3

Army Regulation 25–1

Information Management

Army Knowledge Management and Information Technology

Headquarters
Department of the Army
Washington, DC
15 July 2005

UNCLASSIFIED

SUMMARY of CHANGE

AR 25-1
Army Knowledge Management and Information Technology

This administrative revision, dated 15 July 2005--

- Adds DA Form 3903 for multi-media/visual information service requests (para 7-4).

- Corrects typographical errors throughout the publication.

This revision, dated 30 June 2004--

- Supersedes Department of the Army Pamphlet 25-4, Information Systems Technical Documentation; Department of the Army Pamphlet 25-6, Configuration Management for Automated Information Systems; and Department of the Army Pamphlet 25-6-1, Army Acquisition Planning for Information Systems and rescinds Department of the Army Form 3903, Visual Information (VI) Work Order.

- Revises the title to add *Army Knowledge Management*.

- Adds guidance regarding quality of information disseminated to the public (chap 1).

- Updates the list of laws, statutes, and Executive orders that the Chief Information Officer has responsibility to implement; requires the Army Chief Information Officer to oversee and direct the Network Enterprise Technology Command/9th Army Signal Command; identifies the Assistant Secretary of the Army for Acquisition, Logistics and Technology as the Army Systems Architect; adds responsibility for command, control, communications, computers, and information technology base operations support responsibility to the Assistant Chief of Staff for Installation Management through the Installation Management Agency and removes the command, control, communications, computers, and information technology base operations responsibility from major Army commands (chap 2).

- Introduces the role of the Army Chief Information Officer Executive Board; requires an information technology management forum at the regional and installation levels patterned similar to the Army CIO Executive Board; clarifies Chief Information Officer designation and the role of senior information management officials at levels below Headquarters, Department of the Army; provides guidance for Chief Information Officer review of information technology expenditures; requires certification of interoperability between information systems; introduces the Army Information Technology Registry; and requires that all systems be webified and linked to the Army Knowledge Online portal (chap 3).

- Introduces Army Knowledge Enterprise Architecture as the infostructure architecture; Army Battle Command Architecture to support integration with Joint systems; and Army Business Enterprise Architecture to support the business domains (chap 4).

- Addresses the use of authoritative data sources and use of unique enterprise identifiers for producing data standards; introduces information exchange systems specifications; requires use of EXtensible Markup Language technology as the transfer mechanism for all data exchanges executed between Web-based solutions (chap 4).

- Introduces the Army Web Risk Assessment Cell to assess ongoing security and threats to public Web sites; requires use of Public Key Infrastructure and biometrics to protect information; requires establishment of information assurance programs and information assurance managers (chap 5).

- Designates Army Small Computer Program Office as the primary program office for establishing commercial information technology contracts; expands telework guidance to include conditions and authorized resources for telework; requires use of enterprise software agreements and enterprise license agreements for acquiring commercial-off-the-shelf software; provides guidance on server consolidation; prescribes additional policy on e-mail use; authorizes limited authorized use of cellular telephones; provides new policy on the Army Networthiness Certification Program; addresses disposal of unclassified Department of Defense computer hard drives; addresses collaboration tools suite standards; expands policy on leasing Government-owned telecommunications assets; clarifies personal digital assistant restrictions; requires Secret Internet Protocol Router Network users to have Army Knowledge Online-SIPRNET accounts and to use their Army Knowledge Online Web mail address within all Army business processes; adds policy on network operations and the operation and management of the Army Enterprise Infostructure; provides further guidance on International Maritime Satellite communications equipment; names Network Enterprise Technology Command as the Army's exclusive agent for Federal Telecommunications System service contracts and requires Network Enterprise Technology Command authorization to obtain all base communications services (chap 6).

- Adds visual information responsibilities for Network Enterprise Technology Command/9th Army Signal Command; reassigns some duties from major Army commanders to regional visual information managers; specifies equipment not to be purchased through the Visual Information Systems Program; clarifies multimedia productions; and implements Department of Defense Instruction 5040.7, which requires that all visual information multimedia/visual information productions be reviewed for public exhibition prior to distribution (chap 7).

- Expands the definition of records; clarifies records administrator responsibilities at the major Army command level; identifies baseline services to be provided by the Installation Management Agency; introduces the Army Records Information Management System; and clarifies information about the Vital Records program (chap 8).

- Updates references (app A).
- Provides the list of telecommunications services authorized for installation activities (app B).
- Adds items to the management control checklist (app C).
- Updates acronyms, references, and definition of terms (glossary).

Headquarters
Department of the Army
Washington, DC
15 July 2005

*Army Regulation 25–1

Effective 15 August 2005

Information Management

Army Knowledge Management and Information Technology

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army

History. This publication is a rapid action revision.

Summary. This regulation establishes the 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. The regulation implements Public Law 104–106, the Clinger–Cohen Act of 1996 (formerly Division E, Information Technology Management Reform Act, Defense Authorization Act for 1996), and establishes the Army's Chief Information Officer. The full scope of Chief Information Officer responsibilities and management processes is delineated throughout this regulation. These management processes involve strategic planning, business process analysis and improvement, assessment of proposed systems, resource management (to include investment strategy), performance measurements, acquisition, and training.

Applicability. This regulation applies to the Active Army, the Army National Guard of the United States/Army National Guard, and the United States Army Reserve unless otherwise stated. Portions of this regulation, which prescribes 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 Army 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 a direct reporting unit or field operating agency of the proponent 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 Army Regulation 25–30 for specific guidance.

Army management control process. This regulation contains management control provisions in accordance with Army Regulation 11–2 and identifies key management controls that must be evaluated (see app 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, ATTN: SAIS–EIG, 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 Chief Information Officer/G–6, ATTN: SAIS–EIG, 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 of the United States/Army National Guard, and the United States Army Reserve.

*This regulation supersedes AR 25–1, dated 30 June 2004.

UNCLASSIFIED

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Responsibilities • 1–4, *page 1*
Recordkeeping requirements • 1–5, *page 1*
Managing information resources and IT • 1–6, *page 1*
Information as a resource • 1–7, *page 1*
Army Knowledge Management • 1–8, *page 2*
Information transmission economy • 1–9, *page 2*
Use of IT to improve mission efficiency and effectiveness • 1–10, *page 3*
User/customer focus and the relationship between the customer and the IT community • 1–11, *page 3*
Ensuring quality of information disseminated to the public • 1–12, *page 3*

Chapter 2
Responsibilities, *page 4*
The Army Chief Information Officer/G–6 • 2–1, *page 4*
The NETCOM/9th ASC • 2–2, *page 6*
Principal HQDA officials • 2–3, *page 7*
ASA(FM&C) • 2–4, *page 8*
ASA(ALT) • 2–5, *page 8*
The Office of General Counsel • 2–6, *page 8*
The Administrative Assistant to the Secretary of the Army • 2–7, *page 8*
The Chief of Public Affairs • 2–8, *page 9*
The Director of the Army Staff • 2–9, *page 9*
The Deputy Chief of Staff, G–1 • 2–10, *page 9*
The Deputy Chief of Staff, G–2 • 2–11, *page 9*
The Deputy Chief of Staff, G–3 • 2–12, *page 10*
The Deputy Chief of Staff, G–8 • 2–13, *page 10*
Assistant Chief of Staff for Installation Management • 2–14, *page 10*
The Judge Advocate General • 2–15, *page 10*
MACOM commanders • 2–16, *page 10*
Commanding General, U.S. Army Training and Doctrine Command • 2–17, *page 11*
Commanding General, U.S. Army Materiel Command • 2–18, *page 11*
Commanding General, U.S. Army Forces Command • 2–19, *page 11*
Commanding General, United States Army Special Operations Command • 2–20, *page 12*
Commanding General, U.S. Army Intelligence and Security Command • 2–21, *page 12*
The Army Surgeon General/Commanding General, U.S. Army Medical Command • 2–22, *page 12*
Commanding General, United States Army Corps of Engineers • 2–23, *page 12*
Commanders of the Army Component combatant commands • 2–24, *page 12*
Commanding General, U.S. Army Reserve Command and the Chief, National Guard Bureau • 2–25, *page 13*
Commanders or directors of MSCs, field operating agencies, DRUs, separately authorized activities, tenant, and satellite organizations • 2–26, *page 13*
State Area Command, U.S. Army Reserve Command, or comparable-level community commanders • 2–27, *page 13*
Program, project, and product managers and IT materiel developers • 2–28, *page 13*
PEOs and direct-reporting PMs • 2–29, *page 14*

Chapter 3
CIO Management, *page 14*
General • 3–1, *page 14*
Information management organizations below HQDA • 3–2, *page 14*

Contents—Continued

IM/IT resource management • 3–3, *page 15*
Process analysis and business/functional process improvement • 3–4, *page 17*
CIO validation of requirements • 3–5, *page 18*
IT performance measurements • 3–6, *page 18*
IT acquisition process • 3–7, *page 19*
IM/IT human capital management • 3–8, *page 19*
Registry for major information systems inventory, reduction, webification, and security • 3–9, *page 20*

Chapter 4
The Army Enterprise Architecture, *page 20*
Introduction • 4–1, *page 20*
AEA structure • 4–2, *page 20*
Operational View (OV) • 4–3, *page 21*
System View (SV) • 4–4, *page 21*
Technical View (TV) • 4–5, *page 21*
Use of Architecture information validation and compliance tools • 4–6, *page 21*
Army Net-Centric Data Management Program • 4–7, *page 21*
Army data standards management • 4–8, *page 22*
Authoritative data sources (ADSs) • 4–9, *page 23*
Enterprise identifiers (EIDs) • 4–10, *page 23*
Information exchange systems specifications (IESSs) • 4–11, *page 23*
Extensible Markup Language (XML) • 4–12, *page 24*

Chapter 5
Information Assurance, *page 24*
Mission • 5–1, *page 24*
Management structure for information assurance • 5–2, *page 25*
Information system certification/accreditation • 5–3, *page 25*
Physical security • 5–4, *page 26*
Software security • 5–5, *page 26*
Hardware security • 5–6, *page 26*
Procedural security • 5–7, *page 26*
Personnel security • 5–8, *page 26*
Communications security • 5–9, *page 27*
Risk management • 5–10, *page 27*
Army Web Risk Assessment Cell • 5–11, *page 27*

Chapter 6
Command, Control, Communications, and Computers/Information Technology Support and Services, *page 27*
IT support principles • 6–1, *page 27*
Computing services • 6–2, *page 31*
Network operations (NETOPS) • 6–3, *page 34*
Telecommunications systems and services • 6–4, *page 35*
Long-haul and deployable communications • 6–5, *page 46*
IT support for military construction (MILCON) • 6–6, *page 48*

Chapter 7
Visual Information, *page 49*
General • 7–1, *page 49*
Combat camera (COMCAM) • 7–2, *page 50*
VI responsibilities • 7–3, *page 50*
VI activities • 7–4, *page 51*
VI activity operations • 7–5, *page 52*
Automated information management system • 7–6, *page 52*

Contents—Continued

Equipment and systems • 7–7, *page 52*
Products • 7–8, *page 54*
Services • 7–9, *page 57*
VI records management • 7–10, *page 57*
VI documentation (VIDOC) program • 7–11, *page 58*
Restrictions • 7–12, *page 58*

Chapter 8
Records Management Policy, *page 60*
Mission • 8–1, *page 60*
Management concept • 8–2, *page 60*
Life-cycle management of records • 8–3, *page 63*
Tenets • 8–4, *page 64*
Major subprograms • 8–5, *page 64*
General policies • 8–6, *page 65*
Record media • 8–7, *page 67*
Electronic records management • 8–8, *page 68*

Chapter 9
Publications and Printing, *page 68*
Management concept • 9–1, *page 68*
Central configuration management • 9–2, *page 68*
Statutory restrictions for publications • 9–3, *page 68*
Statutory requirements for printing • 9–4, *page 69*
Requisitioning printing • 9–5, *page 69*

Appendixes

A. References, *page 71*

B. Telecommunications Services Authorized for Specific Activities, *page 80*

C. Management Control Evaluation Checklist, *page 83*

Table List

Table 7–1: Types of VI Activities, *page 51*

Glossary

Chapter 1
Introduction

1–1. Purpose

This regulation establishes the 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, business systems, and (except as noted) national security systems developed or purchased by the Department of Army. It implements the provisions of Public Law (P.L.) 104–106, Clinger–Cohen Act of 1996 (formerly Division E, Information Technology Management Reform Act, Defense Authorization Act of 1996); the Paperwork Reduction Act of 1995 (as amended); Department of Defense Directive (DODD) 8000.1; and other related Federal laws and DOD directives. It addresses the application of knowledge management concepts and systems across the Army, the management of information as an Army resource, the technology supporting information requirements, and the resources supporting command, control, communications, and computers (C4)/IT. This regulation does not apply directly to information systems acquired under the National Foreign Intelligence Program 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 terms used in this publication are explained in the glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

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 IT

a. 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. IT refers to 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 voice, image, data, or information by the Federal Government. IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

c. IT embedded in or integral to weapon systems, machines, medical instrumentation, servomechanisms, training devices, or test and evaluation (T&E) 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 hard copy and will be 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, information will be managed as a shared resource and made 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. Requirements for information and the supporting IT will be carefully planned. IT and related investments will be evaluated in terms of their support of Army enterprise 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, or otherwise subject to a Freedom of Information Act (FOIA) or Privacy Act exemption or otherwise considered to be sensitive under AR 25–2. It is either routinely made available to the public or provided 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 data or information is defined as personally identifiable and

subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive. Unclassified FOIA-exempt information or data is nonpublic and designated "For Official Use Only." Nonpublic information or data may be shared for official purposes within the Army, 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) portal or other 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 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, 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 "infostructure" capabilities across the Army so that warfighters and business stewards can act quickly and decisively. AKM connects people, knowledge, and technologies.

a. The goals are—

(1) Adopt governance and cultural changes to become a knowledge-based organization. Integrate knowledge management and best business practices into Army processes to promote the knowledge-based force.

(2) Manage the infostructure as an enterprise to enhance capabilities and efficiencies.

(3) Institutionalize AKO as the enterprise portal to provide universal, secure access for the entire Army.

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

b. The end result of the AKM strategy is to manage the Army infostructure as an enterprise and to align the Army with the Global Information Grid (GIG) and the Future Force.

c. As appropriate, Army organizations will develop communities of practice (CoPs) as 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) CoPs may also be referred to as structured professional forums, knowledge networks, or collaborative environments.

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

d. The use of AKO and Army Knowledge Online–secret Internet protocol router network (SIPRNET) (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 or as otherwise prescribed by the Department of the Army (DA). (See also para 6–2*h*.)

e. AKO is the single Army portal for authenticating users to gain access to Army enterprise systems and subportals. (See also para 6–4*n*(2).)

f. Active, Reserve, National Guard, civilian, and appropriate contractor personnel will make full use of AKO 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.

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

a. The use of IT facilitates the streamlining of business operations. Improvements in customer support, internal processes, and supplier relationships are achieved by applying IT to specific business practices. The Army has adopted a number of commercial best practices under a strategy known as Electronic Army (e-Army). The e-Army approach emphasizes IT-enabled end-to-end process transformation and the creation of Army-wide enterprise processes in support of the Future Force. The process transformation is based on a "one network, one portal, one database" enterprise philosophy. The approach promotes self-service Web-based applications and support for a paperless office environment. Implementation of e-Army concepts to streamline processes will provide capabilities to save manpower, reduce redundancy, increase accuracy, speed transmission, increase availability of information, and allow functions to be performed that would be impractical or impossible without using e-Army methodologies. When appropriate and cost-effective, e-Army concepts will be used to support Army business processes.

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.

c. Process improvement and the integration of information systems throughout the organization increases efficiency and results in improved coordination among functional areas and the availability of consistent information. The Army will work toward total process transformation, implementing integrated, enterprise-wide, multifunctional, end-to-end services that provide reliable information throughout the enterprise.

d. Retention of information stored in electronically readable format for the prescribed period of time ensures its availability for use in Army decision-making and business processes.

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

a. The IT community provides information capabilities and services to the larger Army and Government community. IT capabilities and services are not ends in themselves. Ultimately, they have value only in the support of the warfighter or to those who provide other forms of support to the warfighter. 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 process must foster a similar dialogue. Although primary responsibility must be assigned for the various aspects of that process, both parties must remain actively engaged for it 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 IT management 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 in 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. P.L. 106–554, the Federal Information Quality Act (Section 515, of the Treasury and General Government Appropriations Act for Fiscal Year 2001), requires Federal agencies to maintain a basic standard of quality (objectivity, utility, and integrity) and take appropriate steps to incorporate information quality criteria into public information dissemination practices. (See Army guidance at http://www.army.mil/usapa/epubs/pdf/i25_03_2.pdf as well as DOD guidance on information quality at http://www.army.mil/CIOG6/references/policy/docs/U01678–03.pdf.) Army organizations will follow 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."

b. 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 use of 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 CIO/G–6 will—

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

b. Provide functional policy and guidance on C4/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 all information systems.

(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 information technologies to promote Army efficiency and productivity in all of its activities.

(4) Serve as functional proponent for the business/functional process improvement program with a C4/IT impact.

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

(6) Provide the information technology management (ITM) strategic planning perspective to the Army strategic planning process, to include alignment of the C4/IT investment strategy with Army strategic vision, goals, and objectives.

(7) Develop and implement IT performance measurements.

(8) Establish and implement Army-wide IT architecture.

(9) Serve as member of the Federal CIO Council and the Defense CIO Executive Board.

(10) Chair the Army CIO Executive Board.

(11) Provide oversight of the Army Information Assurance Program.

(12) Provide oversight for National Security Systems (NSS) (that is, all systems that have C4/IT requirements and include such functions as requirements review, prioritization, resource management, and acquisition).

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

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) P. L. 105–277 (Title XVII—The Government Paperwork Elimination Act).

(2) Title 15, Section 7001, United States Code (15 USC 7001) (2000), Electronic Signatures in Global and National Commerce Act (also known as the "E–Sign Act").

(3) 44 USC, Chapter 35, Coordination of Federal Information Policy (P.L. 104–13, Paperwork Reduction Act of 1995).

(4) 40 USC 1401 (P.L. 100–235, Computer Security Act of 1987).

(5) 47 USC 151, 157, 158, 201, 203, 552, 553, 571–73 (P.L. 104–104, Telecommunication Act of 1996).

(6) P.L. 104–106, Clinger–Cohen Act of 1996 (formerly Division E, Information Technology Management Reform Act of the Defense Authorization Act of 1996).

(7) P.L. 106–398, Fiscal Year (FY) 2001 National Defense Authorization Act, Iitle X, Subtitle G (Government Information Security Reform Act).

(8) P.L. 107–347, E–Government Act of 2002.

(9) Executive Order (EO) 13011, Federal Information Technology.

(10) EO 13103, Computer Software Piracy.

(11) 10 USC 2224 (Annual Information Assurance Report to Congress).

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

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

(1) 44 USC 211, chapters 29, 31, and 33 (P.L. 94–575, Federal Records Management).

(2) 44 USC Chapter 35.

(3) 5 USC 552 (Freedom of Information Act).

(4) 5 USC 552a (Privacy Act of 1974).

(5) P.L. 97–375 (Congressional Reports Elimination Act of 1982).

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

i. Support the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)) (Army Acquisition Executive) in the acquisition of information systems and on aspects of other major systems, 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) Work Army Acquisition Corps IT issues through the Acquisition Support Center.

j. As the Army Enterprise Architect and Army Technical Architect, integrate Army-wide IT architectures.

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 4–7 through 4–12.)

l. Manage and execute the e-Army/Electronic Business/Electronic Government Programs, including review, approval, and general oversight of e-Army activities, initiatives, and solutions.

m. Provide oversight and direction for 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) Compatibility and interoperability of tactical command, control, communications, and intelligence (C3I) systems.

(4) T&E for the Joint Tactical Communications Program.

(5) Oversight for tactical switched systems and joint network management.

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

(7) Member of the Committee on National Security Systems.

(8) Army "lead" for Joint Transformation Communication Program.

o. Serve as senior authority for Army visual information (VI) and manage nontactical VI and multimedia products per OMB Cir A–130, DODD 5040.2, DOD Instruction (DODI) 5040.4, DODD 5040.5, DODI 5040.6, DODI 5040.7, and 36 Code of Federal Regulations (36 CFR), 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 IM personnel are addressed and that career development plans, programs, and objectives are established. Duties include—

(1) Serve as the functional chief for the Information Technology Management Career Program (CP–34).

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

q. As the HQDA proponent responsible for the information systems supporting C4/IT programs—

(1) Serve as the Army focal point for C4/IT system (to include NSS) issues; receive, coordinate, and integrate these issues; and ensure the integration of systems and development efforts that cross functional and/or technical lines.

(2) Participate and provide representation in Planning, Programming, Budgeting, and Execution (PPBE) process decision groups; exercise centralized oversight of C4/IT expenditures for all appropriations.

(3) Develop, coordinate, and implement a C4/IT capital planning and investment program.

(4) Ensure C4/IT system conformance to the approved Joint Technical Architecture–Army (JTA–A), Operational Architecture (OA), Technical Architecture (TA), and Systems Architecture (SA); coordinate and support the priorities within C4/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 corporate management processes and their associated information systems.

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

(7) Coordinate resource requirements for C4/IT support activities.

(8) Facilitate adoption of approved standards for information and information system interoperability with joint, unified, combined, Federal Government, and other Army systems, as required.

(9) Ensure interoperability among C2 systems and coordinate Army survival, recovery, and reconstitution system and continuity of operations plans (COOP) support requirements.

(10) Ensure that essential information services in support of DA COOP are available to alternate sites of HQDA agencies and MACOMs, major subordinate commands (MSCs), and installations.

(11) In conjunction with the Office of the Deputy Chief of Staff, G–1 (DCS, G–1), ensure that records management requirements are included in the life cycle of information systems beginning at the initial milestone.

r. Provide oversight of the planning and programming 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.

2–2. The NETCOM/9th ASC

The NETCOM/9th ASC, as a direct reporting unit to the CIO/G–6, will—

a. Serve as the single authority assigned to operate, manage, and defend the Army's infostructure at the enterprise level.

(1) Manage the "army.mil" and "army.smil.mil" Internet domain 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) Operate, manage, and defend the Army Enterprise Portals.

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

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

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

(8) Conduct Army Infostructure Architecture and Systems Design Review.

(9) Manage enterprise-level C4/IT common user services and signal forces.

(10) Exercise technical control (TECHCON) over all organizations that operate and maintain portions of the AEI.

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

d. Operate, sustain, and defend the Army's portion of the GIG.

e. Exercise TECHCON and configuration management authority for the Army's networks, systems, and functional processing centers. Configuration management authority provides the governance guidelines and direction for which all Army enterprise IT assets are configured.

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

(2) Provide centralized management and TECHCON of C4/IT belonging to or under the purview of regional CIOs (RCIOs), installation directors of information management (DOIMs), MACOMs, functional activities, and communities of practice C4/IT.

f. Manage the Army Information Assurance Program.

g. Serve as the responsible official for joint network management.

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

i. Serve as functional proponent for Army network operations (NETOPS).

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

k. Manage and provide personnel resources for the NETCOM liaison staff for the Installation Management Agency (IMA) headquarters and the RCIO staff for the IMA regional directors.

l. Serve as the C4/IT Service Management Program operational authority for the Army in support of the CIO/G–6.

m. Provide a central VI office for the execution of CIO/G–6 VI programs and functions.

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

o. 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 requests for service.

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

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

q. Provide a C4/IT operational engineering force with worldwide deployment capability to provide quick-reaction

support to plan, integrate, install, operate, and maintain C4 systems from the power projection platform to the tactical theater of operations.

r. 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.

s. 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.

