into a medium understandable and usable to humans.

Management Decision Evaluation Package (MDEP)
A nine-year package of dollars and manpower to support a given program or function. The MDEP justifies the resource expenditure.

Master/community antenna television (M/CATV) system
A facility consisting of a television reception service that receives broadcast radio frequency television signal and/or FM radio programs and distributes them via signal generation, reception, and control equipment.

Master plan
An enterprisewide planning directive that establishes the vision, goals, and objectives of the enterprise; establishes an enterprise-level procedure for achieving the vision, goals, and objectives; specifies actions required to achieve the vision, goals, and objectives; identifies roles and assigns responsibilities for executing the specified actions; establishes priorities among actions and relevant supporting programs; and establishes performance measures and responsibilities for measuring performance.

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; data or information about data; 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, with their purpose, assigned to military organizations, units, or individuals for execution.

Mission Area (MA)
A defined area of responsibility with functions and processes that contribute to mission accomplishment.

Mission Critical Information System
A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations.

Mission Essential Information System
A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The definition of "the Organizational Mission" is one of the organizational missions of the Army - not just a single command or DA functional proponent.)

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 allocating of resources).

Morale, welfare, and recreation (MWR) 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 that provide for the mission sustainment and community support for authorized DOD personnel.

Motion media
A series of images viewed in rapid succession, giving the illusion of motion, obtained with a motion picture or video camera.

Multimedia
The synchronized use of two or more types of media, regardless of the delivery medium.

Narrowband Operation
Equipment in the frequency bands 138-150.8 MHz, 162-174 MHz, 380-399.9 MHz, and 406.1-420 MHz operating in 11 KHz or less of necessary bandwidth as defined by the National Telecommunications and Information Administration.

National Security System
Any telecommunications or information system operated by the United States Government, the function, operation, or use of which 1) involves intelligence activities, 2) involves cryptologic activities related to national security, 3) involves C2 of military forces, 4) involves equipment that is an integral part of a weapon or weapons system, or 5) is critical to the direct fulfillment of military or intelligence missions (ref. 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 on 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.

News clip
A news story of an event recorded and released on motion picture or videotape for viewing by an internal Army audience or the general public.

Nonappropriated fund(s) (NAF)
Cash and other assets received from sources other than monies appropriated by the Congress of the United States. (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 Treasury of the United States. They are used for the collective benefit of the authorized patrons who generate them.

Nonappropriated fund instrumentalities (NAFIs)
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/information
Data/information that is personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive.

Nonpublic Web site
Army Web site with access restricted by password or PKI user authorization.

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 (OV) (Architecture)
A description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish or support a warfighting function. It defines the type of information, the frequency of exchange, and the 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 that is 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 those goals, and report on the success in meeting those goals.

Performance measure
A quantitative or qualitative characterization of performance.

Performance measurement
A process of accessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those 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.

Periodical
A nondirective classified or unclassified Army magazine or newsletter-type publication published annually or more often to disseminate information necessary to the issuing activity with a continuing policy regarding format, content, and purpose. A periodical is usually published to inform, motivate, increase knowledge, or improve performance. It contains official or unofficial information or both.

Permanent record
Information that has been determined by the Archivist of the United States to have sufficient value to warrant its preservation by the NARA for the life of the Republic.

Persistent cookies
Cookies that can be used to track users over time and across different Web sites to collect personal information.

Planning, Programming, Budgeting, and Execution (PPBE) process
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Portfolio Management (PfM)
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
A Privacy Impact Assessment (PIA) is an analysis of how personal information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating personal information in an information system, and (iii) to examine

and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a means to assure 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, with a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process owners
HQDA functional proponents, Army commands, and others who have responsibility for any mission-related or administrative work process.

Procurement/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.

Publications
Items of information that are printed or reproduced, whether mechanically or electronically, for distribution or dissemination usually to a predetermined audience. Generally, they are directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by or for the Army.

Publicly accessible Web site (or public Web site) on the WWW
Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a Web site through a browser.