(6) Ensure Army compliance with DISA telecommunications procedures in accordance with DISA Circular 310–130–1.

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

u. Manage the administration of amateur radio operations and the Army Military Affiliate Radio System (MARS) program, including acquisition, storage, distribution, and accounting for MARS surplus property.

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

w. Serve as Army responsible official for operating and maintaining designated Defense Red Switch Network, Army's portion of Military Satellite Communications (MILSATCOM) for Defense Satellite Communications, Defense Information Infrastructure (Microwave and Fiber Optic Cable Systems), unclassified but sensitive Internet protocol router network (NIPRNET) and SIPRNET routers, Defense Messaging System operational requirements, Defense Switched Network, and operational requirements for combatant command communications teams in support of the Army.

x. Serve as the focal point for intelligence support to identify and analyze threats to the AEI and its enabling technologies.

2–3. Principal HQDA officials

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

a. Serve as HQDA proponent for information requirements within assigned functional area of responsibility.

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

c. Provide, as required, representation to the Army CIO Executive Board 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 C4/IT capital planning and investment strategy process. (Refer to para 3–3.)

f. Request and defend the information requirement and supporting resources needed for the development, deployment, operation, security, logistics support, and modification of information systems through the PPBE process.

g. Develop AEA architecture 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. Develop, coordinate, and submit to U.S. Army Training and Doctrine Command (TRADOC) the OA data in support of warfighting capabilities.

i. Use electronic business/government technologies to the maximum extent practicable to promote the goal of a paper-free (or near paper-free) business environment within the Army.

j. Appoint in writing a records official to manage the internal records of the organization and its subelements. Each official will act as a point of contact (POC) for recordkeeping requirements of the respective functional area and will perform duties as prescribed in paragraph 8–2*g*.

k. Identify functional requirements for the Army Enterprise portals (AKO and AKO–S) and participate, as required, in AKO Configuration Control Board (CCB) activities.

2–4. ASA(FM&C)

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 Information Technology Budget, to include Exhibit 300's, IT–1, and Exhibit 53. ASA(FM&C), in concert with the CIO/G–6, will jointly certify Army IT budget submission.

2–5. ASA(ALT)

Responsibilities for the ASA(ALT) are defined in AR 70–1 and in paragraph 2–3. Those ASA(ALT) responsibilities unique to C4/IT are listed below:

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

b. Direct and review communications, command, control, and intelligence 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 information systems required for strategic and tactical programs.

d. Execute the RDT&E and procurement portions of C4/IT programs and budgets.

e. Oversee the C4/IT technology base relative to impacts to the Army Industrial Base.

f. Review C4/IT system readiness for testing during full-scale development.

g. Review and approve for acquisition category (ACAT) ID and ACAT IAM programs the Army position 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.)

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

i. As Executive Architect for SA, validate Army SAs and develop integrated system architectures in accordance with Army priorities.

j. Act as final decision authority to resolve conflicts among SA profiles.

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

2–6. The Office of General Counsel

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

a. Advise on legal issues that arise during information system acquisitions.

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

2–7. 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 paragraph 2–3—

a. 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 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.

b. 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 a MACOM.

c. Serve as the authenticating official for all Departmental publications except policy publications, which are authenticated by the SECARMY.

d. 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.

e. 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.

f. Manage IT for the internal use of HQDA. 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 also—

(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 responsibilities for HQDA as those assigned to the MACOM commanders (see para 2–16).

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

g. Supervise and operate the Defense Telecommunication Service–Washington (DTS–W) per DODD 4640.7 and DODI 5335.1.

h. Serve as the records official for HQDA as a MACOM.

2–8. 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.

2–9. The Director of the Army Staff

The Director of the Army Staff will accomplish all the C4/IT responsibilities assigned to the principal HQDA officials for the OCSA (see para 2–3).

2–10. The Deputy Chief of Staff, G–1

The DCS, G–1 will, in addition to the responsibilities in paragraph 2–3—

a. Serve as Archivist of the Army.

b. Serve as the senior Army official for records management and its various subprograms.

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

d. Promulgate policy and procedures for the records management program and its various subprograms, to include—

(1) Official mail and distribution.

(2) Correspondence management.

(3) Privacy Act and systems notices.

(4) Freedom of Information Act.

(5) Vital records.

(6) Army Records Information Management System (ARIMS).

(7) Record collections.

(8) Management Information Control System.

(9) Army Rulemaking Program.

(10) Terminology, Abbreviations, and Brevity Code Management.

e. Implement declassification requirements in accordance with EO 12958.

f. 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.

g. 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 Office of Management and Budget. (See also para 1–12.)

2–11. The Deputy Chief of Staff, G–2

The DCS, G–2 will, in addition to duties listed in paragraph 2–3—

a. Provide policy to the CIO/G–6 for the C4/IT activities of the intelligence community and advise the CIO/G–6 accordingly.

b. Represent for the CIO the National Foreign Intelligence Program (NFIP)–funded C4/IT efforts under the Defense Agency NFIP Program Manager's programs and other Intelligence CIO programs. Major C4/IT NFIP/intelligence program concerns will be brought to the CIO's attention.

c. Provide staff supervision for counter-intelligence, information systems security monitoring, and counter-HUMINT (human intelligence) activities in support of Army information assurance (IA) efforts.

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

e. Serve as staff proponent for sensitive compartmented information (SCI) IA policy and procedures pertaining to information systems processing intelligence information.

f. Develop and implement policy and procedures for security certification and accreditation for information systems processing intelligence data.

g. Provide oversight for NFIP or other intelligence program intelligence systems.

2–12. The Deputy Chief of Staff, G–3

The DCS, G–3 will, in addition to duties listed in paragraph 2–3—

a. Exercise proponency for C2.

b. Ensure that Army-wide C4/IT priorities are supportive of overall Army-wide priorities.

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

d. Determine requirements for operational information at HQDA.

e. Establish priorities for developing and acquiring materiel and force structure in support of C4/IT programs.

f. Functionally integrate all major Army C4/IT requirements.

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

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

i. 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.

2–13. The Deputy Chief of Staff, G–8

The DCS, G–8, in addition to the responsibilities in paragraph 2–3, will serve as the approval authority for changes to the base case system in the Intra-Army Interoperability Certification (IAIC) process.

2–14. 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 base operations support (BOS) services, including daily IT support requirements, to installation tenants through the IMA.

b. Integrate the NETCOM/9th ASC-developed list of C4/IT services into the Army baseline services.

c. Plan and program IT resources to support the installation BOS C4/IT requirements.

d. Provide HQDA oversight of the U.S. Army Community and Family Support Center (CFSC), which serves as the proponent and focal point for matters concerning Army morale, welfare, and recreation (MWR) information systems.

2–15. The Judge Advocate General

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

a. Provide C4/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.

2–16. MACOM commanders

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

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

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

c. Identify the MACOM's C4/IT requirements and ensure that mission requirements are validated, coordinated, and integrated per AR 71–9. BOS C4/IT requirements will be documented per AR 70–1 and forwarded via the respective DOIM.

d. Manage the MACOM mission-related IM requirements throughout their life cycle, including those requirements for subordinate organizations located on other installations for C4/IT requirements not included as part of established BASOPS support.

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

f. Fund MACOM-unique IT requirements in support of mission and business, including long-haul communications, information assurance, and other C4/IT requirements not identified as part of BASOPS support.

g. Coordinate IT plans, programs, and requirements with appropriate information assurance managers per AR 25–2.

h. Assess all assigned programs prior to their milestone reviews and recommend programs to be continued, modified, or terminated as part of the milestone reviews for milestones A, B, and C.

i. Obtain certificates of networthiness and certificates to operate for MACOM-unique C4/IT systems.

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

k. Ensure JTA–A compliance for designated systems.

l. Implement the ANCDMP as guided by the Army CDAd. (See chap 4 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. Appoint a command records administrator to oversee the Records Management Program throughout the command.

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 every 3 years.

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

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

s. Administer the MACOM-level IT performance measurements.

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

The Commanding General (CG), TRADOC will, in addition to the duties listed in paragraph 2–16—

a. Formulate IM/IT doctrine for the Army.

b. Serve as the Army Operational Architect. (See also para 4–3.)

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 C4/C3 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 2–16—

a. Provide functional support to the C4/IT PEOs and PMs as designated by the Army Acquisition Executive (AAE).

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

c. Establish and maintain configuration management of the C4/IT materiel component systems based on top-level, functional, and subsystem and interface specifications.

d. Ensure that C4/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.

e. Prepare, maintain, and promulgate to the C4/IT materiel developers the requirements and the systems materiel integration and interoperability plan.

f. Validate information systems technical requirements and associated cost estimates for all Army MILCON projects, except for those projects specifically designated to U.S. Army Forces Command (FORSCOM).

g. Develop and acquire technical and support solutions for information systems for which AMC is the assigned materiel developer.

h. Plan, program, and conduct new equipment training for assigned systems and recommend required training to TRADOC, U.S. Army Medical Command (MEDCOM), TJAG, and the Chaplain Corps for inclusion in their Army schools programs.

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

j. Coordinate C4/IT systems designs with TRADOC.

k. Provide input and trade-off analysis to TRADOC as required for developing the warfighting Operational View (OV).

l. Perform system engineering for the combat service support battlefield functional area of the command, control, and subordinate systems (CCS2).

m. Develop technical specifications and acquisition requirements packages for standard (indefinite delivery/indefinite quantity) contracts for acquisition of commonly used IT assets, except for VI assets.

n. Develop the Army logistics systems' integrated business processes.

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

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

a. Exercise operational control over NETCOM/9th ASC for tactical continental United States (CONUS) force provisioning.

b. Designate a COMCAM planner to develop and maintain operation plans.

c. Coordinate for 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. Commanding General, U.S. Army Intelligence and Security Command

The CG, U.S. Army Intelligence and Security Command (INSCOM) will, in addition to the duties listed in paragraph 2–16—

a. 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.

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

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

d. Manage and execute NFIP and intelligence program-funded intelligence systems maintained by the command.

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

f. Coordinate C4/IT systems designs of proponent systems with TRADOC.

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

h. Provide relevant information and intelligence to the CG, NETCOM/9th ASC (in his or her capacity as the Deputy Commander Army Forces-Computer Network Defense) to defend the Army portion of the GIG.

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

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

a. Provide C4/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 of 1996 (HIPAA) for the protection of health information, to include specific security measures required to support HIPAA standards.

2–23. Commanding General, United States Army Corps of Engineers

The CG, United States Army Corps of Engineers (USACE) will, in addition to the duties listed in paragraph 2–16—

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 military and Civil Works data elements.

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

2–24. Commanders of the Army Component combatant commands

These commanders will—

a. Develop combat and materiel development plans for C4/IT elements within their command and provide the plans to TRADOC, AMC, and FORSCOM as required.

b. Provide data pertaining to all C4/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 C4/IT combat and materiel developments.

d. Maintain POCs with staff elements that recommend to TRADOC, AMC, FORSCOM, INSCOM, or MEDCOM new or improved C4/IT-related doctrine, force structure, training, and materiel.

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

f. Integrate tactical VI (COMCAM) requirements and activities into operational plans per Joint Operations Planning System, Volume I and IV. 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.

2–25. Commanding General, U.S. Army Reserve Command and the Chief, National Guard Bureau

The Commanding General, Army Reserve Command, and the Chief, National Guard Bureau have the same responsibilities as specified in paragraphs 2–14*a* and *c* and 2–16.

2–26. Commanders or directors of MSCs, field operating agencies, DRUs, separately authorized activities, tenant, and satellite organizations

Commanders or directors of MSCs, field operating agencies (FOAs), DRUs, 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 mission, size, responsibilities, 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 MACOM level.

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 BOS C4/IT common services.

(3) Designate in writing a subordinate organization records administrator who will perform duties as described in paragraph 8–2*g*.

2–27. State Area Command, U.S. Army Reserve Command, or comparable-level community commanders

State Area Command (STARC), U.S. Army Reserve Command, 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 Base-Level 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 nontactical VI documentation support within VI activity capabilities and request additional support through the RCIO VI manager when local capabilities cannot meet requirements.

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

2–28. Program, project, and product managers and IT materiel developers

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

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

(1) Develop architectures and architecture products for assigned systems under their purview.

(2) Design or acquire systems within 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) Coordinate their systems architectures with MACOMs, RCIOs, and DOIMs prior to fielding systems.

b. Coordinate fielding plans for their systems with senior IM officials of gaining commands and installations 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 for approval any intended initiatives or expenditures over $1 million (before obligation) to the Under Secretary of Defense Business Moderation and System Integration Office.

g. Ensure compliance with the Army's Networthiness Program for all PM-developed C4/IT systems.

2–29. PEOs and direct-reporting PMs

PEOs and direct-reporting PMs will—

a. Develop AEA architectures (OV, TV, and SV) and act as the integrator for system of systems under their purview and coordinate with CIO/G–6.

b. Develop and coordinate architecture data as input to AEA.

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 for approval any intended initiatives or expenditures over $1 million (before obligation) to the Under Secretary of Defense Business Moderation and System Integration Office.

f. Ensure records management requirements are included in systems throughout their life cycle. Ensure compliance with the Army's Networthiness Programs for all PM-developed C4/IT systems.

Chapter 3
CIO Management

3–1. General

The Clinger–Cohen Act of 1996 (P.L. 104–106) established the position of CIO in executive agencies. CIO management focuses on those policies, processes, and organizational responsibilities necessary to accomplish the information resources management (IRM) missions defined as primary 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, and IT workforce. This chapter covers the required participation of HQDA, MACOMs, regions, installations, and other Army activities in executing the IRM processes and assisting the CIO. All statements regarding the CIO refer to the Army-level CIO unless otherwise indicated.

a. The CIO/G–6 is the only federally mandated CIO in the Army.

b. A CIO's primary responsibility is IRM. Governing legislation cited in paragraph 2–1 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, consistent with established investment decisions and priorities. The full spectrum of CIO responsibilities (including IM/IT and NSS) is delineated throughout this regulation.

c. This chapter details the CIO's primary responsibilities and applicable policy. Other CIO responsibilities and policy are delineated in other chapters throughout this regulation. In addition to CIO responsibilities in the Clinger–Cohen Act, the SECARMY directed other duties. These include validating warfighting requirements and undertaking the resourcing and prioritization of individual IT programs in coordination with the DCS, G–3 and subject to the oversight, review, and approval of the ASA(FM&C).

d. The CIO process will not routinely address IT systems that are funded under the NFIP or other intelligence programs. The DCS, G–2 will represent Army NFIP-funded C4/IT under the DOD and NFIP program manager's programs. The DCS, G–2 will bring any C4/IT-related NFIP concerns to the CIO's attention.

e. The Army CIO Executive Board plays a key role in the management and execution of CIO missions. It 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 to conduct analyses, research, or accomplish a given task. These groups will report recommendations/findings directly to the board.

f. RCIOs/DOIMs will establish forums similar to the Army CIO Executive Board (for example, councils, boards, and so on) for the purpose of developing and implementing C4/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 HQDA

a. Subordinate organizations below HQDA. Subordinate organizations below HQDA, except as indicated below, may at their discretion designate the senior IM official as a "Chief Information Office" 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.

b. Regional CIOs (RCIOs). Every region under the IMA will have an RCIO. The director/commander of the NETCOM/9th ASC regional unit is "dual-hatted" as the RCIO of the respective IMA regional director. In addition, specific non-IMA entities (for example, the United States Army Reserve Command, Army National Guard (ARNG),

INSCOM, MEDCOM, USACE, CFSC) 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) Monitor shared and common-user IT systems within their region and provide technical control and oversight 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) Develop architectures for respective Army installations.

(8) Appoint records managers and official mail managers for regional and installation levels.

(9) Designate regional VI managers. (See also para 7–4.)

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

(11) Provide required information assurance support and oversight to DOIMs within their assigned region.

c. MACOMs. Every MACOM will have a senior IM official as a principal staff officer with CIO-like duties. The duties pertain to IT support of MACOM functions and exclude BASOPS support, except for the development of BASOPS requirements. (See para 2–16 for a detailed list of responsibilities.)

d. Major subordinate commands. MSCs may establish an equivalent IM official with the same staff responsibilities as a MACOM senior IM official. (See para 2–26 for more specific information.)

e. Installations. The installation information manager is designated the DOIM. There will be only one DOIM at an installation designated by the IMA garrison commander. The installation DOIM will be the focal point for providing IT support (to include long-haul, base communications (BASECOM) services and information assurance) and the single authority to validate purchase of information resources on the installation including all tenant organizations/activities.

(1) Other activities on an installation will not establish a DOIM but may have an IMO or other personnel 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.

(2) The STARC is equivalent to an installation. (See para 2–27 for more information.)

f. Other. Tenant and satellite organizations, separately authorized activities, Government-owned/contractor-operated facilities, regional support activities, U.S. Army Reserve regional readiness commands, FOAs, and major staff entities will designate an IMO. The IMO will identify their organization's information requirements to the supporting DOIM. These organizations will coordinate with the DOIM and respective RCIO as required for support agreements.

3–3. IM/IT resource management

The CIO/G–6 will review, prioritize, and support resourcing for C4/IT requirements for Army enterprise solutions during the planning, programming, budgeting, and execution processes.

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 publish the Army Modernization Plan (AMP), which provides specific information on and direction for battlefield and supporting systems. C4/IT modernization plans are in the AMP annexes.

(2) *HQDA C4/IT strategic planning.* The broadest strategic C4/IT perspective for the Army is in the AKM Strategic Plan and associated implementation documents. The Army Vision, the Army Transformation Vision, and AKM planning documents form the basis for the future direction of C4/IT.

(3) *Other C4/IT strategic planning.* Using the guidance from HQDA strategic plans, MACOMs, RCIOs, and HQDA proponents will develop their own strategic plans appropriate to their respective missions. MACOM/RCIO C4/IT strategic plans 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. These plans will form the basis for applicable resource requests to HQDA. C4/IT strategic plans should include, at a minimum, the organizational vision, core missions, goals, and priorities. These plans describe how the vision and goals support the Army strategic vision, missions, and goals; any architectural and webification developments; and how these and other existing or ongoing efforts conform to the AEA. They will also include any new business process improvement efforts that may result in an IT investment, performance measurements in conjunction with organizational processes, and new systems partnerships with other

organizations. The organization's investment strategy, server consolidation, acquisition strategy, and information assurance prerequisites are other areas for consideration. C4/IT planning guidance at subordinate organizations (below MACOM/RCIO level) is at the direction of the respective MACOM senior IM official, RCIO, or HQDA functional proponent, as applicable.

b. C4/IT capital planning and investment strategy. Capital planning provides the link between C4/IT investment and mission outcomes as required by the Clinger–Cohen Act of 1996. C4/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. The goals of capital planning are twofold: first, to make the best use of available funds to achieve strategic goals and objectives, and second, to manage a portfolio of capital assets to achieve performance goals with the lowest life-cycle cost and the least risk.

(1) The CIO/G–6 is responsible for the development and coordination of the C4/IT Investment Strategy Plan. The CIO/G–6 Resource Integration Directorate (SAIS–ZR) is responsible for managing the C4/IT Capital Planning and Investment Management (CPIM) process.

(2) The CPIM process includes selecting the C4/IT investments and establishing their priorities throughout the PPBE process and acquisition processes. The process addresses capability gaps, investment risks, and IT interdependencies across multiple areas of IT investments. The CPIM process and the resulting C4/IT investment strategy is 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 Clinger–Cohen Act.

(3) 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 C4/IT Capital Plan. The investment strategy uses a performance-based methodology and incorporates enterprise-wide 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.

(4) All C4/IT expenditures (centralized and noncentralized programs), 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, United States Army Reserve (USAR) and ARNG, IMA regions, MACOMs, DRUs, and installations. (See para 3–5 concerning the required review of nonwarfighting IT.)

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

c. Programming.

(1) CIO representatives at the colonel/GS–15 level will participate as members in program evaluation group (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, billpayers, 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 C4/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 life cycle) 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 C4/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.

d. Reporting of capital and other IT expenditures. The CIO will prepare and submit the IT budget on IT investments as part of the POM/budget estimate submission and the President's budget submission. Specific instructions are published in the Resource Formulation Guidance (available on the Data Analysis Query System on the ASA(FM&C) Web site: http://www.asafm.army.mil). See also DOD 7000.14–R, Vol. 2B, chapter 18.

e. Execution of C4/IT investments.

(1) HQDA proponents and MACOMs will execute their FY C4/IT budgets by selecting one of the following alternatives:

(a) Follow POM guidance and spend the programmed funds in 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 waiver for all IT expenditures using non-IT programmed funds that exceed the dollar thresholds as published in the annual resource guidance. Non-IT programmed dollars will not be spent on IT requirements without a CIO waiver.

(2) The third alternative assists the Army in ensuring that the HQDA proponents and MACOMs will curtail IT investments unless they have IT-programmed funds or a waiver from the Army CIO.

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

(4) Senior IM officials and HQDA proponents will monitor IT expenditures to comply with the conditions listed above. Additionally, IM officials and functional proponents will participate in the Army Knowledge Online Configuration Control Board as necessary to identify their requirements for AKO.

3–4. Process analysis and business/functional process improvement

a. Per the Clinger–Cohen Act, 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 MACOM, Defense, or 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 (BPR). 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 the installation level and above 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 (Clinger–Cohen Act). 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 information systems.

(10) Integrating duplicative information across processes.

(11) Creating an integrated environment to promote enterprise-wide 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 best practices and adopt, 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, Joint Chiefs of Staff Instruction (CJCSI) 3170.01D 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 nonwarfighting 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 or replacing office computers).

g. The Army Business Initiative Council (ABIC) was developed to improve the efficiency of DA business operations by identifying and implementing business initiatives that create savings to be reallocated to higher priority efforts

(that is, people, readiness, modernization, and transformation). Process improvement is a significant portion of the ABIC mission.

3–5. CIO validation of requirements

a. The CIO validates and the CSA approves all C4/IT warfighting requirements through the review of appropriate requirements documents. Warfighting C4/IT requirements are defined as C4/IT in direct use by, or in support of, the Army warfighter in training for and conducting operational missions (tactical or other) or connecting the warfighter to the sustaining base. Validation criteria will include—

(1) Determination that nonmateriel alternatives were judged to be inadequate per AR 71–9 and a process analysis (DOTMLPF analysis) has been completed to make this determination.

(2) A statement that all materiel solutions must be JTA–A compliant.

(3) Evaluation of emerging technologies.

(4) Inclusion of outcome-oriented performance measurements.

(5) Compliance with information assurance requirements.

(6) Inclusion of spectrum management criteria.

(7) Evaluation of a new or modified requirement against existing systems.

(8) Other criteria as appropriate.

b. The DCS, G–3 manages the requirements review process, including the Army Requirements Oversight Council and the Requirements Review Council (RRC). The CIO/G–6 participates as a member of these councils to represent the C4/IT perspective on the requirements review process.

(1) The CIO also reviews and validates BASOPS IT up to $10 million for those requirements not defined as warfighting IT. These requirements will be reviewed under the CPIM process and associated guidance.

(2) MACOMs will follow a similar process for reviewing their respective IT-related requirements.

3–6. IT performance measurements

a. IT performance measurement. Measuring IT performance is the process of assessing 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, culture change) and achieving at least the intended outcomes (mission effectiveness, 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 Readiness System (SRS) or the IT Metrics Program.

d. Performance measurements in requirement documents. Performance measures in support of warfighting materiel requirements with a C4/IT impact 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 Army-wide 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 SRS. Data from the Army Information Technology Registry (AITR) and the Base-Level IT Metrics Program (see *i*, below) will be used as input. IT measures at the Army enterprise level will ensure that—

(1) Investments are synchronized with overall DOD/Army mission priorities.

(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 MACOMs 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 Army-wide decisions.

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

(2) Performance will be customer-oriented.

h. Program/project level. Performance measures at the program/project level will assess progress toward accomplishing expected functional mission outcomes and results of C4/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 Base-Level IT Metrics Program. This program establishes the use of metrics to assess the current 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 an annual basis via the IT metrics database (http://doim.hqda.pentagon.mil/it_metrics/). Compiled IT metrics data will be used to identify mission capability shortfalls and to support the reallocation of IT investment resources.

j. Cost–benefit analysis. A cost–benefit analysis must be applied against any proposed performance measurement system.

3–7. IT acquisition process

The acquisition process begins when an organization's C4/IT needs are established in the appropriate capability document per AR 71–9. The acquisition process involves the description of capabilities to satisfy the needs, how the business process analysis was accomplished, outcome and output-oriented performance measurements, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the acquisition process per AR 70–1.

a. CIO oversight. The CIO will ensure that C4/IT is acquired and information resources are managed within an integrated framework. The CIO provides oversight for C4/IT systems during the acquisition approval process (AR 70–1).

b. CIO assessment. The CIO will recommend whether to continue, modify, or terminate Army programs with a C4/IT impact (Clinger–Cohen Act). CIO assessments, which incorporate multiple factors, will be conducted at the appropriate milestone.

(1) The CIO will assess all ACAT I and II programs. PMs of ACAT I and II programs will provide a self-assessment of compliance for every program to the CIO. (See AR 70–1 and DODI 5000.2 for additional information on acquisition program categories.)

(2) Non-ACAT investments for IT services will also be assessed. The CIO/G–6 will perform these assessments.

c. Information systems intra-Army interoperability. In accordance with CJCSI 6212.01C, the CIO/G–6 will ensure that information systems have the appropriate interfaces and data exchange requirements to achieve an integrated and interoperable warfighting capability in the Joint environment.

(1) The intra-Army interoperability certification process will be used to certify horizontal and vertical interoperability of all Army systems—regardless of their acquisition category—prior to their release for fielding. This process allows a smoother transition of new IT systems into the Army's operational through tactical-level C4/IT systems framework.

(2) The software blocking process is designed to facilitate the development and sustainment of system-of-systems interoperability in support of Army Transformation. (Refer to AR 70–1, para 8–6, for more complete policy on the software blocking process.) Organizations responsible for acquiring or maintaining specific systems with interoperability requirements will ensure compliance with the software blocking process. PEO/PMs will implement software blocking in their respective programs.

(3) The CIO/G–6 (SAIS–IOQ) will provide a memorandum of certification upon successful completion of certification testing. This certification memorandum does not preclude any other certification requirements. For changes to base case systems, the system proponent will submit requests to DCS, G–8. The DCS, G–8 reviews and approves the changes to the base case certification package. Upon approval, the DCS, G–8 will submit the certification package to the Central Technical Support Facility (CTSF) through the IAIC 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/.)

3–8. IM/IT human capital management

The CIO is responsible for the policy, oversight, and management of the Army Civilian ITM Career Program-34 (CP–34). 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 Information Resources Management College curricula.

3–9. Registry for major information systems inventory, reduction, webification, and security

a. The Army Information Technology Registry (AITR). The AITR is the Army's single, authoritative registry for IT systems. The AITR provides data on the inventory of Army systems/applications in order to manage compliance with AKM goals and applicable laws.

b. AITR entry. MACOMs and DA functional proponents will—

(1) Ensure that all Army applications/systems are correctly registered in the AITR and that all data fields are correctly updated at all times. Use AKO for AITR data entry. (See the AITR home page at https://www.us.army.mil/portal/jhtml/akm/wsd_home.jhtml.)

(2) Search the AITR for existing applications that can satisfy the requirement without further expenditure of funds prior to developing new applications or enhancing existing applications.

(3) Review and update AITR data at least semiannually.

c. Information system inventory.

(1) Per the E–Government Act of 2002 (P.L. 107–347), the Army is required to annually maintain an inventory of mission critical (MC) and mission essential (ME) systems and certify its accuracy and completeness. This list of systems becomes part of the DOD IT registry, which is used by OSD and entities outside of OSD for budget and other Congressional issues.

(2) The inventory will include an identification of the interfaces between each system and all other systems or networks and identify systems by either MC or ME.

(3) AITR will be used for systems entry and reporting.

d. Information systems reduction. The Army goal is to eliminate duplicative IT systems through streamlining and system consolidation. HQDA staff elements and MACOMs will report reduction plans in the AITR. standard commercial off-the-shelf (COTS) desktop office automation (that is, word processors, spreadsheets, and so on) is exempt from the reporting requirements of this document.

e. Information systems webification. All systems must be webified (that is, Web-enabled and linked to the AKO portal) or receive a waiver from the CIO/G–6. MACOMs and DA functional proponents must report webification status and future webification plans within the AITR.

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

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

Chapter 4
The Army Enterprise Architecture

4–1. Introduction

The AEA is the Army's framework/decision tool used to guide IT investments, acquisitions, and fielding of integrated system-of-systems capabilities. It includes guidance to develop integrated architectures by incorporating Operational Views (requirements), System Views, and Technical Views (technical standards) for Army tactical units, functional areas, and installations. This chapter outlines the AEA and implements IT-related guidance that applies to the development, promulgation, implementation, management, and maintenance of the AEA.

4–2. AEA structure

The AEA spans the Army enterprise from the institutional Army through the tactical level. The three areas comprising the AEA are as follows:

a. Army Knowledge Enterprise Architecture (AKEA). The AKEA is the blueprint for implementing the Army Knowledge Enterprise. Army knowledge is the interactivity of enterprise business practices, processes, and the associated application of DOTMLPF. The AKEA is the Army infostructure architecture that includes communications,

IM, computers, enterprise applications, and network operations. These five components map to the Net-Centric Operations and Warfare Reference Model. The AKEA is not applicable to IT that is embedded in devices with no external interfaces. The AKEA is the Army's portion of the DOD GIG.

b. Battle Command Architecture. Army Battle Command is defined as "the art and science of applying leadership and decision-making to achieve mission success." As the unifying element that integrates multiple capabilities to enable such success, the Army Battle Command Architecture has been organized to support Joint Capabilities and Integrated Development System (JCIDS), acquisition of System-of-Systems (SoS) and Family-of-Systems (FoS), software blocking, force development, and lessons learned from operations.

c. Army Business Enterprise Architecture (ABEA). The ABEA is the business processes and organizations that support the Army's warfighters. The ABEA defines structures for growth and changes, traces infrastructure requirements to business unit needs, phases in development and rollout of infrastructure, ensures infrastructure and application security, uses COTS components, and migrates current systems infrastructure. The ABEA ensures that the Army's transformation to net-centric warfare, enterprise application integration, and business process modernization align with the seven DOD BEA domains: Acquisition/Procurement, Human Resource Management, Finance and Accounting, Logistics, Technical Infrastructure, Installations and Environment, and Strategic Planning and Budgeting.

4–3. Operational View (OV)

OV products must be in conformance with the current approved Department of Defense Architecture Framework (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.

4–4. System View (SV)

SV products must be in conformance with 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.

4–5. Technical View (TV)

TV products must be in conformance with the current approved DODAF document. TVs provide the technical perspective of the force. AEA development will adhere to the following Army technical architecture community authority: CIO/G–6 is the Army's Executive Architect to serve as the Army's Technical Architect.

4–6. Use of Architecture information validation and compliance tools

a. The Architecture information validation and compliance tools support the validation and compliance testing of architecture information standards. The tools help developers implementing these standards detect and fix interoperability problems early in a system's development cycle by reducing cost and effort. In addition, developers do not need to develop duplicate tools.

b. The CIO/G–6 is responsible for the architecture information standards for DA.

c. All Army IT developers are mandated to use the following validation and compliance tools:

(1) Variable Message Format Test Tool for the JTA Variable Format Message Standard.

(2) United States Message Text Format Test Tool for the JTA US Message Text Format Standard.

(3) Combat Net Radio Protocol Test Tool for the JTA MIL–STD–188–220 Standard.

d. Tool technical information may be obtained through the U.S. Army Communications-Electronics Command (CECOM).

4–7. Army Net-Centric Data Management Program

a. The ANCDMP establishes policies and procedures intended to control the production and applicability of data standards required to ensure data interoperability for data exchanges among information systems 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 information systems throughout the Army, DOD, and the Federal Government. The ANCDMP implements the information standards portion of the JTA–A 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 para 1–7 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 any information system 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. PEOs, PMs, MACOMs, and agencies 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.

4–8. Army data standards management

a. Data standards (expressed as authoritative data sources (ADSs), information exchange standards specifications (IESSs), enterprise identifiers (EIDs), and eXtensible Markup Language (XML) and specified in the JTA–A and other guidance documents) 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 communities of interest (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 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 as to 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 5-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 Army-wide, COI DAds 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 information systems 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 information systems life cycle.

4–9. 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 information systems PMs and/or managers will implement Army enterprise-level ADSs in their information systems.

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 information systems.

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

4–10. 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 information systems to ensure maximum data integration and data interoperability.

(2) Use EIDs in legacy systems. Specified legacy systems (that is, those scheduled to remain active past FY04 and beyond), 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 (that is, those scheduled to become active in FY04 and beyond) 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.

4–11. 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 information systems, 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 information systems 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/materiel developer responsibilities:

(1) Each PM/materiel developer 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 materiel developer is responsible for integrating COTS software and ensuring interoperability with the existing metadata contained in the DPPS.

e. Data standards producers will—

(1) Use FIPS 184 (IDEF1X) and the approved database standard (that is, Army National Standards Institute (ANSI) Standard SQL 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 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.

4–12. 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 (XSL/T) 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 information systems 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, 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 following order of precedence (highest to lowest) for selection:

(a) Joint COI IESS-based tags.

(b) Army COI IESS-based tags.

(c) Federal department COI IESS-based tags.

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

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

Chapter 5
Information Assurance

5–1. Mission

Per DODD 8500.1, IA provides the means to ensure the confidentiality, integrity, and availability of information processed by the Army's information-based systems. It provides a measure of confidence that the security features,

practices, procedures, and architectures of an information system accurately mediates and enforces the security policy. IA recognizes that interconnected systems create shared risks and vulnerabilities where an intruder only has 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 authentication and integrity of the data. Authentication and integrity are as important as confidentiality of information. IA includes security of information and related systems, C2, physical, software, hardware, procedural, personnel, network, communications security (COMSEC), operational, intelligence, and Web risk assessment.

a. Information Assurance Vulnerability Alert (IAVA) is a process within the C2 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 information and information-based systems essential to the minimum operations of the Army. They include, but are not limited to, telecommunications, weapons systems, transportation, personnel, budget, BASOPS, and force protection. (See also AR 25–2 for more policy on information assurance.)

b. IA components will be designed to protect information 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.

c. IA seeks to maintain 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 nonrepudiation of the infrastructures and the information contained within. Per DODD 8500.1, IA-enabling technologies such as Public Key Infrastructure (PKI) and biometrics will be used to protect information.

5–2. Management structure for information assurance

An appropriate management structure will be established at all levels to implement the IA program and the IAVA process for the protection of critical information infrastructures. In addition, commanders will appoint, as appropriate, personnel who are responsible for enforcing the IAVA process.

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

b. The scope of the MACOM IA program includes information systems that are unique to the MACOM. The exception is the MACOM's responsibility to appoint tenant information assurance managers (IAMs) and IA security officers (IASOs) that support the installation IAMs and RCIOs.

c. The IAPM will ensure the appointment of the appropriate number of IA personnel (alternate IAPM, IA network manager, IA network officer (IANO), IAM and tenant IAM, and IASO) necessary to execute the IA duties and responsibilities.

d. The RCIO IAPM will ensure the installation IAM and IANO are appointed for each installation or cluster of small posts/camps/stations within the region.

e. MACOMs, PEOs, direct reporting PMs, and RCIOs are responsible for disseminating IAVAs, IA bulletins, and IA technical tips and for reporting compliance in accordance with HQDA policy.

f. System administrators will operate network(s) and all aspects of network security under their purview.

5–3. Information system certification/accreditation

a. All information systems and networks will be subjected to an established certification and accreditation process that verifies the required levels of information assurance are achieved and sustained.

b. Only Army-approved IA products will be used. information systems and networks will be certified and accredited per DODI 5200.40 or Director of Central Intelligence Directive (DCID) 6/3. The Defense Information Technology Security Certification and Accreditation Process (DITSCAP) considers the system mission, environment, and architecture while assessing the impact of the operation (or loss of operation) of that system on the Army's information infrastructure.

c. NETCOM has overall responsibility for ensuring that all information systems are properly certified and accredited in accordance with the DITSCAP. MACOMs, PEOs, and direct reporting PMs will be responsible for certification and accreditation of MACOM, PEO, and direct reporting PM unique systems that they own and operate. Tenant IAMs are responsible for ensuring that tenant information systems are certified and accredited for that tenant organization. The DITSCAP will be applied to all systems requiring certification and accreditation throughout their life cycle. (See also AR 25–2 and DODI 5200.40.) Where applicable, all IA-related Government-off-the-shelf (GOTS) and COTS hardware, firmware, and software components and IT products used in the Army Information Infrastructure must be evaluated

and acquired in accordance with the National Security Telecommunications Information Systems Security Policy (NSTISSP) No. 11, and other applicable national and DOD policy and guidance identified in this chapter or in AR 25–2.

d. Special Access Program (SAP) system accreditation authorities will be retained at the HQDA level. The CIO/G–6 will designate a colonel or GS–15 as the SAP accreditation authority for all systems that process SAP information. (See also AR 380–381.)

5–4. Physical security

Commanders who operate and maintain any information system will provide adequate levels of physical security per AR 25–2.

5–5. Software security

a. Controls will be implemented to protect system software from compromise, subversion, or tampering. The installation IAM, Configuration Management Board, Configuration Control Board, and designated approval authority (DAA) must approve all software used on Army networks prior to installation and operation.

b. When database management systems (DBMS) containing classified defense 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 security services will have appropriate evaluation/certification prior to use or will be selected from the National Security Agency (NSA) NSA/National Information Assurance Partnership (NIAP) product validation list. Other evaluated products may be used based on a valid justification and approval from the DAA. Agencies responsible for distribution of software security products will those products comply with DITSCAP (DODI 5200.40) certification and accreditation and the product IA protection profiles have been validated by the National Institute of Standards and Technology/NSA NIAP program. (For more information, refer to AR 25–2 and NSTISSP No 11.)

d. Developers of Army systems that include software will 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.

5–6. 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 compensation in other elements of the security and IAVA 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/or physical environment of the system.

5–7. Procedural security

All MACOM, mission, and garrison commanders (or equivalent), and IMA region directors/RCIOs will identify key information assurance 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 appropriate IASO, who will notify the appropriate IAM. The operator, the IAM, and the DOIM will notify the region IAPM or RCIO, the Regional Computer Response Team, and the Army Computer Response Team (ACERT)/Coordination Center.

b. During an information emergency, intrusion, or exploitation, IA personnel below the MACOM 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 ACERT alerts and advisories are reviewed and that corrective measures are taken.

c. Any information system that processes data in an SCI environment will ensure its equipment used for processing, handling, and storing is in compliance with DCID 6/3 and AR 25–2.

d. User identification and password 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 password generation, issuance, and control process.

5–8. Personnel security

All personnel will receive the level of training necessary and appropriate licensing or certification to perform their designated IA responsibilities.

a. All individuals who are appointed as IA program personnel and systems administrators must complete training and certification, as necessary, equal to the duties assigned to them.

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

c. All positions where the incumbent personnel will require access to an IT system will be designated as IT I, II, or III. Personnel assigned to positions with these designations must meet the security investigation requirements of DOD 5200.2–R. (See AR 25–2, para 4–14, for further information.)

5–9. Communications security

Commanders will take the appropriate measures to secure all communications devices to the level of security classification of the information to be transmitted over such communications equipment.

5–10. 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.

5–11. Army Web Risk Assessment Cell

The Army Web Risk Assessment Cell (AWRAC) is responsible for reviewing the content of Army's publicly accessible Web sites. 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. The AWRAC will—

a. Conduct random sampling of Web sites to identify security concerns or review Web site concerns provided by the Joint Web Risk Assessment Cell (JWRAC) or Army leadership.

b. Ensure inappropriate security and personal information is removed from publicly accessible Web sites.

c. Ensure that Army sites are compliant with other Federal, DOD, and Army Web site administration policies (for example, Government Information Locator Service (GILS) registration). (See also para 6–4*n*.)

d. Notify the Web site owner with operational responsibility and the IAPMs of the respective command/activity of the violations and suspense dates for reporting corrective action.

e. As required, report deficiencies and corrections to the Army CIO/G–6 and JWRAC.

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

6–1. IT support principles

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

a. Information transmission economy and systems discipline. MACOM commanders and agency directors will implement procedures to promote optimum, responsive, cost-effective use of all types of DOD information systems and services and ensure the application of sound management practices in accomplishing information systems services economy and discipline. (See also DODD 4640.13 and DODD 8000.1.) Commanders and activity heads will establish procedures to ensure—

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

(2) Information managers (or designated telephone control officers) periodically 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 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 2 years. Review and revalidation must include voice, video, data, and bandwidth utilization of NIPR and SIPR.

b. HQDA continuity of operations plan (COOP). HQDA must ensure the uninterrupted execution of its essential

missions and functions under all conditions. The HQDA COOP (AR 500–3) includes 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 agencies, MACOMs, and other organizations subordinate to HQDA are required to maintain a COOP consistent with AR 500–3. Each C4/IT system deemed critical to essential HQDA missions or functions must be supported by its own COOP that ensures its continuous operation under all conditions. All COOPs must be tested at least biannually. (See also para 8–5*h* on the preservation of vital records.)

c. Electronic business/electronic government (EB/EG). Army activities will use EB/EG technologies to the maximum extent practicable to promote the goal of a paper-free (or near paper-free) business environment. EB/EG solutions must conform to DOD and Army standards, architectures, and interoperability requirements (see DODD 8190.2 for additional guidance on electronic business). Records created using EB/EG and maintained on EB/EG technologies will be preserved per retention schedules in AR 25–400–2.

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 anyone using 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 *e*, below.) 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 for caution when transmitting other sensitive information. (See para 6–4*q* for additional information on communications monitoring.)

(3) Commanders will recover toll charges, as practical, for unofficial/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.

(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. 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 nonpeak, nonduty 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 para 6–4*w* for guidance on cellular telephones.)

(6) Guidance for telephone calls while at a temporary duty 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 and 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 and frequency, 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 personal 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.

(e) 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. Other prohibitions in the use of Army communications systems include the following:

(1) Use of communications systems 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; 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 public laws. This may include, but is not limited to, violation of intellectual property, gambling, terrorist 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) Both Federal law and Army policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to electronic 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) Army communications systems will not be used for purposes 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 listservers 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 smaller populations.

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

g. Web blocking. Per AR 25–2, 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 *f*, above.

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

i. Use of employee-owned IT. Use of employee-owned assets IT hardware or software to process unclassified Army-related work off the Government work site must comply with the provisions of AR 25–2. Use of employee-owned IT hardware or software that connects to the network at the work site is prohibited.

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 agreements. DOIM will provide or obtain IT support services to other Army, DOD, or non-DOD activities on a reimbursable or nonreimbursable basis as determined by support agreements.

(1) Army activities will coordinate with the supporting DOIM to obtain requirements beyond the approved baseline IT services. Support agreements will be established, as appropriate, for obtaining specified IT support. Supported organizations will assist the DOIM in assessing quality of support by providing feedback as requested in customer service surveys.

(2) The DOIM is the primary source for obtaining IT contract support. Consideration may also be given to using contract capabilities available from other DOD and Federal activities. Use of other such capabilities will be coordinated with the supporting DOIM prior to ordering or entering into service contracts. All IT support services will be obtained by the DOIM using existing Army enterprise contracts.

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 baseline IT services. An inter-Service support agreement (ISA) with 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 regional CIO(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 United States Government; the supplying activity is able to provide the support; the support cannot be provided as conveniently or cheaply by a 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 on a nonreimbursable basis is authorized to provide communications and data automation support to—

(1) MWR activities as outlined in AR 215–1 (app D) and temporary duty (TDY), permanent change of station (PCS), and military treatment facility (MTF) lodging programs as outlined in DODI 1015.12 (enclosure 3).

(2) All other NAFI(s) as outlined in DODD 1015.14 (Army and Air Force Exchange Service (AAFES), Civilian Welfare and Restaurant Funds, and so on). NAFI will comply with AR 70–1 and this regulation for acquisition and management of MWR systems that are obtained with appropriated funds. AR 215–4 governs IT supplies and services acquired with nonappropriated funds (NAF). NAFI requiring DOIM-provided IT support will comply with this regulation and those policies promulgated by the installation DOIM.

o. IT support for telework.

(1) Telework is defined as an arrangement in which a civilian employee member of the Armed Forces performs assigned official duties at an alternative worksite on either a regular and recurring, or on an ad hoc basis (not including while on official travel). This 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 and on the DOD telework Web site at http://www.cpms.osd.mil/fas/telework/dod_telework_policy.htm

(2) Use of Government IT resources (such as computers, facsimile machines, modems, and so on) for telework is authorized under certain conditions, which can vary from one installation or activity to another. Government-furnished computer equipment, software, and communications, with appropriate security measures, are required for any regular and recurring telework arrangement. A telework agreement that outlines the terms and conditions (including IT support) of the arrangement is required before the employee commences regular/recurring telework. Where approved, the use of employee-owned computers and equipment for telework on an ad hoc basis is authorized. However, remote-access software must not be loaded onto employee-owned computers for official purposes. All telework agreements will address mandatory information assurance 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 (DSL), cable modems, and analog dial-up lines) within an employee's residence as an alternative worksite may be determined by the local commander. (Telework resources are not intended for individuals who occasionally check e-mail from their residences.)

p. Information access for handicapped Army employees. Public Laws 99–506, 100–542, and 105–220 require computer and telecommunications systems to be accessible to Government employees with disabilities, their supervisors, and others that need access to the employees. Information managers will make all reasonable efforts to accommodate individuals with handicaps, consistent with these laws and AR 600–7. The Computer/Electronic Accommodations Program, 5111 Leesburg Pike, Suite 810, Falls Church, VA 22041–3206, provides assistive technology accommodations and services to persons with disabilities at the DOD at no cost to individual activities. The Computer/Electronic Accommodations Program 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 (TDD), telephone amplifiers, listening devices, closed captioned decoders, and visual signaling devices for those with hearing problems. (See http://www.tricare.osd.mil/cap/ for more information.)

q. Electronic and information technology access for employees and members of the public with disabilities. P.L. 105–220 (Section 508) requires the government to provide disabled employees and members of the public with access to information. Access for disabled persons must be comparable to the access available to nondisabled persons. The law applies to all Army organizations when they develop, procure, maintain, or use electronic and information technology. Electronic and information technology includes equipment or interconnected systems or subsystems of equipment that are used to create, convert, or duplicate data or information. Section 508 applies to computers and networks, hardware, software, Web pages, and e-mail, as well as equipment used for transmitting, receiving, using, or storing information such as fax machines, copiers and telephones. 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.

r. Installation-level technical support and service.

(1) Every DOIM will establish an installation-level help desk. 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 JTA–A-compliant information system. 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 Army Small Computer Program Office (ASCPO) is the primary office for establishing commercial IT contracts. ASCPO is endorsed by the ABIC to make purchasing more efficient through volume buying, thereby simplifying and centralizing IT lifecycle management throughout the Army enterprise.

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

(1) 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) MACOMs, installations, and activities will obtain all IT services through the installation DOIM. (See DODI 4000.19 for procedures on service parameters and estimating annual fees.)