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 and Privacy Acts.

Requirements generation process
The formal method of determining military operational deficiencies and the preferred set of solutions.

Satellite communications (SATCOM)
DOD use of military-owned and 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 (SLA)
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 (SCI)
Information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term encompasses communications intelligence and Special Activities Office information and materials.

Smart card
A credit card-size device, normally for carry and use by personnel, that contains one or more integrated circuit chips and may also employ one or more of the following technologies: 1) magnetic stripe; 2) barcodes, linear or two dimensional; 3) noncontact, radio frequency transmitters; 4) biometric information; 5) encryption and authentication; and 6) photo identification. It may be used to generate, store, or process data.

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, circuit diagrams); usually contrasted with hardware.

Spam
Widely disseminated "junk" e-mail.

Standard
Within the context of the AEA, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. It may also establish requirements for selection, application, and design criteria of materiel.

Still photography
The medium used to record still imagery; includes negative and positive images.

Strategic planning
A continuous and systematic process whereby guiding members of an organization make decisions about its 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 (that is, the application of IT).

Systems Architect
Responsible for integration and oversight of architecture of IT/NSS from a systems perspective.

Systems Architecture
Descriptions, including graphics, of systems and interconnections providing for or supporting functions.

System View (SV) (Architecture)
A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. It 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 (TAP)
This plan is a 16-year strategic planning horizon that includes the 6-year span of the program (POM) years plus an additional 10 years. TAP 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, not specific to a single unit, weapon system, or individual, that enables a mission or function to be accomplished by individuals or organizations.

Technical Architecture (TA)
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.

Technical View (TV) (Architecture)
The minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system to ensure that a system satisfies a specified set of requirements. A TV identifies services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, 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 use of 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 networks which depends primarily on the central server for processing activities which focuses 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, meaning 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 the various companies that serve the banner ads that appear across many Web sites.

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, and/or otherwise applying DOTMLPF products in accomplishment of a designated mission.

Uniform resource locator (URL)
A Web address 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.

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 (VTC)
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 (VI)
Information in the form of visual or pictorial representations of person(s), place(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog and digital video recordings, and hand- or computer-generated art and animations that depict real or imaginary person(s), place(s), and/or thing(s), and related captions, overlays, and intellectual control data.

VI 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.

VI documentation (VIDOC)
Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, and are usually not controlled by the recording crew.

VI equipment
Items capable of continuing or repetitive use by an individual or organization for the recording, producing, reproducing, processing, broadcasting, editing, distribution, exhibiting, and storing of visual information. Items otherwise identified as VI equipment that 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.

VI 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.

VI library
A VI activity that loans, issues, and maintains an inventory of motion media, imagery and/or equipment.

VI 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.

VI materials
A general term, which 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 retained recorded imagery.

VI 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.

VI 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.

VI records
VI materials, regardless of format, related captions, and intellectual control data.

VI records center
A facility, sometimes specially designed and constructed, for the low-cost and efficient storage and referencing of semicurrent records pending their ultimate disposition.

VI report
VIDOC assembled to report on a particular subject or event.

VI resources
The personnel, facilities, equipment, products, budgets, and supplies which comprise DOD visual information support.

VI 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 connecting the warfighter to the sustaining base.

Web portals
Web sites that serve as starting points to other destinations or activities on the Web. Initially thought of as a "home base" type of Web page, portals attempt to provide all of a user's Internet needs in one location. Portals commonly provide services such as e-mail, collaboration centers, online chat forums, searching, content, newsfeeds, and others.

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 net by an enterprise.

World Wide Web (WWW)
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 - called also "Web."

Section III
Special Abbreviations and Terms
This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 253

PIN: 058039–000
DATE: 12- 4-08
TIME: 14:37:48
PAGES SET: 138

DATA FILE: C:\wincomp\r25-1.fil
DOCUMENT: AR 25–1

SECURITY: UNCLASSIFIED
DOC STATUS: REVISION