(3) 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.

c. Other centralized or installation-level processing services. OMB and DOD consider any automated information processing operation to be a data center. For purposes of consolidation or outsourcing, a service is a data center if it has a standing staff of five or more full-time equivalent employees (computer operators, telecommunications specialists, administrative support staff) that perform one or more of the following functions: processes automated application systems, affords time-sharing services to agency personnel, provides office automation and records management services through a centralized processor, and/or provides network management support for agency-wide area networks. A data center can consist of small, medium, or large-scale processors that require controlled environmental conditions. Facilities (for example, functional offices) that merely support local file servers or desktop computers are not categorized as agency data centers.

(1) In CONUS, Army facilities meeting the criteria of a data center will assess information processing alternatives by conducting cost–benefit analysis studies per AR 5–20 to determine whether services should be consolidated, outsourced to the private sector or another federal agency (for example, Defense Enterprise Computing Centers), or retained within the agency. Significant change in mission or funds warrants conducting cost–benefit analysis studies. Any agency planning to consolidate its in-house operations or outsource its information processing services will provide the results of its analysis and planned milestones per AR 5–20, with advance coordination copy to CIO/G–6 ATTN: SAIS–IOM. Any agency requiring an exception to this policy will coordinate with CIO/G–6 through its respective chain of command.

(2) OCONUS data centers will determine and implement their own JTA–A compliant architectures for any centralized processing services if DOD-provided services are not available or economical. TRADOC will determine the organization of processing services in the table of organization and equipment (TOE) force.

(3) All data centers touching an Army network must complete Networthiness Certification.

d. Consolidation of servers. DOIMs on each post will consolidate servers for Army tenants residing on the post within the installation data center or designated server farm locations. Tenants associated with other Army networks that encompass multiple posts may remain within their networks until such time as Army migration efforts are complete. 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. 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. After baselining, DOIMs must report status of server consolidations for all Army tenants to the Army CIO/G–6 for input into the SRS. Army activities not residing on an installation or under the direct support of a DOIM will baseline and report status of their consolidation through the appropriate HQDA functional proponent to the Army CIO/G–6. Data entry on consolidation reporting (server plan registration) is through the AKO Collaboration Web site.

e. Office automation.

(1) *Office equipment.* Office equipment includes desktop personal computers, laptop computers, servers, notebook computers, hand-held computers, and personal digital assistants. Peripheral devices include any device designed for use with personal computers (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 PC operations (for example, operating systems). PC 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 Regulation (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 under the DOD Enterprise Software Initiative (ESI). Enterprise software agreements (ESA) 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 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 ASCPO under the Program Executive Office Enterprise Information Systems is the Army's exclusive source for all software through the ELAs.

(c) The DOIMs will coordinate their acquisition plans with the ASCPO concerning specific products prior to entering into an agreement with any COTS vendors. If the existing ESA does not contain the desired terms and conditions or prices, the DOIM must notify the ESA manager so that the manager may improve the existing ESA prior to the DOIM's executing any other agreement. The ASCPO is responsible for authorizing new ESA agreements and for granting waivers for Army activities to acquire an ESI-managed COTS product from any other source. The ASCPO Web site is http://pmscp.monmouth.army.mil. See also the DOD ESI homepage, which lists all ESI-managed software: http://www.don-imit.navy.mil/esi/.

(4) *Software control.* Users will not install new software packages, software upgrades, free software, freeware, shareware, and so on, without the authorization of their IAM, Configuration Management Board, Configuration Control Board, and 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 para 5–5 for COTS software installation approvals.)

(5) *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.

(6) *Personal digital assistants (PDAs).* The current range of PDAs includes devices and software, which can be as simple as electronic "Rolodex" files or as complex as a palmtop computer with a full keyboard and the capability to upload/download from workstations. PDAs with network or wireless interface capability will be managed and accounted for as computers.

f. Purchase of energy-efficient computer equipment. All purchases of microcomputers, including personal computers, monitors, and printers, will meet the Environmental Protection Agency Energy Star 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.

(1) Army activities will maximize the use of selected software applications across all forces. Selected application standards will be recorded in the Army systems architecture. (See also para 6–2*e*, above, for COTS purchases.)

(2) CIO/G–6 will identify to Army activities the common/standard Army software applications/modules that are Army or OSD-approved. The CIO/G–6 will also identify selected joint standard systems, Service-specific responsibilities for their development and sustainment, and, for Army-led systems, assign specific responsibilities to Army IT materiel developers.

(3) All organizations that represent the users (for example, combat developers, HQDA staff elements) will consider the emerging software applications' potential for Army-wide use during the requirements definition and life-cycle management phases for IT and will recommend the scope of standardized use to the requirement approval authority. Requirement approval authorities will seek and exploit opportunities for standardizing the use of software applications across all forces and recommend standardization opportunities to the CIO/G–6. The CIO/G–6 will coordinate with the Army Staff (ARSTAF) and MACOMs before designating BASOPS software applications for standardized use.

(4) 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 by the Army Systems Architect. Opportunities to eliminate duplication of development and acquisition efforts will be a factor in decisions regarding software applications. (See para 3–9 on the goal to reduce and webify applications.)

(5) 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.

(6) Software applications will be reviewed at system milestone reviews. The review will be based on a business case that considers information exchange requirements and cost effectiveness as viewed from an Army-wide, not individual system, perspective. At a minimum, software applications will be designed to—

(a) Permit users to access shared data in a consistent standards-based approach, independent of specific vendors' IT.

(b) Be independent of vendor-specific data management and access schemes.

(c) Provide users with transparent access to nonlocal data.

(d) Permit use of data and information as Army-wide assets.

(7) Use standard data formats as approved for use by the DOD Net-Centric Data Management Program described in chapter 4 of this regulation.

(8) Software components will be engineered for reuse in all applicable systems. Determination for software reuse will be based on cost–benefit analysis from a total Army perspective. Software reuse and plans will be assessed at program milestone reviews per AR 70–1.

(9) AR 700–142 and Networthiness Certification, per paragraph 6–3*g*, will apply when fielding software applications to multiple MACOMs for standardized use in TDA organizations. To implement total package fielding for software applications, IT materiel developers and gaining organizations will—

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

(b) IT materiel developers and gaining MACOMs/activities will 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 MACOMs' senior IM officials. The MFP will be finalized prior to scheduling or executing any fielding actions within a MACOM to permit coordination with gaining installations. Gaining MACOMs will staff each iteration of the MFP with their gaining installations and must include the supporting DOIMs in the coordination. MACOMs will ensure each gaining installation is provided with the final MFP 6 months prior to the receipt of the new system. NETCOM/9th ASC (ESTA) ensures systems being fielded comply with the Networthiness process.

(c) MFPs will be developed per DA Pam 700–142, appendix F.

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

(11) IT materiel developers with responsibility for the development of a multi-MACOM software application will initiate its postproduction software support (PPSS). IT materiel developers 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 materiel developer will include planning for PPSS and its estimated cost in milestone decision reviews or in-process reviews, as applicable.

(12) 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 MACOMs will have one configuration manager, assigned by AMC. MACOMs and other users will not independently make changes to a software configuration item without approval from the software application's configuration control board. Source code for these applications will not be provided to users unless it is authorized by the assigned software support activity and the functional proponent. 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 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 procure only the products or services that comply with the JTA–A and established DOD collaboration interoperability standards and that are identified on the approved products list maintained by DISA's Collaboration Management Office (CMO) and the Joint Interoperability Test Command (JITC). (The products list is available at http://jitc.fhu.disa.mil/washops/jtcd/dcts/index.html.) For the purpose of this regulation, collaboration capabilities include, but are not limited to: voice and video conferencing; text, document, and application sharing; awareness and instant messaging; and whiteboarding.

(2) CECOM is the Army focal point for technical matters and the Army interface with the DISA CMO to address interoperability within Army systems. The Army CIO/G–6 will not support the development of new tools or the sustainment of existing collaborative tools that do not 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 the Enterprise Integration Directorate (SAIS–EI), Office of the CIO/G–6, 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 ASCPO whenever possible. Available ESA can be accessed at the ASCPO Web site: http://pmscp.monmouth.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), table of distribution and allowances (TDA), or other appropriate authorization documentation, may be requisitioned

within authorized allowances without submission of any IT specific planning or acquisition documentation to HQDA. MACOMs will determine the documentation requirements and coordination procedures for justifying purchase requests that are within their approval authority. MACOMs may delegate approval authority to subordinate commands, separate reporting activities, and installations. DOIMs will determine the documentation requirements and coordination procedures for justifying 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.

k. Redistribution and disposal of IT assets.

(1) The screening, redistribution, and disposal of IT equipment is 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 (DLA) is the executive agent 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, and DOD 4160.21–M.

(3) DRMS supports EO 12999 through the DOD Computers for Learning 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. DOIMs and/or property book officers will ensure that hard drives are disposed of using the methods and procedures prescribed in the June 4, 2001, DOD memorandum, "Disposition of Unclassified DOD Computer Hard Drives," (http://www.drms.dla.mil/turn-in/asdhddispmemo060401.pdf) or subsequent directive.

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, the Army may copy proprietary software only for limited purposes (such as an archival copy) under the provisions of 17 USC 117.(Also see paragraph 7–8.) Army's private-sector service providers are also subject to software copyright laws and may be required to provide written assurances of compliance.

m. Life-cycle depreciation. In planning life-cycle requirements and calculating economic benefits of automation IT, 3 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 information assurance 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 connected to the network must achieve Networthiness Certification (see para 6–3*g*).

6–3. Network operations (NETOPS)

NETOPS is defined as the operation and management of the AEI. This includes the organizations, procedures, and technologies required to monitor, manage, coordinate, and control the AEI as the Army portion of the GIG. NETCOM is responsible for the operation and management of enterprise-level IT assets throughout the Army. NETCOM provides the technical guidance to the DOIM for all C4/IT services and applications. NETCOM will also obtain CIO/G–6 approval for and execute the Army NETOPS concept of operations.

a. Baseline service levels. Common services and applications are provided in accordance with baseline service levels approved by the CIO/G–6 and funded by ACSIM.

b. Network management. Network management includes systems and application management and consists of fault configuration, accounting, performance, and security management. Network management incorporates all support functions associated with providing customer access to the installation classified and unclassified data, voice, and video network(s) and connection to remote sites, DOD enterprise networks, and the Internet. The DOIM is responsible for operations and management of the installation's infostructure.

c. Inter-installation and regional networks. NETCOM will work closely with DISA in the management of networks external to the installation that enable installations to communicate. The DOIMs will coordinate directly with DISA or through the RCIOs and NETCOM regarding DISA's hardware and software components that affect their supported organizations.

d. Installation network management. Installation DOIM network management includes planning for appropriate network hardware and software technology upgrades and replacements to ensure customer demands are met. Baseline services will be implemented under an SLA. ISAs will be implemented for non-Army tenants to define network management roles, responsibilities, and authorities.

e. Local area network (LAN) administration. The DOIM will perform some or all of the following functions: configuration management, fault isolation, minor engineering, information protection operations, performance management, accounting management, network planning, training, and customer support of common user network resources. Network administrative tasks may include: file server management; metering and virus-scanning software management; server backup; contingency planning and disaster recovery for managed LANs; and providing technical assistance to functional systems administrators and staff who provide support from their servers to their end-user workstations.

f. NETCOM responsibilities. NETCOM responsibilities for Army network operations are below:

(1) Selects, integrates, manages, and deploys standardized NETOPS management capabilities to all Army network operations and security centers.

(2) Develops, implements, and enforces Enterprise Systems Management (ESM) processes and activities.

(3) Provides operational guidance and functional staff oversight for ESM operations to NETCOM/9th ASC units and regional organizations.

(4) Provides technical and operational oversight of the Army's infostructure.

(5) Manages the Common Access Card (CAC)/PKI for the Army enterprise.

(6) Provides Army with near real-time network common operating picture of critical networks and systems.

(7) Identifies requirements and definitions for asset and resource management to include property accountability of logical property used in the operation and maintenance of the infostructure.

(8) Performs C4/IT service management in support of the Army. These duties include—

(a) Develop C4/IT service requirements.

(b) Manage baseline services.

(c) Provide information assurance support to—

1. Protection of the NETOPS domains, configuration management, and enabling technologies.

2. IT security certification and accreditation.

3. Technical insertion relating to the AEI.

4. Certification of Networthiness and Certificate to Operate processes.

5. Architecture Systems and Design Reviews.

6. Vendor selection.

7. Enterprise recapitalization.

(d) Provide security support to—

1. Review C4 IM service contracts impacting enterprise-level operations and management.

2. Onsite security inspections and staff assistance visits as required.

3. Development of classification guides for enterprise-wide application.

g. Networthiness Certification. The Networthiness Certification Program manages the specific risks associated with the fielding of information systems and supporting efforts, requires formal certification throughout the life cycle of all information systems that use the infostructure, and sustains the health of the AEI. Networthiness Certification is concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected. Networthiness Certification applies to all organizations fielding, using, or managing information systems on the AEI.

(1) The CIO/G–6 is responsible for—

(a) Policy and oversight of the Army Networthiness Certification Program.

(b) Monitoring, reviewing, and assessing the progressions of related acquisition processes.

(2) NETCOM/9th ASC serves as the certification authority to validate from a location-centric view that the resulting infostructure can support the information system, that there are no negative impacts to other systems from the information system, that the information system does not introduce any security vulnerabilities, and that the AIS can be managed and maintained. The validation ensures that—

(a) IT systems are documented and validated for meeting supportability, security, compatibility, integration, manageability, and interoperability requirements.

(b) System infrastructure and interfaces are identified, coordinated, approved, and implemented.

(c) Appropriate architecture and systems design are incorporated into the overall networthiness process. New systems or their capabilities will not adversely impact the AEI.

(3) The functional representative must submit a request for Networthiness through the appropriate chain of command to NETCOM. Developers must obtain Networthiness Certification for all information systems and supporting elements. (See AKO/CIO/G–6 Collaboration Web site for current information and procedures.)

6–4. Telecommunications systems and services

Telecommunications provides 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, fascimile (fax) machines, video teleconferencing, cable television, and others. These services provide the warfighter and sustaining base the telecommunications technology needed to achieve their operational objectives. 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) *Defense Switched Network (DSN).* 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 DSN on- and off-net calling.

(2) *Federal Telecommunications System (FTS).* FTS will be used for non-C2 administrative voice services. FTS services will be used for commercial access unless other commercial voice services can be accessed without the expenditure of appropriated funds to increase the number or type of existing commercial circuits. NETCOM is the Army's responsible official for FTS service contracts. All requirements for FTS will be submitted to NETCOM for service provisioning.

(3) *Telecommunications services in the National Capital Region.* Washington Interagency Telecommunications Services provides centralized administrative telecommunications service for DOD in the 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 policy.

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 DFAS–IN 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 official telephone service are—

(1) *Class A.* Class A telephone lines accessing central offices, toll trunks (local, FTS, international), DSN, and Government telephone systems/services (that is, voice mail). Class A official telephone service will normally be subdivided as follows:

(a) Class A1. Provides access to all on-post telephone numbers and direct dial access to international, FTS, DSN (routine and, if available, precedent,) and local off-post trunks only. Access to precedent DSN trunks must be fully justified and command approved.

(b) Class A2. Provides access to all on-post telephone numbers and direct dial access to FTS, routine DSN, and local off-post trunks only.

(c) Class A3. Provides access to all on-post telephone numbers and direct dial access to routine DSN and local off-post trunks only.

(d) Class A4. Provides access to all on-post telephone numbers and direct dial access to local off-post trunks only.

(2) *Class C.* Class C official telephone service is normally not subdivided. Class C telephone lines are for transacting official Government business on Army installations. This service does not provide direct-dial access to off-base trunk lines (toll trunks, FTS or commercial, international or DSN). These lines can receive calls from off base and have dialing access to the switchboard operator.

(3) *Class D.* Class D official lines for official Government business. DOIMs will restrict the use of these lines to special services such as fire, security, and other special services/alarms. This service will normally be subdivided as follows:

(a) Class D1. Fire alarm service.

(b) Class D2. Security alarms and camera circuits.

(c) Class D3. Other special services/alarms (data circuits, energy management circuits, special circuits, and so on).

(4) *Class B (unofficial telephone service).* The subscriber pays all charges associated with this service according to 10 USC 2686, DOD criteria, and this regulation. Class B service is provided only when an installation cannot reasonably obtain commercial service for its unofficial needs. Class B subscribers can access commercial telephone central offices and toll trunks (except where restricted). Class B service does not have direct in-dial or out-dial access to DSN and other Government private line services. Class B service has the following categories:

(a) Class B1. Telephone lines in Government-owned and Government-leased quarters for family or personal use including telephone lines in visiting officers' quarters, family housing, and hospital suites.

(b) Class B2. Telephone lines at a military location for activities such as public schools, American Red Cross (ARC), motion picture services, exchanges, credit unions, Boy Scouts, Girl Scouts, nurseries, thrift shops, commercial contractors, concessionaires, and other businesses operating on behalf of DOD if on or near a DOD installation.

c. Requesting telephone and telephone-related service.

(1) DOIMs will submit all BASECOM service requests to NETCOM/9th ASC. NETCOM/9th ASC will obtain all BASECOM services—such as local central office trunks, commercial business lines, Foreign Exchange (FX) trunks/lines, cellular telephones, pagers, and wireless devices—via consolidated local service contracts that are competed among interested service providers. NETCOM/9th ASC will satisfy requirements through contract/awards. If the existing consolidated contract cannot be used to satisfy the requirement, NETCOM/9th ASC will competitively award a

new contract to satisfy the requirement. NETCOM/9th ASC will determine whether an existing consolidated contract will be modified or a new contract will be required to fulfill service requirements.

(2) 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 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 ASC contracting officer.

(3) DOIMs will obtain operation and maintenance (O&M) for installation telephone plants through NETCOM/9th ASC.

d. Long distance calling.

(1) 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) The NETCOM subordinate command/regional RCIO 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 switches will be programmed for least-cost routing of official telephone calls to ensure calls are placed over the most economic route.

(4) DSN (see para 6–4*a*(1), above).

(5) FTS (see para 6–4*a*(2), above).

(6) The installation commander will determine the local policy for handling incoming official collect calls.

e. Verification of bills and payment for telephone services.

(1) *Verifying bills.* Federal statutes require the SECARMY or designee to certify long-distance telephone calls as official before paying for them. The purpose of verification is to collect payment from those making unofficial calls. Per the Decision of the U.S. Comptroller General B–217996, 65 Comptroller General 19 (October 21, 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 were 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).

(2) *FTS verification.* The DOIM will use a judgment sampling to verify bills for FTS. The DOIM will credit the amount collected to the account that originally paid the bill. The GSA is the Government's contracting agency for FTS.

(3) *Billing and payment.* The telephone control officer 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.

(4) *Accountability procedures.* DOIMs will establish and maintain accountability procedures for telephone calling cards.

f. Use of calling cards (includes prepaid and postpaid cards) and Government Emergency Telecommunication Services (GETS) cards.

(1) Installation commanders will approve the acquisition and use of telephone calling cards.

(2) 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.

(3) Individuals who misuse telephone calling cards are subject to disciplinary action.

g. Official telecommunications services in personal quarters. Official voice (telephone), data (SIPRNET/NIPRNET), and video service is authorized for key personnel whose position requires immediate response and/or has 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) Official service will not have direct dial access to the local commercial exchange system.

(2) Direct dial access to the DSN and Defense Telephone System (DTS) 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, FTS and commercial telephone exchange service will be through the local installation switchboard operator) or a local command operations center.

(3) Service will be restricted to the conduct of official Government business for C2 or tactical purposes.

(4) 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) 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.

(6) Access to classified network will be by exception only and approved on a case-by-case basis.

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) Secure phones are 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 Narrow-band 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) 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) 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 SCIFs).

(4) When talking at a classified/sensitive level, personnel must be aware of the environmental conditions, including the proximity of uncleared individuals. The cognizant security authority should implement a common-sense approach to acoustic security concerns. Introduction of the secured wireless/wired devices into an area should not change those requirements normally implemented in areas conducting classified or sensitive unclassified operations.

i. Automated service attendant. RCIOs may 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 RCIO.

j. Telephone service charges. Charges for installation telephone services will be used to determine charges for telephones services provided from Government-owned or commercially leased telephone systems.

k. Authorized telecommunications devices. Telecommunications services authorized for specific installation activities are identified in appendix B.

l. Pay per use and unofficial telephones. Pay per use telephone service (coinless and coinbox) and other unofficial telecommunications are MWR functions. NAF procedures will be used. Contractor fee payments per these contracts will be paid to the NAFI. The AAFES is the sole activity authorized to contract for pay telephone and other unofficial telecommunications requirements (for example, barracks telephone, cellular telephone). Any requirements for such unofficial telecommunications services will be referred through command channels to Headquarters (HQ), AAFES, for appropriate contracting action. Contractor fee payments to AAFES are shared through the Army MWR Fund with local installation MWR funds. Other unofficial telecommunications initiatives are separately pursued by MWR and AAFES in accordance with their respective areas of responsibility.

m. E-mail. Broadly defined, e-mail includes COTS e-mail systems and Web mail.

(1) Army activities will use electronic means for coordination on a worldwide scale, as required, to efficiently execute mission requirements.

(2) Only Government-provided e-mail services (as designated by the local DOIM) are permitted. Commercial e-mail services are prohibited for Army business communications. Automatically forwarding from an official Government account to an unofficial (commercial service) is prohibited. The Chief Technology Officer and DOIMs will ensure that the "auto-forward" default settings on AKO Web mail and e-mail are modified to preclude 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.

(3) DOD PKI will be used to digitally sign messages that are created and sent from any DA e-mail system other than the Defense Message System (DMS).

(a) The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates.

(b) A DOD PKI encryption certificate may be used to encrypt sensitive information for transmission via e-mail. To minimize use of bandwidth, encryption should only be used to send—

1. Information that is required to be protected by the Privacy Act (5 USC 552a).

2. Information considered as "For Official Use Only" (FOUO).

3. Information protected under HIPAA. (See also para 2–22*c* and References.)

4. Sensitive information (as defined in the glossary).

(4) Soldiers, civilians, and contractors who are authorized e-mail accounts are required to also have AKO Web mail.

To register, log on to https://www.us.army.mil. Follow the instructions under "I'm A New User." SIPRNET users must also have AKO–S accounts. Army e-mail users will use their AKO "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, and so on).

(5) Only AKO and other Government-provided COTS Web mail services (as designated by the local DOIM) are permitted. All other commercial Web mail services are prohibited for Army business communications.

(6) 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.

(7) When using AKO Web mail, the following bandwidth restrictions are in effect:

(a) Only mission-essential attachments will be transmitted. Users must limit individual Web mail message transmissions (including attachments) to 20 megabytes. Users are encouraged to use file compression when sending large file attachments to multiple addressees via e-mail, especially when file attachments exceed 5 megabytes.

(b) When internally staffing documents within an organization, place the documents on shared drives or on organizational intranets instead of attaching the documents to Web mail.

(c) When sharing documents external to an organization, place documents that exceed 20 megabytes, in the aggregate, on a Web server and provide the uniform resource locator (URL) where the documents are located. DOIMs/IMOs will inform users that posting documents to a Web site is preferable to distributing documents by e-mail to a large number of people. Activities will use AKO and AKO–S portals as the primary tools for collaboration. Web site maintainers will install access-control mechanisms, as required. (See para 6–4*n*, below, for prohibitions on posting specific information on public Web sites.)

(8) 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. RCIOs/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.

(9) Army e-mail users will observe JTA–A standards in attaching files to e-mail notes for inter-installation/activity transmission. JTA–A selects specific file formats for the interchange of common document types such as text documents, presentation graphics, spreadsheets, and databases.

(10) Army policies for records management apply to e-mail traffic. Designated records managers, records coordinators, and records custodians will monitor the application of records management procedures to e-mail records per chapter 8 of this regulation and AR 25–400–2.

(11) Refer to paragraph 6–5*f* for policy on the DMS.

n. Internet (World Wide Web (WWW)), intranets, and extranets. Official Army Web sites may exist on any of the above forms of "nets." The use of these net communications can support execution of Army missions through information sharing and save resources currently expended on traditional means of communication. Users are encouraged to make it their preferred and routine choice to access, develop, and exchange information. Army Web sites must be in compliance with the DOD Web site administration policy located at http://www.defenselink.mil/webmasters/ or contained within subsequent DOD directives. The following Army policies also apply:

(1) Access to all forms of nets is authorized according to the controls applied by the Web site owners.

(2) AKO (www.us.army.mil) is the enterprise portal for Army unclassified intranets and the NIPRNET. AKO is the single Army portal for authenticating users to gain access to Army systems and Web servers. Existing Army portals or Web servers with authentication services will migrate authentication support to AKO unless waived by CIO/G–6. The AKO–S is the enterprise portal for classified intranets and the SIPRNET. The use of AKO 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 resources, features, and tools in order to reduce the need for installation and MACOM investment in the same types of IT resources.

(a) Army Web-enabled business applications are required to be linked to the AKO portal. Initial minimum standard to link applications to AKO is a URL link on the Army portal. The objective standard to link applications to AKO is to use the AKO directory services for authentication as well as a URL link on the Army portal.

(b) Proponents are required to establish the appropriate mechanisms to protect sensitive information from being accessed by unauthorized individuals. AKO is responsible for generating user IDs and accounts, performing authentication via secure Lightweight Directory Access Protocol (LDAP) directory services, publishing updates to the technical

mechanism used for directory services, and incorporating appropriate security measures. All applications, Web sites, and messaging services will use the AKO LDAP to authenticate users unless the CIO has granted a waiver.

(c) For organizational space on the AKO portal, organizations will assign a community page administrator for their primary community presence, and, where needed, assign additional administrators or other personnel to manage the content on the Knowledge Collaboration Center.

(3) NETCOM/9th ASC manages the ".army.mil" Web site assignment of subdomains requested by other Army organizations. NETCOM/9th ASC promulgates procedures for Army subdomain managers, to include assignment, formatting, and any centralized registration of addresses for servers, gateways, organizations, and individual users.

(4) Because the Internet is a public forum, Army organizations will ensure that the commander, the public affairs officer (PAO), and other appropriate designee(s) (for example, command counsel, force protection, intelligence, and so on) have properly cleared information posted to the WWW or to the AKO in areas accessible to all account types. Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the WWW. (See also para 5–10.) 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 minimum review will include all of the Web site management control checklist items at appendix C, paragraph C–4. 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. In addition, Army organizations using the WWW will not make the following types of information available on publicly accessible Web sites:

(a) Classified and restricted or limited distribution information.

(b) FOUO information.

(c) Unclassified information that requires special handling (for example, Encrypt For Transmission Only, Limited Distribution, and scientific and technical information protected under the Technology Transfer Laws).

(d) Sensitive information such as proprietary information, predecisional documents, and information that must be protected under legal conditions such as the Privacy Act.

(e) FOIA-exempt information. Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA are prohibited on the WWW. 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.

(f) Documents or information protected by a copyright.

(g) Draft publications (see also para 9–2.)

(5) The Army CIO/G–6 will provide policies, procedures, and format conventions for Web sites and will promulgate such guidance in this regulation and on the Army Web site at http://www.army.mil/webmasters/.

(6) Army organizations will assign a Web master/maintainer for each of their Web sites. Army organizations will provide their Web masters/maintainers sufficient resources and training. Web masters/maintainers will have technical control over updating the site's content and will ensure the site conforms to Defense- and Army-wide policies and conventions.

(7) Organizations maintaining publicly accessible Web sites must:

(a) Register the fully qualified domain name, (for example, http://www.us.army.mil or http://www.apd.army mil) for Army sites with the GILS at http://sites.defenselink.mil/ and update the contact information annually. (GILS is used to identify public information resources throughout the U.S. Federal Government.)

(b) Ensure that Web servers are IAVA compliant and are placed behind a reverse proxy server or implement an alternative security procedure.

(8) Organizations requiring private Web sites (for example, intranets, extranets) must register them with the NETCOM/9th ASC Theater Network Operations and Security Center (TNOSC) and assure that the secure sockets layer (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 ASC TNOSC.

(a) All Web applications will use AKO LDAP to authenticate clients, unless waived by NETCOM/9th ASC.

(b) All unclassified, private Army Web servers will be enabled to use DOD PKI certificates for server authentication and client/server authentication. The following type of Web server is exempt from this mandate: any unclassified Army Web server providing nonsensitive, 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) to limited access site(s) (and not the information resources).

(9) To ensure ease of access, public Web sites that collect sensitive but unclassified information from the general public as part of their assigned mission are authorized to use approved commercially available certificates to provide SSL services. Select from the trusted and validated products lists on DISA's Web site (http://iase.disa.mil/common/index.html).

(10) Every Army organization that maintains a Web site must observe Federal, Defense, and Army policies for protecting personal privacy on official Army Web sites and must establish a process for webmasters/maintainers to routinely screen their Web sites to ensure compliance. At a minimum, Web sites must comply with the following Web privacy rules:

(a) Web masters/maintainers 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 (official Web site of the Department of Defense: http://www.defenselink.mil). For management purposes, statistical summary information or other nonuser 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 cookies will be purged from public Web sites.

(11) All Army private (nonpublicly accessible) Web sites must be located on a ".mil" domain.

(12) Web masters/maintainers will provide a redirect page when the URL of the Web site is changed.

(13) Army organizations maintaining Web sites are required to achieve Web site compliance 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 nondisabled Federal employees and members of the public. Guidance on Section 508 standards concerning Web-based, Intranet, and Internet 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 paras 6–1*p* and *q* on information access.)

(14) Internet Web sites published and sponsored by Army commands but hosted on commercial servers (servers other than "army.mil") are considered official sites and are subject to this policy.

(15) 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 personnel and their families, mission-related needs, and public communications and community relations objectives. No compensation of any kind may be accepted in exchange for a link placed on an organization's publicly accessible official Army Web site. Listings of Web links on Army Web pages must separate external Web links from Government and military links. 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."

(16) Internet Web site owners notified by the AWRAC of a violation will close the Web site or link until corrections have been completed. (See para 5–11 for additional information.)

o. Internet service providers (ISPs). The only authorized access from Army computers, systems, and networks to the Internet is through a DISN-controlled and monitored connection or a NETCOM-controlled and monitored gateway with an exception to policy. Exceptional situations may exist where Army organizations connected to the NIPRNET may also require direct connection to the Internet, for example, through an ISP. These exceptional situations must be protected per DOD security requirements. The organization must submit a waiver request for validation by the DOIM through chain of command to HQDA, CIO/G–6, which then transmits the waiver request to the DISN Security Accreditation Working Group (DSAWG) for final approval. The DSAWG represents the DISN DAA and is the DOD approval authority. (See Web site http://iase.disa.mil/dsawg/ for additional information.)

(1) 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. These "stand-alone" ISP connections must adhere to the HQDA and OSD waiver process.

(2) Internet connections for educational (off-duty or nonduty related) or MWR activities are permitted, but no computer, system, or network used for these purposes can be further 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. AR 215–4 governs IT supplies and services acquired with NAF. These Internet connections will be coordinated through the DOIM with the NETCOM support office prior to connection.

(3) If local Internet access is not available, unit commanders may authorize the use of unit funds (NAF) to establish

ISP accounts for mission requirements per DOD guidelines. Such accounts must receive prior approval by the unit fund manager per AR 215–1.

(4) 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).

(5) 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). VTC facilities designated as a baseline service will be managed by the installation DOIM. The RCIO is responsible for establishing common-user VTC policy, procedures, and guidelines for the respective region. The DOIM or other designate will approve all VTC systems. All items will meet DOD Video Conferencing Profile (FTR 1080B–2002 (body and app A)) standards. Army activities will consider contract vehicles managed centrally by DISA, GSA, DOD, and Army when acquiring VTC equipment and services. Funding for equipment and personnel to operate, maintain, and install VTC facilities is in accordance with the Army baseline service agreement. All standards will be in full compliance with the JTA–A. 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.

(1) VTC fixed (permanent) facilities costing over the Other Procurement, Army (OPA) threshold will be validated by the requesting DOIM, approved by the chain of command, prioritized by the MACOM/FOA commander, and funded by CIO/G–6. VTC investment items are DA-controlled with a cost threshold established by Congress.

(2) Defense 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.

(3) 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 para 6–4*p*(1), 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 IMA POM submissions.

(4) The video teleconferencing 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 AR or DODD (that is, AR 380–53 and AR 25–2 for information systems security monitoring; AR 190–53 for law enforcement purposes; AR 380–10 for electronic surveillance; and DODD 4640.1 for the monitoring or recording of telephone conversations for business purposes). 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/information systems directory. Each DOIM is responsible for maintaining a telephone/information systems directory that provides local organizations' telephone numbers.

(1) *Publishing directories.* Each Army installation will publish an organizational telephone/information systems directory at least annually. Organizational directories made available to the public will list organizational titles rather than names of individuals. Exceptions will be determined by the local PAO. When the telephone exchange serves several installations, the main installation publishes the directory and includes listing for the subinstallations. 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). Directories will contain the mandatory warning banner per AR 380–53 and AR 25–2. 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 or AKO–S, as appropriate, but not on the WWW. Every effort will be made to publish e-directories and avoid printing and distribution costs. (See also para 6–4*n*, above.)

v. Global Broadcast Service. Global Broadcast Service (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.

w. Portable, mobile, and cellular telephones.

(1) 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 para 6–1*e* for authorized use.)

(2) 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 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 follow:

(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) 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 BASECOM services through NETCOM/9th ASC or other approved Army support contracts. DOIMs will coordinate with NETCOM/9th ASC to order services and hardware using appropriate blanket purchase agreements (BPAs).

(5) 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) 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) DOIMs will educate cellular telephone users in policies and procedures to prevent security violations and inappropriate use.

x. Secure cell systems. Tactical units in a deployed environment will use only the Army's encrypted secure cell systems.

y. 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 6–4*w*, above.) All Army organizations will use NETCOM/9th ASC BPAs established to provide economies of scale. Beepers/pagers will be authorized service based upon the following service areas:

(1) *Local.* The area directly adjacent to an Army installation or facility.

(2) *State.* The geographic area of any state in the United States.

(3) *CONUS.* The geographical region of the CONUS.

(4) *Worldwide.* The service will reach any country in the world.

z. Fax machines. Only plain paper fax machines will be acquired. Information managers will pro-actively 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.

aa. Handheld and mobile/transportable satellite terminal equipment. Handheld and mobile satellite terminals are

nontactical radio transmission terminals that require satellite spectrum use approval and have a billed cost associated with transmission time.

(1) *International Maritime Satellite (Inmarsat).* This technology is a commercial international satellite system, which provides global transportable satellite communications for commercial, emergency, and safety applications on land, at sea, and in the air. Inmarsat use is limited to "peaceful purposes." 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 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. Per Assistant Secretary of Defense (ASD) (Networks and Information Integration) direction, Inmarsat must be used with a STU III, STE, or other NSA-approved device.

(a) Procurement of Inmarsat equipment. MACOMs are responsible to fund Inmarsat terminal acquisition and airtime. Organizations/units will submit their requirements for approval to DCS, G–3, ATTN: DAMO–RQ. Organizations/units will submit a request for service (RFS) for equipment acquisition and airtime through their respective MACOM/supporting DOIM to NETCOM/ESTA–G. The using organization/unit is responsible for arranging the commissioning of Army Inmarsat terminals into satellite access operation by arrangement through NETCOM/ESTA–G.

(b) Operation of Inmarsat equipment. MACOMs/J–6s/G–6s will ensure field operators configure Inmarsat units to the correct Inmarsat land-earth station. MACOM/J–6/G–6 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.

(c) Equipment readiness. MACOM/J–6/G–6s 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.

(2) *IRIDIUM.* IRIDIUM is a unique handheld global satellite terminal system that connects into the DOD satellite gateway via DSN routine secure voice, FTS, ILD, Hawaii local and toll-free number. 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.

(a) MACOMs are responsible for funding IRIDIUM handset acquisition and airtime.

(b) Organizations/units will submit an operational needs statement for approval through the MACOMs/supporting DOIM to DCS, G–3, ATTN: DAMO–RQ.

(c) Organizations/units will submit an RFS for acquisition and airtime through the respective MACOM/supporting DOIM to NETCOM/ESTA–G.

bb. Army management of electromagnetic spectrum. AR 5–12 governs Army-wide 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.

cc. Radio System Support Services.

(1) 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) Installation radio systems support services consist of fixed, trunked, mobile, and portable radio systems. Installation radio system support services are authorized when existing information systems 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. See also chapter 5 of this regulation.

(3) 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.

dd. Leasing of Government-owned telecommunications assets.

(1) 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 information systems 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) 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 paid by telephone companies for lease of any Government-owned appropriated-funded 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 Department of Defense 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) The revenue from the lease of NAF telecommunications assets will be deposited into the NAF activity's fund.

(5) 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 between U.S. Federal departments and agencies.

(6) OCONUS leasing activities will follow this practice in negotiating for new or revising 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.

ee. Wireless Priority Service (WPS) and Wireline GETS. WPS/GETS provides 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. Wireless telephones with the WPS must be obtained through NETCOM/9th ASC via existing BPAs.

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.

a. Defense Information Systems Network (DISN). DISN is DOD's integrated worldwide enterprise-level network for exchanging secure and nonsecure data, voice, and video information.

(1) All Army activities requiring telecommunications services will use the DISN when those services are available and technically and economically feasible to the Army. Requirements will be processed per DODI 4640.14, DISA Circular (DISAC) 310–130–1, and the supporting Army activity's procedures. 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 ASC to ensure DISN is the best solution for the requirements considering the bandwidth, security, connectivity, and other technical issues.

(2) MACOMs, 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 ASC 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 focused on supporting the operational requirements of the Army and capable of supporting a Joint task force headquarters to support contingencies.

(e) Ensure 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. Defense Switched Network (DSN). DSN is the DOD preferred means of providing voice communications for C2. DSN may be used to transmit unclassified facsimile traffic.

(1) Defense Red Switch Network (DRSN) services:

(a) The component commanders and Defense agencies coordinate the overall Joint requirements for DRSN services. The MACOMs are responsible for providing 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.

(b) Unique requirements will be forwarded through the MACOM to HQDA, CIO/G–6, ATTN: SAIS–IOC, for coordination and validation.

(2) Servicing MACOMs 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.

c. Federal Telecommunications System (FTS). FTS is the preferred network for administrative long distance voice communications. (See para 6–4*a*.)

d. Satellite communications (SATCOM) systems.

(1) SATCOM includes those systems owned or leased and operated by the DOD that communicate to and/or receive communications from spacecraft and those commercial satellite communications 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 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.

(2) The CJCSI 6250.01A 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. 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.

(a) Army is assigned PPBE process responsibility for the payload and network control systems of the MILSATCOM System, the Wideband Gapfiller System, and the Advanced Wideband System/Transformational Communications Architecture.

(b) Army is designated as lead Military Department for the development and acquisition of ground SATCOM earth terminals (less Military Strategic and Tactical Relay System (MILSTAR) ground command post and GBS Primary Injection Point terminals).

(c) All Army components requiring SATCOM service from DISA will submit an RFS through NETCOM/ESTA. 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/ESTA.

e. 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). 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.

f. The Defense Message System (DMS).

(1) The DMS has been designated as the DOD record messaging system. DMS is the replacement for AUTODIN. The DMS will be implemented in all environments. Army activities that require the use of official organizational messaging will migrate to the DMS. Organizational messaging is defined as correspondence that is used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies official positions, or issues official guidance is considered an organizational message. DMS migration will be accomplished through centralized fielding by the Army DMS PM.

(2) Attachments to DMS messages are limited to the maximum size specified in Allied Communication Publication (ACP) 123A.

g. 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 C.

h. Military telecommunications agreements.

(1) Army activities will adhere to U.S.-ratified international standardization agreements (including NATO standardization agreements and ABCA Quadrapartite standardization agreements) when designing or procuring telecommunications equipment. Exceptions may be requested through CIO/G–6 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) Army activities will carry out assigned responsibilities contained in formally consummated Memoranda of Understanding or similar documents between the U.S. Government and U.S. Agencies, and NATO and NATO nations, to include formal U.S. commitments made in support of NATO and NATO member communications plans, programs, and policy.

(3) 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) When NATO and NATO member communications are nonexistent, inadequate, or not cost-effective for use, the United States 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 United States to provide minimum essential unilateral control of the U.S. forces and to complement NATO and NATO member nation communications.

(5) Interoperability will be achieved on a planned, step-by-step basis and efforts toward consolidated, collocated, interconnected, interoperable systems will result in mutually supportive U.S., NATO, and NATO member systems that satisfy NATO, other NATO members, and U.S. requirements.

i. Compatibility and interoperability of tactical C3I systems.

(1) 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 nontactical C3I systems.

(2) The coordination and validation of requirements, to include required joint coordination, will be accomplished per AR 70–1 and AR 71–9.

(3) For the interfaces between tactical and nontactical 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 DOD directives and joint directives.

(4) The J–6, Joint Staff, 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) 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 and evaluation of tactical C3I systems will be performed during the acquisition process. T&E will be conducted throughout the acquisition process via established system bench marking 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. Developers of performance measurements (that is, functional proponents, PMs) will use these performance measurements to ascertain performance and results-based management of C3I systems. Interoperability testing will be conducted at the CTSF and/or the JITC to ensure compliance and certification.

6–6. IT support for military construction (MILCON)

IT requirements must be considered for MILCON so that the resulting building has a built-in IT infrastructure that satisfies the occupants' requirements on the beneficial occupancy date (BOD).

a. Planning, designing and monitoring construction. The supporting DOIM will provide oversight on 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 requirements involved in each construction project, from concept design to BOD. The DOIM identifies IT functional requirements (both inside and outside plants). The DOIM provides the IT functional requirements, to include mission-related and base support, for inclusion in the Corps of Engineers' 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. Cost estimates and funding. The DOIMs will ensure that IT cost estimates are identified for each component

supporting MILCON facilities. The RCIO will approve the DOIM input to the DD Form 1391. IT funding and installation responsibilities will be identified for inclusion to the DD Form 1391 (FY, Military Construction Project Data) per AR 415–15, appendix L. The requesting organization and IMA will ensure the IT requirements identified in the DD Form 1391 are submitted to the POM manager.

c. Host and tenant relationships. Inter-Service support agreements (ISAs) and interagency support agreements will include IT support for MILCON.

d. 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, 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.

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 PSYOPS 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 regional 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 7–11).

(11) Non-VI activities using COTS office business graphic software (such as PowerPoint) 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 advertising and sales mission.

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. Combat camera (COMCAM)

a. 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 G–3 will ensure that all contingency and war plans include COMCAM requirements in their operation annexes.

b. COMCAM teams will provide still and motion imagery coverage of force deployments and events before, during, and after military engagements.

c. FORSCOM is responsible for COMCAM mission taskings. Requirements for COMCAM support will be identified to FORSCOM and copy furnished to NETCOM/9th ASC.

d. Corps COMCAM teams are organic to specific corps units and provide VI documentation at corps headquarters down to division and brigade level. COMCAM soldiers will be trained and equipped to respond as an integral part of the combat support force.

e. Army COMCAM teams will be tasked to participate in DOD joint exercises along with COMCAM teams from other services. Only the Chairman, Joint Chiefs of Staff (CJCS) and combatant commanders have the authority to task joint service COMCAM teams. (Also see DODD 5040.4 and FM 6–02.40).

f. COMCAM capabilities will be maintained by the region/FOAs to augment Active Army resources and to support mobilization plans.

g. COMCAM is not a contractible function.

h. 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.

7–3. VI responsibilities

a. ASD (Public Affairs) Defense Visual Information (DVI) assigns various responsibilities to the military departments to provide VI support to more than one DOD component. Army responsible official responsibilities are as follows:

(1) AVID will provide a central capability to rent, lease, procure, or produce multimedia/VI productions in support of Army, DOD, other military departments, and Government agency requirements as requested. AVID is the only authorized Army activity to issue production procurement contracts exceeding the 49 percent limit for support services (see para 7–8*a*(11)). AVID will also provide support to OSD, JS, other Army organizations, and Federal agencies within the Pentagon reservation and the NCR.

(2) The Armed Forces Institute of Pathology (AFIP) will operate and maintain a still and motion media record center for medical pathology materials to support DOD organizations and the Veterans Administration hospitals. AFIP will also provide medical/scientific exhibit design, construction, shipment, installation and storage services in support of DOD, military departments, and the Department of Veteran Affairs.

b. The NETCOM/9th ASC VI office will—

(1) Execute the DA Multimedia/VI production and Distribution Program (DAMVIPDP).

(2) Recommend changes to VI activity authorization documents per table 7–1.

(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.

(6) Compile and analyze VI Annual Workload and Cost Data Report information.

c. Regional/FOA VI managers will—

(1) Develop a 6-year VI systems acquisition plan and submit the investment portion of the plan and annual updates to CIO/G–6 (VI) for POM development.

(2) Validate, consolidate, and submit VI investment system requirements for the VISP.

(3) Approve and/or validate VI production multimedia requirements, maintain production registers, and submit requirements for the annual DAMVIPDP.

(4) Annually review, validate, approve as authorized, and forward requests (DA Form 5697, Visual Information Activity Authorization Record) for establishment, expansion or disestablishment of VI activities per the level of authority in table 7–1.

(5) Annually review and forward the VI Annual Workload and Cost Data Report.

(6) Conduct commercial activity reviews for assigned VI functions (T–807–Visual Information) per AR 5–20.

(7) Serve as the representative to the Army Visual Information Steering Committee.

(8) Manage VI nontactical documentation quarterly submissions to the VI documentation (VIDOC) program.

7–4. VI activities

a. A VI activity performs or provides any product or service listed in paragraphs 7–8 and 7–9. 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*.) The VI types of activity authorizations are at table 7–1. The approval level to establish, change capability, or disestablish VI activities is provided in table 7–1.

b. VI 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 re-establish combat and combat support elements or rotational positions to support war plans.

c. Authorized VI activities will be assigned a Department of Defense Visual Information Activity Number (DVIAN) by the regional VI manager in coordination with the NETCOM/9th ASC VI office and the CIO/G–6. DA Form 5697 will be used to assign the DVIAN and to identify the VI activity's authorized capabilities and is available on the Army Publishing Directorate (APD) Web site and the Army Electronic Library (AEL) CD–ROM. 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.

d. Authorized VI activities may establish satellite activities to provide more responsive support to their customers. A satellite activity does not require a separate DVIAN.

e. VI activities will submit a VI Annual Workload and Cost Data Report (RCS CSIM–59). The products and services provided by a satellite activity will be included in the parent organization's report. (See DA Pam 25–91).

f. 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 document that identifies 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 Regional 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) VI activities may be authorized to fabricate VI aids, displays, and exhibits.

(3) VI 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.

g. Media loans will be recorded on DA Form 4103 (Visual Information Product Loan Order). 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 APD Web site and the AEL CD–ROM.

Table 7–1
Types of VI Activities

Type	Primary function	Description of capabilities	Level of approval
A	VI support center	Provides VI support services to all organizations on an installation or within a defined geographic area (region/FOAs). Note: Activities should list their specific capabilities here (for example, still photography, motion picture, linear and/or digital video, audio recording, graphic art, VI media and/or equipment loan, maintenance, presentation support, digital photography, chemical processing, and so on).	CIO/G–6
B	VI production (local)	Includes production, reproduction, and distribution of local multimedia/VI productions to support an individual organization, an installation, or a defined geographic area.	Region
C	VI production (nonlocal)	Includes all functions of type 'B' activities, plus production of VI productions (video and multimedia) for use outside of the local installation or defined geographic area.	CIO/G–6
D	VI production (contracting)	Provides commercial contracting, purchase, or rental of VI productions.	CIO/G–6
E	VI records centers	Central management and storage facility for VI products.	ASD(PA)
F	Component Accessioning Point	Central point for VI imagery screening and for forwarding imagery to the VI records center.	CIO/G–6
H	VI documentation	Recording of technical and nontechnical events. Note: Activities should list their specific types of VIDOC being recorded here.	CIO/G–6

Table 7–1
Types of VI Activities—Continued

Type	Primary function	Description of capabilities	Level of approval
I	Product distribution	Central VI product distribution activity.	ASD(PA)
J	VI mgt	Includes staff functions and management and administration of VI activities.	
1	HQDA		ASD(PA)
2	MACOM, DRU, or FOA		CIO/G–6
3	Common Spt		Region
4	Dedicated		Region
K	VI support center (dedicated)	Provides VI support to a specific organization or organizational element only (also see type A, above). Note: Activities should list their specific capabilities here (for example, still photography, motion picture, linear and/or digital video, audio recording, graphic art, VI media and/or equipment loan, maintenance, presentation support, digital photography, chemical processing, and so on).	CIO/G–6 or region
Q	Broadcast	Includes closed-circuit television support to a defined area. Note: Activities should specify their type of broadcast capability (for example, CCTV, master/community antenna, command channel(s), and so on).	Region
S	National Guard Activities	Includes DA military photos, photojournalism, electronic photojournalism, and other VI media to support public affairs (command information, news gathering, and community relations) for TOE/MTOE public affairs units only.	CIO/G–6

7–5. VI activity operations

a. VI 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. VI 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. VI activities with a unit identification code (UIC) may maintain a dedicated property book of VI equipment and systems.

7–6. Automated information management system

All VI activities are required to use the current version of VIAMS. Each VI activity will maintain VIAMS data for the current year plus 2 previous years (FY+2). The CIO/G–6 is the VIAMS functional proponent, with FORSCOM acting as the responsible official. A CCB, established by the Army VI Steering Committee, will validate, approve, and prioritize all requested application changes.

7–7. Equipment and systems

a. Definition. VI 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 (FSC) 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. (Ref AR 25–30.)

b. Funding requirements. VI 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 regional/FOA VI manager and coordinated with IMA regional offices prior to forwarding to NETCOM/9th ASC. 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. Regions/FOAs 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 Regional/FOA VI manager. This authority may be delegated further.

c. Resourcing. VI 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 Regional/FOA VI manager in a consolidated 6-year plan. This plan is the basis for establishing annual funding increments for equipment replacement. Regional/FOA VI managers will also submit investment VI equipment requirements for inclusion in the regional/FOA POM submissions. VI activity managers will plan for VI expense and investment equipment through installation resource management channels as part of their annual operating budget.

(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 (RCS: CSIM–46)), available on the APD Web site and the AEL CD–ROM. (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 DODD 5040.2. Per AR 710–2, user/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) Regional 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, VHS tape players, TVs, or portable projection screens. The following guidelines will be observed when exercising this option:

(a) Only expense-funded VI equipment with a per item/system cost under $25,000 may be considered for end-user ownership.

(b) The user/owner will ensure that all equipment meets interoperability standards, JTA–A and VI architectures. User/owners will maintain their own equipment. (VI 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, depending upon the terms of the contract, be included in the total procurement cost.

(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.

d. Certification of assets.

(1) The Army must certify VI equipment and systems with network or wireless interface capability as JTA–A-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 $2.5M million. Equipment and systems between $250,000 and $900,000 are certified through the regional VI manager and the CIO/G–6 and the VISP. 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 RCIO or delegated to the regional VI manager. Certification authority may be delegated to the lowest level that assures

(2) *Releasing telephone/information systems directories to the public.* All installation directories will be unclassified. Installation telephone/information systems 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 further 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 or other private Web site.

(3) *The AKO/Community Pages.* The AKO/Community Pages will be utilized for publishing directories containing individuals' names. The AKO is the primary tool for individual locator information.

s. Cable television (CATV). CATV distributes one or more television programs by modulated radio frequency or other signals through a cable distribution system to standard television or radio receivers of subscribers who pay for such service.

(1) CATV facilities 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 CATV is the responsibility of the CIO/G–6 at the Army level and will be executed at the local level at the discretion of the installation commander.

(2) Cable television service is primarily intended for the use and enjoyment of personnel occupying quarters on military installations and in this regard should be considered the equivalent in purpose to MWR activities. DOD installations are cable television franchising authorities for the purpose of the applicable cable televisions laws. As a result, installations may issue a franchise, which grants a cable television company access to the installation and designated rights of way to permit the cable company to serve its subscribers. The individual subscriber to the cable television service contracts directly with the cable company for service and payment of subscription fees and no appropriated funds are involved. Provisions of the Federal Acquisition Regulation (FAR) are applicable only when a DOD component subscribes to cable television service for official DOD business and appropriated funds are utilized for payment of subscriber fees.

(3) Army policy is to provide for nonexclusive 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 of CATV by the Army and is not governed by the FAR. The franchise agreement must not obligate the Army to procure CATV services for official purposes. If services are to be procured using appropriated funds, they will be procured by contract in accordance with the FAR and its supplements.

(4) Appropriated funds available for morale and welfare purposes may be spent for user and connection fees for services to appropriated fund activities that serve the community as a whole per AR 215–1. Examples of these activities are hospital patient lounges and barracks day rooms.

(5) No Army member will be coerced to subscribe to a franchisee's services. Installations will not use military funds or personnel to produce free programming solely for the benefit of a commercial CATV company.

(6) The Army will require that the CATV 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 CATV 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 CATV 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 Public Affairs Office will support installation programming by providing advice and 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), CATV, or other systems for internal public affairs purposes.

t. Master/Community Antenna Television (M/CATV) systems. Existing Government-owned M/CATV systems will be converted to commercial CATV systems. The expenditure of appropriated funds to expand Government-owned M/CATV systems to provide entertainment television service to NAF activities or individual persons is not authorized unless such M/CATV expenditures are justified under provisions of AR 415–15.

u. Commercial satellite television services. Commercial satellite television services may be obtained when CATV is unavailable to the installation/building. When obtaining commercial satellite television services, the same policies for obtaining CATV apply. The individual subscriber to the commercial satellite television services contracts directly with the service provider and is responsible for payment of any subscription fees. Provisions of the FAR are applicable to obtaining services when an Army activity subscribes for official DOD business and appropriated funds are utilized for payment of subscribers' fees. DOIM validation is required before any official services can be obtained.

positive and effective controls and ensures compliance with the JTA–A. Written certification must be provided to the contracting officer prior to procurement for VI equipment and systems under $250,000.

e. Visual information systems program (VISP). The VISP provides for the annual identification, funding, and acquisition of requirements for COTS VI investment (DA controlled) equipment and systems. TDA 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. DA-controlled equipment/systems are investment items above the threshold established by Congress. CIO/G–6 is the functional proponent for the VISP and the program executor is NETCOM/9th ASC. 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) VI equipment used exclusively for RDT&E.

(2) Medical peculiar VI items such as medical life support and patient monitoring systems, MEDCASE items (radiological graphic processors), medical information display systems, and so on.

(3) Permanently installed installation public address systems (including bugle-call systems), 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) VI 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.

f. Funding. Investment VI equipment and systems are normally funded with OPA–2 dollars. Operations and Maintenance, Army funds support expense items.

g. 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. Regional/FOA VI managers will ensure that only authorized VI activities with established DVIANs purchase JTA–A-compliant VI equipment.

7–8. Products

a. Multimedia/VI productions. Multimedia/VI productions are usually 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, video tape, hard disk, removable magnetic or optical disk, CD–ROM, interactive video disk (IVD), digital video disk (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 (17 USC, Copyrights) unless prior permission from the copyright owner is obtained in writing. (Also see para 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) VI report content that is obsolete within a year does not require life-cycle management. Examples include VI reports (technical, intelligence, maintenance reports), video reports, and videos of briefings, seminars, conferences, classroom instruction, or commanders' messages to their troops that are for short-term immediate use.

(c) VI 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 produced for the purpose of communicating clinical, histo-pathological, 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 4040.7 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 this area.

1. Local productions will be reviewed annually for currency.

2. Total cost will not exceed $15,000, and 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 Army-wide 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. (Ref DA Pam 25–91, chapter 6).

6. Activity VI managers will maintain a PAN register for all local in-house produced productions. The in-house production register will be maintained on file by the installation VI manager for current fiscal year plus 2 additional years (FY+2).

(b) Nonlocal productions. These productions are for multi-installation, regional/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.

2. Nonlocal productions will be assigned a production identification number (PIN). A PIN register or log will be maintained to ensure control and accountability of nonlocal multimedia/VI productions. (See DA Pam 25–91 for format.)

3. Joint VI Service Distribution Activity (JVISDA) distributes nonlocal 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.

5. Nonlocal multimedia/VI productions (in-house and COTS) will be reviewed by the office of primary responsibility (OPR) for obsolescence within 5 years of their initial distribution and every 3 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).

(7) The DAMVIPDP provides for the annual identification, funding, and acquisition of multimedia/VI production and distribution requirements. All Army organizations will identify their requirements for nonlocal multimedia/VI productions and forward their requests to their supporting regional/FOA VI manager for validation. Regional/FOA VI managers will forward valid requirements to CIO/G–6 for certification and inclusion in the DAVIPDP. Multimedia/VI productions will be managed throughout their life cycle and will be distributed so as to ensure legal, efficient, and cost-effective usage.

(8) 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 as amended by P.L. 105–220 and DOD guidance.

(9) 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.

(10) Contracting: 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 5040.7.

(a) When the total production contract support exceeds 49 percent of the total production cost (excluding replication and distribution), the production will be assigned to the designated Army contracting activity for production. Regional/FOAs will use AVID procurement contracts to procure multimedia/VI productions. (See table 7-1.)

(b) Regional/FOA, installation VI managers, AVID 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.

(11) The VI production activity (for in-house production) or the AVID 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.

(12) 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 in-house capabilities when this method of acquisition is the most cost-effective. Production support services will not exceed 49 percent of the total cost of the production.

(c) When COTS proprietary productions are purchased, leased, or rented.

(13) 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.

(14) Reproduction of any Army production in whole or in part is prohibited without the approval of the proponent, regional/FOA 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.

(15) 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—

(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 DUSA will make the final determination.

(16) 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 requirements for nonlocal multimedia/VI productions. (See para 7–8*a*(7).)

(17) 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 a 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.

(18) Requests to translate or rescore new nonlocal multimedia/VI productions into a foreign language will be processed in the same manner as all other nonlocal 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.

(19) 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 NTIS/NAC, 5285 Port Royal Road, Springfield, VA 22161.

(20) 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.

(21) Current authorized distribution formats for official Army multimedia/VI productions are 1/2-inch VHS videotape, CD-ROM, or videodisc. As equipment and communications become available existing formats will migrate to DVD or an online network for distribution.

b. Video/audio documentation. Recordings of specific types of official events as they occur (for example, briefings, seminars, VIP visits) are authorized. These recordings are not edited and are normally provided to the customer in their raw form or may be incorporated into a VI production. VI activities will discuss possible retention of these recordings as record material with the customer. (Also see paras 7–9*c* and 7–12.)

(1) *Images.*

(a) Imaging, either 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) VI activities will not prepare galley-formatted text for printing. Typesetting support is the responsibility of the local servicing publications and printing activity.

(c) 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 DODD 5040.5 and DA Pam 25–91.)

(d) 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.

(e) Use, duplication, and electronic alteration of commercially obtained electronic images will be in accordance with applicable copyrights and licenses.

(f) Only authorized VI activities may process official military personnel file photographs and electronically submit the Department of the Army 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 of a music score prior to delivery to the customer. These types of reports will be accomplished as a low priority service. These video reports will not be reported as VI productions on the VI Annual Workload and Cost Data Report. (See *b*, above, or DA Pam 25–91.)

c. Use of digitized text. Life-cycle management of multimedia products containing only digitized text is governed by printing and publications guidelines.

7–9. Services

a. Customer self-help. VI 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. VI activities will provide customer consultation services in support of official requirements for customer and professionally developed VI products and services.

c. Ready access file. VI activities will develop a consolidated electronic source of imagery that is accessible by official customers. CIO/G–6 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 (DAVIS). The 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 will be searched prior to any start of a new VI production to determine if a suitable product already exists. ASD(PA) DVI is the database manager and provides policy guidance concerning the operation of DAVIS functions. The DAVIS is accessible at Web site http://dodimagery.afis.osd.mil.

f. Broadcast services.

(1) *CATV.* The VI activity will operate only the command channel(s) provided as part of the CATV franchise agreement. See chapter 6 of this regulation for CATV policy.

(2) *CCTV.* The VI activity will operate installation 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.

7–10. VI records management

a. Original local or nonlocal Army multimedia/VI productions and VI products with their associated administrative documentation are controlled as official records throughout their life cycle and disposal of 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 OSD Web site and the AEL CD–ROM.

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. VI managers will maintain continuous custody of permanent or unscheduled VI records prior to their retirement or submission to the Component Accessioning Point (CAP).

f. All VI managers will prevent the accidental or deliberate alteration (see DODD 5040.5) or erasure of VI records.

g. 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 Defense Visual Information Center (DVIC).

h. All VI record documentation will be forwarded quarterly for accessioning through command channels to the VI activity's assigned CAP.

i. Nonlocal 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.

7–11. VI documentation (VIDOC) program

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 this 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 VI documentation program includes both tactical and nontactical documentation.

a. Tactical documentation. Record VI documentation 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 Joint Combat Camera Center (JCCC) 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 to AVID for accessioning into the DVIC. (See DA Pam 25–91.)

b. Nontactical documentation.

(1) Nontactical (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 quarterly submissions of record VI documentation to an authorized CAP. The capturing and submission of record VI documentation will be considered high priority by all VI activities.

(3) Nontactical record documentation includes linear and digital video, photographic imagery, graphic artwork (including recruiting and safety posters/artwork), or audiotape. VI activities, to meet minimum submission requirements, 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 member.

(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; 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 2 years after the date of recording; earlier destruction is authorized.

d. Use of chain-of-command photographs is a MACOM decision. Photographs of the President, Secretary of Defense, SECARMY, and the CSA may be obtained by local VI activities from JVISDA.

7–12. Restrictions

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 regional VI manager 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 5040.2). 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 waken or cast doubt on the credibility of the Army or DOD.

c. Prohibited recordings. Title 18, Chapter 25, United States Code 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 (Ref. 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. 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 in to 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 5040.7, AR 25–55, AR 340–21, AR 380–5, and DA Pam 25–91.

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. All VI multimedia/VI productions will be reviewed for public exhibition prior to distribution (see DODI 5040.7). 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) Requests for public clearance review will be submitted to the installation PA office.

(3) All cleared still or electronic images or stock footage will be forwarded to AVID for accessioning into the DVIC.

(4) 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 VI 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. The statutory authority for records management is contained in AR 25–400–2. In addition, civil penalties may be imposed for violating the Freedom of Information Act (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 1997–24, the records management function transferred from the CIO/G–6 (formerly known as DISC4) to the DCS, G–1. 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 law and regulatory guidance.

8–2. Management concept

a. Records management plans, policies, and programs provide for the modern, efficient, and systematic life-cycle management of all information of record value, regardless of format or media. It establishes requirements for agency heads and commanders at all echelons to document the Army's official business and ensure accessibility of record information throughout the lifecycle of the information; keeps the DA in compliance with information access laws; and

protects the rights and interests of the Army, its soldiers, veterans and their families, and the American public. In addition, civil penalties may be imposed for violating the Freedom of Information Act (AR 25–55), and civil and criminal penalties may be imposed for violating the Privacy Act (AR 340–21).

b. This chapter implements the following DOD directives and instructions:

(1) DOD 4525.8–M, Official Mail Manual.

(2) DODD 5025.12, Standardization of Military and Associated Terminology.

(3) DODD 5015.2, DOD Records Management Program.

(4) DOD 5400.7–R, DOD Freedom of Information Act Program.

(5) DODD 5025.1, DOD Directives System

(6) DODD 5400.11, DOD Privacy Program.

(7) DODD 8910.1, Management and Control of Information Requirements.

(8) DOD 5015.2 STD, Design Criteria Standard for Electronic Records Management Software Applications.

(9) DODI 5040.6, Life-Cycle Management of DOD Visual Information (VI).

c. Title 44, Section 3102 of the United States Code (44 USC 3102) requires the head of each Federal Agency to maintain a continuing program for the economical and efficient management of the records of the agency.

d. The Records Management Program includes the following provisions:

(1) Creating by the most efficient, economical, and technologically advanced methods only that information essential for conducting operations and preserving that information as records.

(2) Establishing effective controls over the creation, organization, maintenance, use, and disposition of Army record information.

(3) Providing 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) Ensuring that permanently valuable information is preserved and all other record information is retained, reviewed, and disposed of systematically as prescribed by AR 25–400–2.

(5) Establishing the management program for Army electronic recordkeeping systems.

e. 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 (hard disks, tapes, diskettes), optical recording media (for example, laser disk, optical disk, optical card, optical tape, CD, DVD), all electronic formats (office automation software—for example, word processing, spreadsheet, presentation), e-mail, Web sites, information systems, 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.

f. The following are not included within the statutory definition of the word "record" (DOD 5400.7–R, 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, that 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.

g. Records management official's duties:

(1) Army proponent records management duties are specified in paragraph 2–10, DCS, G–1 responsibilities.

(2) The Director, U.S. Army Records Management and Declassification Agency (USARMDA) has operational responsibility (as determined by the DCS, G–1) for records management and its subprograms as defined in paragraph 8–5. (See AR 25–400–2 for a complete list of duties.)

(3) MACOM functions pertaining to records management are specified in chapter 2. MACOM records administrators have command-wide responsibilities for ensuring the creation and preservation of official mission records throughout subordinate units and activities. Under ARIMS, the records administrator has the ability to create, modify, and approve office record lists (ORLs) for all subordinate units within the MACOM and can view all of those units' records. Records administrators will—

(a) Be appointed in writing.

(b) Provide policy interpretation, procedural guidance, and oversight of mission-unique records management programs.

(c) Manage, oversee, and direct the records management program and its subprograms.

(d) Survey and appraise the agency or command records management program at least once every 3 years and prescribe and ensure necessary corrective action is taken.

(e) Ensure availability of records management training for personnel.

(f) Oversee, survey, and appraise the methods and operations of records holding areas (RHAs) of the agency or command. Maintain liaison and coordinate records transfer, retirement, and retrieval with Federal Records Centers and local National Archives and Records Administration (NARA) offices.

(g) Monitor and coordinate records transfer, retirement, and retrieval with central records holding area facilities and the Army Electronic Archives.

(h) Maintain liaison with and provide advice and assistance to security managers in developing and executing a program to reduce classified records holdings.

(i) 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. Ensure that records management requirements are documented and included in systems acquisition as appropriate. Keep abreast of and/or implement new IT for access storage, retrieval and disposition of information. Ensure records management factors are considered for the MACOM's C4/IT acquisitions.

(j) Ensure compliance with the DA Freedom of Information Act Program, the Army Privacy Program, and EO 12958.

(k) Ensure compliance with and enforcement of DA policies and rules governing management information requirements under the Management Information Control System.

(l) 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.

(m) Provide technical assistance to the VI records managers as required.

(n) Ensure records management factors are considered for all C4/IT acquisitions.

(4) MSCs, FOAs, DRUs, separately authorized activities, tenant and satellite organization records managers will—

(a) Be appointed in writing.

(b) Approve ORLs for the organization's units.

(c) Serve as local authority for records management procedures/issues.

(d) Manage, oversee, and direct the organization's records management program and its subprograms.

(e) Survey and appraise the organization's records management program at least once every 3 years and prescribe and ensure that necessary corrective action is taken.

(f) Maintain liaison and coordinate records transfer, retirement, and retrieval with the installation RHA.

(g) When not served by an installation RHA, index records to be turned in by the organization's offices into the ARIMS Records Input Processing System.

(h) Ensure records are properly arranged and packed prior to movement from the organization to a records center. Maintain liaison and coordinate records transfer, retirement, and retrieval with the National Records Center facilities and local NARA offices.

(i) Ensure availability of training for records management personnel.

(j) 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.

(k) Provide technical assistance to VI records managers.

(5) IMA will provide program coordination to the regional records managers, as required.

(6) Regional-level records managers will—

(a) Provide functional management and oversight of the records management program and its subprograms for the

installations in their respective regions in accordance with AR 25–400–2, AR 25–55, AR 340–21, DA Pam 25–51, AR 380–5, AR 25–50, AR 25–58, AR 335–15, AR 25–52, and DA Pam 25–50.

(b) Regional mail managers will execute the official mail cost control program in their respective regions per AR 25–51.

(7) Installation-level records managers serve on the installation staff and have installation-wide responsibilities. They will—

(a) Be appointed in writing.

(b) Approve ORLs for subunits.

(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 installation's records management program at least once every 3 years and prescribe and ensure that necessary corrective action is taken.

(f) Manage and provide staff direction for the operation of the RHA. Ensure records are properly arranged and packed prior to movement from the records holding area to a records center. Maintain liaison and coordinate records transfer, retirement, and retrieval with the Federal Records Centers and local NARA offices. Index records turned in by installation offices and tenant offices into the ARIMS Records Input Processing System.

(g) Ensure that records management factors are considered for all installation level IT/C4I acquisitions.

(h) Ensure availability of training for records management personnel.

(i) 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.

(j) Provide technical assistance to VI records managers, as required. Installation mail managers will execute the official mail cost-control program throughout the installation per AR 25–51.

(8) Records coordinators will be designated at subelements as necessary for program execution. Coordinators will perform records management duties as assigned:

(a) Develop ORL for their unit.

(b) Coordinate transfer of T (long-term/permanent) records to the installation or central RHA.

(c) Serve as the subject matter expert for the unit's records.

(d) Resolve indexing problems with the contractor.

(e) Perform other records management duties as assigned.

(9) An action officer is any individual who creates official records on behalf of the Army. The action officer (at all levels of command) has the capability to search the Army's office record instructions to help determine if a document is an official record, create a draft ORL to be maintained for each office symbol within a unit or organization, submit records to a designated records holding facility, and search for and request records in ARIMS. The action officer can also view all records submitted to ARIMS internal to the unit. In addition, the action officer identifies records as K (short-term) or T and, for e-records, registers in ARIMS, and submits records via the e-mail capture and store feature of ARIMS.

8–3. Life-cycle management of records

a. Maintaining 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, chap 6, 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. Protect the rights and interests of the Army, its uniformed members and their dependents, civilian employees, and affiliated personnel.

c. Control the quantity and quality of records produced by the Army.

d. 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.

e. Simplify the activities, systems, and processes of record creation and of record maintenance and use.

f. Direct continuing attention to the life-cycle management of information from initial creation to final disposition.

g. 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.

h. Employ modern technologies and cost effective provide alternatives for storage, retrieval, and use of records.

i. Ensure records are preserved in a manner and on media that meet all legal and archival requirements.

j. Incorporate standards and technical specifications in all information systems' functional requirements to ensure the life-cycle management of record information.

k. 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 information resources management review process.

8–4. Tenets

In executing the mission, objectives, and subprograms, 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 subprograms

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 noncurrent records in accordance with NARA-approved disposition schedules. (See AR 25–400–2.)

(1) *ARIMS.* The ARIMS provides policy and procedures for the systematic identification, maintenance, retirement, and destruction of Army record information. It provides for the establishment and operation of central and overseas command records holding areas, and furnishes the legal authority for destruction of nonpermanent Army records by organizational elements. ARIMS replaces the Modern Army Records Keeping System (MARKS).

(2) *Electronic recordkeeping systems.* Electronic recordkeeping systems collect, organize, and categorize records to facilitate their preservation, retrieval, use, and disposition. These systems may include audio, e-mail, office automation software applications, databases, and visual and image information systems utilizing IT.

(3) *Manual recordkeeping systems.* Life-cycle management of information contained in manual information systems includes paper, image, audio, photo, and visual information.

b. Official mail and distribution management.

(1) Official mail and distribution management provides rapid handling and accurate delivery of official mail throughout the Army at minimum cost. To do this and to increase efficiency, processing steps are kept to a necessary minimum; sound principles of workflow are applied; modern equipment, supplies, and devices are used; and operations are kept as simple as possible. This subprogram includes responsibility for ZIP+4 addressing and office symbols. (See AR 25–51.)

(2) Office symbols are used to identify originators of correspondence and electronically transmitted messages and to denote the proper placement of Army organizations in the Army structure for historical and records purposes. They are also used as part of the address when forwarding correspondence and mail to, from, or within HQDA. Office symbols will be as short as possible. Office symbols should be added or deleted when new organizational elements are created, existing organizational elements are terminated, or organizational elements are divided or merged. The first two letters of an office symbol indicate the organization's primary command. "SA" is reserved for OSA or an OSA activity; "DA" for other HQDA staff elements. Office symbols of HQDA FOAs, staff support agencies, and DRUs will begin with two letters representing the parent staff agency.

(3) The basic office symbol for MACOMs will be constructed using the HQDA construction method and assigned by the U.S. Army Records Management and Declassification Agency. (See https://www.arims.army.mil for procedures.) The AASA (for the Secretariat and ARSTAF) and MACOMs will submit their requests for deletions, additions, and corrections to the U.S. Army Records Management and Declassification Agency, ATTN: AHRC–PDD–RP, 7701 Telegraph Rd, Rm 102, Alexandria, VA 22315–3860. Other units and activities will submit to their next-higher headquarters.

(4) Requests for exceptions to the HQDA construction standards as outlined in the USARMDA Web site https://www.arims.army.mil will be submitted through the organization's chain of command to USARMDA for approval.

c. 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.)

d. Rulemaking. The rulemaking program satisfies the legal requirement for the Army to publish, in the Federal Register, Army regulations or other issuances and notices that have a substantial and continuing impact on the public. (See AR 25–58.)

e. FOIA 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.)

f. 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.)

g. Management Information Control Office (MICO). The HQDA 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 requirement control symbols (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 Army IM requirements, IT products, and public information requirements. (See AR 335–15.)

h. 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.

(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. Per AR 500–3, HQDA, MACOMs, and certain activities maintain copies of emergency operating records at predesignated relocation and alternate sites. (See also para 6–1*b*.)

(2) *Rights and interests records.* These are records essential to the preservation of the legal and financial rights and interests of individual citizens and the Army (including its Service members). These records include retirement records; finance and accounting records; medical records; payroll records; personnel action records; certain records from operational deployments; records related to contracts, entitlements, and/or leases; and other valuable research records.

i. Terminology, abbreviations, and brevity code management. The Terminology Standardization Management Program contains two interrelated areas:

(1) *Dictionary of Army Terms.* This program is designed to assist in reaching a more-common understanding of the meaning of terminology used extensively by the U.S. Army and with the DOD and International Standardization usage.

(2) *Authorized abbreviation and brevity codes.* This program prescribes authorized abbreviations and brevity codes and procedures for their use within the Army. Program objectives are to standardize abbreviations and brevity codes used within DOD and between DOD elements and NATO countries and assist in reaching a mutual or common definition and meaning of terminology between DOD elements, and between DOD elements and NATO member countries.

j. 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 awaiting transfer of legal authority over the records to the National Archives.

k. Oversight records administration of Joint/multi-Service/DOD. These are records that have been transferred into a Federal Records Repository and for which DOD has designated the Army as executive agency for record administration until legal authority is transferred to the National Archives.

l. Archivist of the Army. The DCS, G–1 is the Archivist of the Army and is responsible for the senior 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 Archivist of the Army takes final action to offer records to NARA. Standard Form (SF) 258 (Agreement to Transfer Records to the National Archives of the United States) is used to offer Army records formally to the Archivist of the United States and to accession records into the National Archives. Use of SF 258 is limited to DCS, G–1 (DAPE–ZXI–RM) or as designated by the DCS, G–1.

m. Defense Visual Information Center (DVIC). 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.)

n. Armed Services Center for Unit Records Research 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.

8–6. General policies

a. Personal papers pertain solely to an individual's private affairs. 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. For convenience of reference, a Government official may accumulate extra copies of records that they have drafted, reviewed, or otherwise acted upon while in office. 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. Government officials may accumulate these extra copies, if this action does not—

(1) Diminish the official records of the agency.

(2) Violate national security or confidentiality required by privacy or other interests protected by law.

(3) Exceed normal administrative costs.

c. Army general officers and senior civilian executives (normally limited to SES 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 preserve the integrity of these collections with the identification of the donor, such as the "Abrams Papers," or the "Bradley Papers." During the donors' lifetimes, their own collections will be open to them for research, reference, or historical inquiry. 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 Freedom of Information Act or the Privacy Act.

(6) Any record, including any normally nonrecord 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.

(8) Records identified below may be removed when the individual creating them retires, resigns, or otherwise terminates his or her tenure of office.

(a) All personal and private papers that do not contain references to official business.

(b) Personal diaries, logs, notes, memoranda, tapes, disks, and summaries of telephone conversations, if all official information has been duplicated in official memoranda for record for retention in the official files.

(c) Reference books and other personal items brought from private life.

e. Separation and control of personal papers at the time of creation is the best way to avoid mixing personal papers with official records.

f. 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, 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 (AR 25–400–2, AR 340–21, AR 380–5).

(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; or when hostile action by a foreign power appears imminent, if their potential capture by the enemy is prejudicial to the interests of the United States. If emergency destruction is done, a list of records destroyed, their inclusive dates, and the date destroyed will be compiled as much as possible. This information will be forwarded through channels to the U.S. Army Records Management and Declassification Agency, ATTN: AHRC–PDD–R, Stop 5603, 6000 6th Street, Fort Belvoir, VA 22060–5603, as expeditiously as theater or operational conditions permit.

g. All Army users are reminded that one AKM goal is to actively seek ways to identify, catalog, file, search, and retrieve data (that is, records). Commanders must discourage hoarding of information by subordinates and instead

encourage creation of internal business processes, Web sites, relational databases, repositories, or libraries of related information for all command users and eventually all qualified Army users with a need to know to access.

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. 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 records retention schedule–Army, such as retention period for the 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. Where more than one ARIMS file series is contained in the record, systems of records, or database, the longest included retention schedule will apply. Electronic records management automated information systems will comply with DOD 5015.2–STD.

(2) 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 United States, however, transfers legal custody from the Army to the Archivist of the United States.

(3) 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 retrieve records in these media.

(4) 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 both the Army and any individual members, dependents, employees, or citizens that it affects.

(5) VI original materials are retained in their original format.

(6) When microforms are the recording media for permanent records, silver halide film must be employed. For records that do not have a permanent retention requirement, the original microform can be either dry silver or silver halide, and the choice is dependent upon which provides the most efficient and economical filming process. The original microform copy normally will be used only to make either diazo or vesicular duplicates. Duplicate microforms will be used for current day-to-day reference or operations, as they are more economical and scratch resistant than the original microform.

(7) When the record copy from an information system 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. It is the responsibility of the appropriate information manager to ensure that the type of film used meets established retention requirements. If the document being converted to microform contains a permanent ARIMS record series as determined by the Archivist of the United States, special conditions noted in *c*, below, apply.

(8) When the permanent record copy is on microform, an archival film test (sometimes called the methylene blue technique) is required to ensure damaging chemicals that will deteriorate the recorded information are not retained on the film. In addition to the film test, all microforms produced will conform to quality standards and formats.

c. 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 U.S. Army Records Management and Declassification Agency, address at paragraph 8–6*f*.

d. Due to personal health risks, agencies will not destroy optical media (CDs, 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.

8–8. Electronic records management

a. 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 information system 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 disposition of electronic records must be determined as early as possible in the life cycle of the information system.

b. VI digital still and motion images are excluded from this paragraph. VI 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

Note: Per DA General Order 1997–23, this function transferred from CIO/G–6 (formerly DISC4) to the AASA. Performance of the missions and functions will continue to be subject to the oversight of the CIO/G–6.

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. These subprograms provide a means to execute the established laws, regulations, and directives that govern the publications and printing discipline. It also includes initiatives to modernize the Army publications system with new publishing management concepts and to access state-of-the-art printing, duplicating, self-service copying, and related equipment, including electronic means. 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 the Army Enterprise Portal (AKO). 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 JTA–A compliant.

b. APD manages the two official Web sites for Army-wide 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. Proponents and Army commands will staff unclassified draft publications and forms electronically by posting to AKO or AKO–S. Use of e-mail attachments will be kept to the minimum. If attachments to e-mail must be used, proponents are encouraged to use file compression when sending large file attachments to multiple addressees via e-mail, especially when file attachments exceed 5 megabytes. 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. Unless otherwise granted an exception by the Office of the Administrative Assistant, staffing of paper copies will be done only when necessary to staff sensitive or classified material or to accommodate addresses that do not have access to e-mail or the Internet. See also paragraph 6–4*n* for guidance on staffing publications on controlled access Web sites. 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

a. Publishing and printing materials.

(1) An Army organization will not publish, print, or reproduce material, mechanically or electronically, unless an official designated by the commander certifies that the material is required for the official conduct of Government business.

(2) No periodical or nonrecurring publication will be printed unless approved by the appropriate HQDA or MACOM review committee.

(3) No private or commercial printing will be done at any Army printing or duplicating facility even though the Army is offered reimbursement.

(4) A proposed Army publication will be considered nonessential and will not be printed or reproduced in any media, to include electronic, if—

(a) It is not directly needed to effectively, efficiently, and economically conduct official business.

(b) It cannot be produced and distributed in time to fully serve its intended purpose.

(c) It duplicates, beyond the requirements for clarity, material already available to the publication's users.

b. Unauthorized products. Unauthorized publications or products will not be printed or reproduced. They include—

(1) Elaborate conference or other program reports.

(2) Any publication with material that tends to glorify persons, units, or activities of the DA. (Official publications announcing the issue of citations and awards are exempt.) This will apply whether the publication will be produced by an Army printing or duplicating facility procured through the Defense Automated Printing Service (DAPS) or for the Army under contract. It will also apply whether APF or NAF will be used.

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

All Army printing and duplicating (including CD–ROM replication) will be done through one of the following methods. All organizations exempted from the provisions of Defense Management Resource Decisions (DMRD 998) and Program Budget Decisions (PBD 415) may continue to procure printing directly from GPO regional printing procurement offices.

a. Departmental printing and replication.

(1) HQDA agencies and designated commands will obtain departmental printing through APD. APD will procure this printing through DAPS.

(2) Commands and field activities will not produce or procure departmental printing unless authorized by APD under a decentralized printing program.

b. Field printing and duplicating. Every effort must be made to requisition field printing requirements from DAPS.

(1) In-house reproduction must be limited to those items that are—

(a) Not available within the time constraints required.

(b) Not available on an existing DAPS contract.

(c) Not conducive to the establishment of a DAPS contract.

(d) Not repetitive in nature.

(2) Only the regional and installation designated functional managers are authorized to procure printing from DAPS regional offices.

c. Effectiveness and economy in accomplishing mission objectives will be considered in determining whether in-house or commercial resources will be used.

d. 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.

e. 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 (SAAA–PP), 105 Army Pentagon, Washington, DC 20310–0105.

Appendix A
References

Section I
Required Publications

AR 5–20
Commercial Activities Program. (Cited in paras 6–2*c*(1) and 7–3*c*(6).)

AR 25–2
Information Assurance. (Cited in paras 1–7, 1–8, 2–16*g*, 2–27*a*(6), 4–7*h*, 5–1*a*, 5–3*c*, 5–4, 5–5*b*, 5–5*c*, 5–7*c*, 5–8*c*, 6–1*g*, 6–1*i*, 6–4*q*, 6–4*r*, 6–4*cc*, 7–8*a*(17), and 8–8*a*.)

AR 25–30
The Army Publishing Program. (Cited in paras 7–7*a*, 9–1, and 9–4.)

AR 25–55
The Department of the Army Freedom of Information Act Program. (Cited in paras 1–7, 7–12*i*, 7–12*l*, 8–2*f*, 8–2*g*(6), and 8–5*e*.)

AR 25–400–2
The Army Records Information Management System (ARIMS). (Cited in paras 1–5, 2–12*i*, 2–24, 6–1*c*, 6–4*m*(10), 7–10*a*, 7–12*l*, 8–2*d*(4), 8–2*g*(2), 8–2*g*(6), 8–3*a*, 8–5*a*, 8–6*f*, 8–7*a*, 8–7*b*, and 8–8*a*.)

AR 70–1
Army Acquisition Policy. (Cited in paras 2–5, 2–16*c*, 3–2*b*(4), 3–7, 6–1*n*(2), 6–2*g*(8), 6–5*i*, and 7–2*h*.)

AR 71–9
Materiel Requirements. (Cited in paras 2–16*c*, 3–4*f*, 3–5*a*(1), 3–6*d*, 3–7, 6–5*i*, 7–2*h*, and B–4*b*(17).)

AR 215–1
Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities. (Cited in paras 6–1*n*, 6–4*o*, and 6–4*s*.)

AR 215–4
Nonappropriated Fund Contracting. (Cited in paras 6–1*n*(2) and 6–4*o*.)

AR 340–21
The Army Privacy Program. (Cited in paras 1–7, 7–12*i*, 7–12*l*, 8–2*g*(6), 8–5*f*, and 8–6*f*.)

AR 360–1
The Army Public Affairs Program. (Cited in paras 6–4*n*(4) and 6–4*s*(6)(*f*).)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 4–7*h*, 7–8*a*(17), 7–12*i*, 8–2*g*(6), 8–6*c*, 8–6*d*(3), and 8–6*f*.)

AR 380–53
Information Systems Security Monitoring. (Cited in paras 6–4*q* and 6–4*r*.)

DA Pam 25–1–1
Installation Information Services. (Cited in paras 6–2*k*(3) and 8–5.)

DA Pam 25–91
Visual Information Procedures. (Cited in paras 7–4*e*, 7–5*e*, 7–7*c*(1), 7–7*e*, 7–8*a*(6), 7–8*b*(1), 7–10*a*, 7–10*b*, 7–11*a*, 7–11*b*, 7–12*i*, and 8–8*b*.)

DOD 5500.7–R
Joint Ethics Regulation (JER). (Cited in paras 1–8 and 6–1*d*(1).) (Available at http://www.dtic.mil/whs/directives.)

DODD 1015.14
Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources. (Cited in para 6–1*n*.) (Available at http://www.dtic.mil/whs/directives.)

DODD 5040.2
Visual Information (VI). (Cited in paras 2–1*o*, 7–7*c*(2)(*a*), and 7–12*b*.) (Available at http://www.dtic.mil/whs/directives.)

DODI 4640.14
Base and Long-Haul Telecommunications Equipment and Services. (Cited in para 6–5*a*(1).) (Available at http://www.dtic.mil/whs/directives.)

DODI 5000.2
Operation of the Defense Acquisition System. (Cited in paras 2–5*g* and 3–7*b*(2).) (Available at http://www.dtic.mil/whs/directives.)

DODI 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP). (Cited in paras 5–3*b*, 5–3*c*, and 5–5*c*.) (Available at http://www.dtic.mil/whs/directives.)

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). (Cited in para 6–4*n*(13).) (Available at http://www.gpoaccess.gov/uscode/index.html.)

P.L. 107–347
E–Government Act of 2002 (Cited in paras 2–1*e*(8) and 3–9*c*.) (Available at http://thomas.loc.gov/bss/.)

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.

ACP 123(A)
Common Messaging Strategy and Procedures. (Available at http://www.jcs.mil/j5/cceb/acps/.)

AR 5–11
Management of Army Models and Simulations.

AR 5–12
Army Management of the Electromagnetic Spectrum.

AR 5–22
The Army Proponent System.

AR 10–5
Headquarters, Department of the Army.

AR 12–8
Operations and Procedures.

AR 25–6
Military Affiliate Radio System (MARS).

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 105–70
Amateur Radio Operations.

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 340–26
Duplicate Emergency Files 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 415–15
Army Military Construction Program Development and Execution.

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.

CJCSI 3170.01E
Joint Capabilities Integration and Development System. (Available at http://www.dtic.mil/cjcs_directives.)

CJCSI 6110.01A
CJCS–Controlled Tactical Communications Assets. (Available at http://www.dtic.mil/cjcs_directives.)

CJCSI 6212.01C
Interoperability and Supportability of Information Technology and National Security Systems. (Available at http://www.dtic.mil/cjcs_directives.)

CJCSI 6215.01B
Policy for Department of Defense Voice Networks. (Available at http://www.dtic.mil/cjcs_directives.)

CJCSI 6250.01B
Satellite Communications. (Available at http://www.dtic.mil/cjcs_directives.)

CTA 50–909
Field and Garrison Furnishings and Equipment

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 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.)

DFARS Subpart 208.74
Enterprise Software Agreements. (Available at http://www.acq.osd.mil/dpap/dfars/index.htm.)

DFAS–IN Regulation 37–1
Finance and Accounting Policy Implementation. (Available at http://www.asafm.army.mil/budget/di/di.asp.)

DISA Circular 310–130–1
Submission of Telecommunications Service Requests. (Available at Web site https://disa-ca.dtic.mil/pubs.)

DISA Circular 310–130–4
Defense User's Guide to the Telecommunications Service Priority (TSP) System. (Available at Web site https://disa-ca.dtic.mil/pubs.)

DOD 4160.21–M
Defense Materiel Disposition Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD 4525.8–M
DOD Official Mail Manual. (Available at http://www.dtic.mil/whs/directives.)

DOD 5015.2–STD
Design Criteria Standard for Electronic Records Management Software Applications. (Available at http://www.dtic.mil/whs/directives.)

DOD 5200.2–R
Personnel Security Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 5400.7–R
DOD Freedom of Information Act Program. (Available at http://www.dtic.mil/whs/directives.)

DOD 7000.14–R (vol. 2B, chap. 18)
Department of Defense Financial Management Regulations (FMRs) (Information Technology/National Security Systems). (Available at http://www.dtic.mil/whs/directives.)

DODD 1015.2
Military Morale, Welfare, and Recreation (MWR). (Available at http://www.dtic.mil/whs/directives.)

DODD 1035.1
Telework Policy for Department of Defense. (Available at http://www.dtic.mil/whs/directives.)

DODD 3020.26
Defense Continuity Programs. (Available at http://www.dtic.mil/whs/directives.)

DODD 4630.5
Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). (Available at http://www.dtic.mil/whs/directives.)

DODD 4640.1
Telephone Monitoring and Recording. (Available at http://www.dtic.mil/whs/directives.)

DODD 4640.7
DOD Telecommunications System (DTS) in the National Capital Region (NCR). (Available at http://www.dtic.mil/whs/directives.)

DODD 4640.13
Management of Base and Long-Haul Telecommunications Equipment and Services. (Available at http://www.dtic.mil/whs/directives.)

DODD 5015.2
DOD Records Management Program. (Available at http://www.dtic.mil/whs/directives.)

DODD 5025.1
DOD Directives System. (Available at http://www.dtic.mil/whs/directives.)

DODD 5025.12
Standardization of Military and Associated Terminology. (Available at http://www.dtic.mil/whs/directives.)

DODD 5040.3
DOD Joint Visual Information Services. (Available at http://www.dtic.mil/whs/directives.)

DODD 5040.4
Joint Combat Camera (COMCAM) Program. (Available at http://www.dtic.mil/whs/directives.)

DODD 5040.5
Alteration of Official DOD Imagery. (Available at http://www.dtic.mil/whs/directives.)

DODD 5230.9
Clearance of DOD Information for Public Release. (Available at http://www.dtic.mil/whs/directives.)

DODD 5400.11
DOD Privacy Program. (Available at http://www.dtic.mil/whs/directives.)

DODD 5530.3
International Agreements. (Available at http://www.dtic.mil/whs/directives.)

DODD 8000.1
Management of DOD Information Resources and Information Technology. (Available at http://www.dtic.mil/whs/directives.)

DODD 8100.1
Global Information Grid (GIG) Overarching Policy. (Available at http://www.dtic.mil/whs/directives.)

DODD 8190.3
Smart Card Technology. (Available at http://www.dtic.mil/whs/directives.)

DODD 8500.1
Information Assurance (IA). (Available at http://www.dtic.mil/whs/directives.)

DODI 1000.15
Private Organizations on DOD Installations. (Available at http://www.dtic.mil/whs/directives.)

DODI 1015.12
Lodging Program Resource Management. (Available at http://www.dtic.mil/whs/directives.)

DODI 4000.19
Interservice and Intragovernmental Support. (Available at http://www.dtic.mil/whs/directives.)

DODI 5040.6
Life-Cycle Management of DOD Visual Information (VI). (Available at http://www.dtic.mil/whs/directives.)

DODI 5040.7
Visual Information (VI) Production Procedures. (Available at http://www.dtic.mil/whs/directives.)

DODI 5330.2
Specifications for DOD Letterheads. (Available at http://www.dtic.mil/whs/directives.)

DODI 5335.1
Telecommunications Services in the National Capital Region (NCR). (Available at http://www.dtic.mil/whs/directives.)

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.)

Executive Order 12600
Predisclosure Notification Procedures for Confidential Commercial Information. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Executive Order 12845
Requiring Agencies to Purchase Energy Efficient Computer Equipment. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Executive Order 12958
Classified National Security Information. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Executive Order 12999
Educational Technology: Ensuring Opportunity for all Children in the Next Century. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Executive Order 13011
Federal Information Technology. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Executive Order 13103
Computer Software Piracy. (Available at http://www.archives.gov/federal_register/executive_orders/disposition_tables.html.)

Federal Acquisition Regulation
Government Printing and Binding Regulations. (Available at http://www.arnet.gov/far/.)

FM 6–02.40
Visual Information Operations

General Order 1997–23
Transfer of Publications and Printing

General Order 1997–24
Transfer of Records Management

General Records Schedule 21
Audiovisual Records, Transmittal No. 8, December 1998. (Available at http://www.archives.gov/records_management/ardor/.)

JCS 1–02
Department of Defense Dictionary of Military and Associated Terms. (Available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.)

Joint Travel Regulations
(Available at http://secureapp2.hqda.pentagon.mi./perdiem/.)

National Security Decision Directive 145
National Policy on Telecommunications and Automated Information Systems Security. (Available at http://www.fas.org/irp/offdocs/direct.htm.)

National Security Directive 42
National Policy for the Security of National Security Telecommunications and Information Systems. (Available at http://www.fas.org/irp/offdocs/direct.htm.)

NSTISSD No. 900, Section IV (Responsibilities)
Governing Procedures of the National Telecommunications and Information Systems Security Committee (NSTISSC). (Available at http://www.cnss.gov/policies.html.)

NSTISSP No. 11
National Information Assurance Acquisition Policy. (Available at http://www.cnss.gov/policies.html.)

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–109
Major Systems Acquisitions. (Obtain hard copy (only) from the Office of Management and Budget, telephone (202) 395–3080.)

OMB Cir A–130
Management of Federal Information Resources. (Available at http://www.whitehouse.gov/omb/circulars/index.html.)

P.L. 92–463
Federal Advisory Committee Act. (Available at http://www.epic.org/open_gov/faca.html.)

P.L. 97–375
Congressional Reports Elimination Act of 1982. (Available at http://thomas.loc.gov/bss.)

P.L. 104–106 (40 USC 1401 et seq.)
The Clinger–Cohen Act of 1996 (formerly Div E, Information Technology Management Reform Act, Defense Authorization Act of 1996). (Available at http://www.gpoaccess.gov/plaws/index.html.)

P.L. 104–191
Health Insurance Portability and Accountability Act of 1996 (HIPAA). (Available at http://thomas.loc.gov/bss/.)

P.L. 105–220
Rehabilitation Act Amendments of 1998. (Available at http://http://thomas.loc.gov/bss/.)

P.L. 105–277
The Government Paperwork Elimination Act (Div. C, Title XVII 112 STAT, 2681–751, Oct 21, 1998). (Available at http://http://thomas.loc.gov/bss/.)

P.L. 106–398
Government Information Security Reform Act (Title X, Subtitle G of the 2001 Defense Authorization Act (Sections 1061–1065)). (Available at http://http://thomas.loc.gov/bss/.)

P.L. 106–554
Federal Information Quality Act (Section 515, FY 2001 Treasury and General Government Appropriations Act). (Available at http://http://thomas.loc.gov/bss/.)

SB 700–20 (EM 0007 FEDLOG)
Army Adopted/Other Items Selected for Authorizations/List of Reportable Items. (Available at http://weblog.logsa.army.mil/index.shtml.)

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.)

5 USC 552a
The Privacy Act. (Available at http://www.gpoaccess.gov/uscode/index.html.)

5 USC 601–612 (chapter 6)
The Analysis of Regulatory Functions. (Available at http://www.gpoaccess.gov/uscode/index.html.)

10 USC 2686
Utilities and Services: Sale; Expansion and Extension of Systems and Facilities. (Available at http://www.gpoaccess.gov/uscode/index.html.)

15 USC Chapter 96 (P.L. 106–229)
Electronic Signatures in Global and National Commerce Act (also known as the "E–Sign Act"). (Available at http://www.gpoaccess.gov/uscode/index.html.)

17 USC 101, 501
Copyrights. (Available at http://www.gpoaccess.gov/uscode/index.html.)

18 USC 701
Official Badges, Identification Cards, Other Insignia. (Available at http://www.gpoaccess.gov/uscode/index.html.)

29 USC 762 (P.L. 101–336)
Americans with Disabilities Act of 1990. (Available at http://www.gpoaccess.gov/uscode/index.html.)

29 USC 794d (P.L. 99–506))
Rehabilitation Act of 1975. (Available at http://www.gpoaccess.gov/uscode/index.html.)

31 USC 1115, 1116 (P.L. 103–62)
The Government Performance and Results Act (GPRA). (Available at http://www.gpoaccess.gov/uscode/index.html.)

40 USC 759 (P.L. 100–235)
Computer Security Act of 1987. (Available at http://www.gpoaccess.gov/uscode/index.html.)

40 USC 762 (P.L. 100–542)
Telecommunications Accessibility Enhancement Act of 1988. (Available at http://www.gpoaccess.gov/uscode/index.html.)

41 USC 413 (P.L. 103–355)
Tests of Innovative Procurement Methods and Procedures (The Federal Acquisition Streamlining Act of 1994 (FASA)). (Available at http://www.gpoaccess.gov/uscode/index.html.)

44 USC 3101–3107 (Chapter 31)
Records Management by Federal Agencies. (Available at http://www.gpoaccess.gov/uscode/index.html.)

44 USC, Chapter 35
Coordination of Federal Information Policy (Paperwork Reduction Act of 1995 and The Federal Information Security Management Act). (Available at http://www.gpoaccess.gov/uscode/index.html.)

44 USC Chapters 29, 31, and 33 (P.L. 94–575)
Federal Records Management Amendments of 1976. (Available at http://www.gpoaccess.gov/uscode/index.html.)

44 USC 3501–3520 (P.L. 96–511)
Paperwork Reduction Act of 1980. (Available at http://www.gpoaccess.gov/uscode/index.html.)

47 USC 151, 157, 158, 201, 203, 552, 553, 571–73 (P.L. 104–104)
Telecommunications Act of 1996. (Available at http://www.gpoaccess.gov/uscode/index.html.)

47 USC 226 (P.L. 101–435)
Telephone Operator Consumer Service Improvement Act. (Available at http://www.gpoaccess.gov/uscode/index.html.)

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
Prescribed Forms

Except where otherwise indicated below, the following forms are available as follows: DA forms are available on the Army Electronic Library (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(3)g.)

DA Form 4103
Visual Information Product Loan Order. (Prescribed in para 7–4*g*.)

DA Form 5695
Information Management Requirement/Project Document. (Prescribed in para 7–7*c*(1).)

DA Form 5697
Army Visual Information Activity Authorization Record. (Prescribed in para 7–4*c*.)

DD Form 1367
Commercial Communications Work Order. (Prescribed in para 6–4*c*(2).)

DD Form 1995
Visual Information (VI) Production Request and Report. (Prescribed in para 7–8*a*(6).)

DD Form 2537
Visual Information Caption Sheet. (Prescribed in para 7–10*b*.)

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. Army National Guard (ARNG)

Installation voice and data services may be provided to off-post 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 BASOPS services with funding provided per the current Army reimbursement policy for BASOPS services. (See ASA(FM&C)Web site: http://www.asafm.army.mil/pubs/pubs.asp.)

B–2. United States Army Reserve (USAR)

Installation voice and data services may be provided to on-post and off-post Army Reserve units and activities on a reimbursable basis with funding from the USAR. On-post voice and data services to USAR units and activities will be provided as common BASOPS services with funding provided in accordance with the current Army reimbursement policy for BASOPS services. (See ASA(FM&C) Web site: http://www.asafm.army.mil/pubs/pubs.asp.)

B–3. Reserve Officer Training Corps (ROTC)

Local voice and data services for senior and junior 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 FTS and equivalent service, should be considered prior to approving commercial service.

B–4. Army MWR programs and NAF activities

The Army policy for providing telecommunications services to Army MWR operations is defined within AR 215–1. Class A–2 official telephone service will be provided in CONUS and OCONUS on a nonreimbursable basis for the conduct of executive control and essential command supervision (ECECS) and C2/management functions. This service provides Army MWR the capability to execute the Army's fiscal and fiduciary responsibility to manage the NAF Government assets from point of receipt to final disposition. Access to data networks or cable plants will be provided per paragraph 6–4 on an as-needed basis. 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. MWR commercial 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 (DeCA)

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 service is provided 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, MACOMs 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 Services (AAFES)

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 commercial 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 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 6215.01B provides guidance on when U.S. civilian contractor personnel can use the DSN.

B–8. Field operating activities/direct reporting units

FOAs and 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 a civil works function. The mix of service type is mutually determined at the local level.

d. Access to data services and networks are 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 dependents on an Army installation. Access to other voice and data services is dependent upon local agreements.

B–10. American Red Cross (ARC)

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 TDY 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 when necessary, from transient billets to DSN and the local calling area. 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 (P.L. 101–435, codified in 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, provide Class C telephone service. The installation DOIM has authority to approve a higher class of service or special features.

B–13. Private telephone service for hospital patients

The hospital administrator will coordinate with the installation DOIM for infrastructure for the local telephone company to provide private unofficial telephone service to hospital patients upon request. 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. Only reimbursable long-distance telephone services may be provided. Labor unions are not authorized DSN access. Access to other voice and data services is dependent upon local 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

Provide reimbursable voice and data service 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 (ACS) Volunteers and Army family support groups

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 FTS) through local operations centers or installation telephone operators as long as such communications support the APF command support functions. 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 information management (IM) and information technology (IT). They include key controls for CIO management, IT Architecture, information assurance, C4/IT support and services, visual information management, records management, and publishing management.

C–2. Purpose

The purpose of this checklist is to assist HQDA, FOAs, MACOMs, 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, 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 5 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 IA managers? (All)

b. CIO management (chap 3).

(1) Are the duties and responsibilities of the senior information manager clearly designated in the organization's mission and function? (HQDA, region, MACOM, FOA)

(2) Has the installation clearly established a region CIO who has the sole responsibility of implementing the region's IM/IT program?

(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, MACOM, FOA)

(4) Does the organization have a strategic plan that is linked to their mission? Is it periodically updated? (HQDA, MACOM, FOA)

(5) Has a forum been established to develop and implement C4/IT procedures, requirements, and priorities? (RCIO/MACOM/DOIM)

(6) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (MACOM, region, FOA)

(7) Does the IT investment screening process include addressing the following questions and resolving all issues prior to making an IT investment and initiating any process analysis or improvement? (HQDA, MACOM, region, FOA)

(8) Does the process support core/priority mission functions? (HQDA, MACOM, region, FOA)

(9) Can the process be eliminated? (HQDA, MACOM, FOA)

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

(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, MACOM, FOA)

(12) Are exceptions to the IT investment-screening process clearly documented? (HQDA, MACOM, FOA)

(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, MACOM, FOA)

(14) Are IT investment decisions made a part of the organization's integrated capital planning process or are IT projects separated out? (HQDA, MACOM, FOA)

(15) Does the organization have a process in place to conduct periodic reviews (in-house 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, MACOM, FOA)

(16) Does the organization have a process for documenting and disseminating results of this review? (HQDA, MACOM, FOA)

(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, MACOM, FOA)

(18) Have webification status and future webification plans been reported within the 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, MACOM, FOA, PEO, PM)

(21) Have IT investments been synchronized to overall DOD/Army mission priorities? (HQDA, MACOM, 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, MACOM)

c. Army Enterprise Architecture (chap 4). (All.)

(1) Has the organization developed the appropriate architectures for the AKEA 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 Joint Capabilities and Integrated Development System (JCIDS), acquisition of SoS and FoS, software blocking, force development, and lessons learned from operations?

(3) Has the organization developed the appropriate architectures for the ABEA that support the migration of current systems infrastructure, net-centric warfare, enterprise application integration, and business process modernization and

align with the seven DOD BEA domains: Acquisition/Procurement, Human Resource Management, Finance and Accounting, Logistics, Technical Infrastructure, Installations and Environment, and Strategic Planning and Budgeting?

d. Information assurance (chap 5) (Applies to MACOM, separate reporting activity, region, installation, unit.)

(1) Has an IA program been established at all levels?

(2) At each level, have the appropriate IA personnel been appointed?

(3) Are IAVA messages being acted upon and reported in a timely fashion?

(4) Are all information systems and networks accredited and certified? When a new information system 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 stand-alone workstations?

(7) Are database management systems 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 level of training necessary and appropriate to perform their designated information assurance 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?

(14) Is the IA manager NTSSI 4011 certified?

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 being conducted of current IT to ensure they are still required and meeting user needs? (HQDA, MACOM)

(4) Are quarterly reviews being conducted of current IT within the AITR and verified by the users that they are still required and meeting users needs? (HQDA, MACOM)

(5) Are evaluations being conducted of existing systems for obsolescence? (HQDA, MACOM)

(6) Is an accurate inventory being maintained and validated annually for IT equipment? (DOIM, IMO)

(7) Are continuity of operations plans and procedures documented, distributed, and tested at least biannually? (MACOM, DOIM)

(8) Has guidance been provided to ensure all software is checked for viruses before being loaded? (DOIM)

(9) Are existing capabilities and/or assets considered prior to upgrading, improving, or implementing local area networks? (RCIO, DOIM)

(10) Are uneconomical IT service contracts identified and terminated? (All)

(11) Has the DOIM coordinated the acquisition of licenses with the ASCPO prior to entering into an agreement with a COTS vendor? (DOIM)

(12) Are spare capacity and functional expansion on IT being considered and/or used when new requirements are identified? (All)

(13) Has the DOIM reported its server consolidation status for all its Army tenants to the Army CIO/G–6? (DOIM)

(14) Are measures being taken to ensure that hard drives are disposed of properly? (DOIM)

(15) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (RCIO, DOIM)

(16) Has guidance been provided to review and revalidate cellular telephones and pagers every 2 years? (RCIO, DOIM)

(17) 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)

(18) Is there a requirement for cellular phones and pagers to be recorded in the property book? (DOIM)

(19) Has the DOIM implemented accountable billing procedures? (DOIM)

(20) Have maintenance and support strategies been devised to minimize overall systems life-cycle cost at an acceptable level of risk? (PEO, PM, MACOM)

(21) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (RCIO, DOIM, IMO)

(22) Are private sector service providers made aware that written assurance of compliance with software copyright laws may be required? (RCIO, DOIM, IMO)

(23) Are existing portals being migrated to AKO and AKO–S? (All)

(24) Does each Web site contain a clearly defined purpose statement that supports the mission of the organization? (All)

(25) 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)

(26) If applicable, does this 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)

(27) Is this Web site free of commercial sponsorship and advertising? (All)

(28) Is the Web site free of persistent cookies or other devices designed to collect personally identifiable information about Web visitors? (All)

(29) Is each Web site made accessible to handicapped users in accordance with Section 508 of the Rehabilitation Act? (All)

(30) 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.

(31) 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, 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/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.

(32) 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, deficiencies.
— Biographies.
— Family support activities.
— Phone directories.
— Lists of personnel.

(33) Are existing infostructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA, MACOM)

(34) Is the fully qualified domain name (for example, http://www.us.army.mil or http://apd.army.mil) for Army sites registered with the GILS at http://sites.defenselink.mil/, and the contact information updated annually?

(35) 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? (RCIO)

(2) Is the VI manager the single staff manager for all VI functions on the installation? (RCIO)

(3) Are all VI services and equipment, except those specifically exempted by the RCIO, consolidated for centralized VI management? (RCIO)

(4) Do all VI activities under the RCIO's purview have a Defense Visual Information Authorization Number (DVIAN)? (RCIO)

(5) Does the VI manager approve all VI equipment required by AR 25–1, chapter 7? (RCIO)

(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, Nonlocal DAVIS entries, using JVIS contracting facility (RCIO and installation).)

(7) Is a production folder maintained for the life cycle of local productions? (FOA and installation)

(8) Has your VI activity developed and implemented a standard level of agreement document to include an SOP? (RCIO and 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?

(3) Are records managers included in the planning process for new or replacement automated systems? (All)

(4) Are records management reviews of agency and commands conducted at least once every 3 years? (All)

(5) Have instructions been issued specifying the degree of protection to be afforded records stored and used electronically in accordance with classification, releasability, Freedom of Information Act, 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?

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 Army-wide 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 31 May 2002.

C–6. Comments

Help make this a better tool for evaluating management controls. Submit comments to CIO/G–6, ATTN: SAIS–EIG, 107 Army Pentagon, Washington, DC 20310–0107.

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

ABEA
Army Business Enterprise Architecture

ABIC
Army Business Initiative Council

ACAT
acquisition category

ACERT
Army Computer Response Team

ACP
Allied Communications publication

ADS
authoritative data source

AEI
Army Enterprise Infostructure

AEL
Army Electronic Library

AFIP
Armed Forces Institute of Pathology

AFRTS
Armed Forces Radio and Television Service

AITR
Army Information Technology Registry

AEA
Army Enterprise Architecture

AKEA
Army Knowledge Enterprise Architecture

AKM
Army Knowledge Management

AKO
Army Knowledge Online

AMC
U.S. Army Materiel Command

AMP
Army Modernization Plan

ANCDMP
Army Net-Centric Data Management Program

ANSI
American National Standards Institute

APD
Army Publishing Directorate

APF
appropriated fund(s)

APP
Army Publishing Program

AR
Army Regulation

ARC
American Red Cross

ARIMS (formerly MARKS)
Army Records Information Management System

ARNG
Army National Guard

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)

ASC
Army Signal Command

ASCPO
Army Small Computer Program Office

ASD
Assistant Secretary of Defense

AVID
Army Visual Information Directorate

AWRAC
Army Web Risk Assessment Cell

BASECOM
base communications

BASOPS
base operations

BOD
beneficial occupancy date

BPA
blanket purchase agreement

BPR
Business process re-engineering

C2
command and control

C3
command, control, communications

C3I
command, control, communications, and intelligence

C4
command, control, communications, and computers

C4I
command, control, communications, computers and intelligence

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 Lifestyle Support

CAP
Component Accessioning Point

CATV
cable television

CCB
Configuration Control Board

CCS2
command, control, and subordinate systems

CCTV
closed circuit television

CDAd
Component Data Administrator

CD–ROM
Compact Disk–Read Only Memory

CECOM
U.S. Army Communications-Electronics Command

CFR
Code of Federal Regulations

CIK
Crypto Ignition Key

CIO
Chief Information Officer

CJCS
Chairman, Joint Chief of Staff

CJCSI
Chairman, Joint Chief of Staff instruction

CMO
Collaboration Management Office

COIs
communities of interest

COIDAds
communities of interest data administrators

COMCAM
combat camera

COMSEC
communications security

CONUS
continental United States

COOP
continuity of operations plan

CoP
community of practice

COTS
commercial off-the-shelf

CPIM
Capital Planning and Investment Management

CSA
Chief of Staff, Army

CSTS
commercial satellite television services

CTA
common table of allowances

CTSF
Central Technical Support Facility

DA
Department of the Army

DAA
designated approval authority

DAB
Defense Acquisition Board

DAPS
Defense Automated Printing Service

DAMVIPDP
Department of the Army Multimedia/Visual Information Production and Distribution Program

DAVIS
Defense Automated Visual Information System

DBMS
database management systems

DCS
Deputy Chief of Staff

DCID
Director of Central Intelligence Directive

DeCA
Defense Commissary Agency

DISA
Defense Information Systems Agency

DISAC
Defense Information Systems Agency circular

DISN
Defense Information Systems Network

DITIS
Defense Instructional Technology Information System

DITSCAP
Defense IT Security Certification and Accreditation Process

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, personnel, and/or facilities

DPP
data performance plan

DPPS
data performance plan system

DRMS
Defense Reutilization and Marketing System

DRU
direct reporting unit

DSAWG
DISN Security Accreditation Working Group

DSN
Defense Switched Networks

DTS
Defense Telephone System

DTS–W
Defense Telecommunications Service-Washington

DVD
digital video disk

DVI
Defense Visual Information

DVIAN
Department of Defense Visual Information Activity Number

DVIC
Defense Visual Information Center

e-Army
Electronic Army

e-mail
electronic mail

EB/EG
electronic business/electronic government

ECECS
executive control and essential command supervision

EID
enterprise identifier

EIPP
Educational Institution Partnership Program

ELA
enterprise license agreement

EO
Executive order

ERP
enterprise resource planning

ESA
enterprise software agreement

ESI
Enterprise Software Initiative

ESM
Enterprise Systems Management

FAR
Federal Acquisition Regulation

FOA
field operating agency

FOIA
Freedom of Information Act

FORSCOM
U.S. Army Forces Command

FoS
Family-of-Systems

FOUO
For Official Use Only

FTS
Federal Telecommunications System

FX
Foreign Exchange

FY
fiscal year

GBS
Global Broadcast Service

GETS
Government Emergency Telecommunication Service

GIG
Global Information Grid

GILS
Government Information Locator Service

GOTS
Government off-the-shelf

GPO
Government Printing Office

GPS
global positioning system

GSA
General Services Administration

HMW
health, morale, and welfare

HQ
headquarters

HQDA
Headquarters, Department of the Army

HQIM
HQDA Information Manager

HUMINT
human intelligence

IA
information assurance

IAIC
Intra-Army Interoperability Certification

IAM
information assurance manager

IANO
information assurance network officer

IAPM
information assurance program manager

IASO
information assurance security officer

IAVA
Information Assurance Vulnerability Alert

IESS
Information Exchange Standards Specifications

IM
information management

IMA
Installation Management Agency

IMI
interactive multimedia instruction

IMO
information management officer

Inmarsat
International Maritime Satellite

INSCOM
U.S. Army Intelligence and Security Command

IRM
Information Resources Management

ISA
inter-Service support agreement

ISP
Internet service provider

IT
information technology

ITM
information technology management

JCCC
Joint Combat Camera Center

JCIDS
Joint Capabilities and Integrated Development System

JITC
Joint Interoperability Test Command

JPO
Joint Program Office

JS
Joint Staff

JTA
Joint Technical Architecture (DOD)

JTA–A
Joint Technical Architecture–Army

JVISDA
Joint Visual Information Services Distribution Activity

JWICS
Joint Worldwide Intelligence Communications System

JWRAC
Joint Web Risk Assessment Cell

LAN
local area network

LDAP
Lightweight Directory Access Protocol

MACOM
major Army command

MARS
Military Affiliate Radio System

M/CATV
master/community antenna television

MCEB
Military Communications-Electronics Board

MDEP
Management Decision Evaluation Package

MEDCOM
U.S. Army Medical Command

MFP
materiel fielding plan

MICO
Management Information Control Office

MILCON
military construction

MILSATCOM
Military Satellite Communications

MILSTAR
Military Strategic and Tactical Relay System

MSC
major subordinate command

MTOE
modified table of organization and equipment

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
U.S. Army Network Enterprise Technology Command

NETOPS
network operations

NFIP
National Foreign Intelligence Program

NIAP
National Information Assurance Partnership

NIPRNET
Unclassified but Sensitive Internet Protocol Router Network

NSA
National Security Agency

NSS
National Security Systems

OA
Operational Architecture

O&M
operation and maintenance

OCONUS
outside of the continental United States

OMB
Office of Management and Budget

OPA
Other Procurement, Army

ORL
office record list

OSA
Office of the Secretary of the Army

OSD
Office of the Secretary of Defense

OV
Operational View

PA
Public Affairs

Pam
Pamphlet

PAN
production authorization number

PBD
Program Budget Decision

PAO
public affairs officer

PC
end-user microcomputer (personal computer)

PDA
personal digital assistant

PEG
program evaluation group

PEO
program executive officer

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

RCIO
regional Chief Information Officer

RCS
requirements control symbol

RDT&E
research, development, test, and evaluation

RFS
request for service

RHA
records holding area

SA
Systems Architecture

SAP
Special Access Program

SATCOM
satellite communications

SB
supply bulletin

SCI
sensitive compartmented information

SCIF
sensitive compartmented information facility

SECARMY
Secretary of the Army

SF
Standard Form

SGML
Standard Generalized Markup Language

SIPRNET
Secret Internet Protocol Router Network

SLA
service level agreement

SOP
standing operating procedure

SoS
System-of-Systems

SRS
Strategic Readiness System

SSL
secure sockets layer

STARC
State Area Command

STE
secure telephone equipment

STU–III
secure telephone unit, type III

SV
System View

TA
Technical Architecture

T&E
test and evaluation

T–ASA
Television-Audio Support Activity

TAP
The Army Plan

TDA
table of distribution and allowances

TDD
telecommunication devices for the deaf

TECHCON
technical control

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

UIC
unit identification code

URL
uniform resource locator

USAR
United States Army Reserve

USARMDA
U.S. Army Records Management and Declassification Agency

USC
United States Code

VI
visual information

VIAMS
Visual Information Automated Management Software

VIDOC
visual information documentation

VIRIN
visual information record identification number

VISP
Visual Information Systems Program

VTC
video teleconferencing

W3C
World Wide Web Consortium

WWW
World Wide Web

XML
eXtensible Markup Language

XSL/T
eXtensible Stylesheet Language/Transformation

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 Army Enterprise Architecture, 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 by contract with appropriated funds of supplies or services (including construction) by 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
The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.

Army Business Enterprise Architecture (ABEA)
The framework of the business processes and organizations that support the Army's warfighters.

Army Enterprise Architecture (AEA)
A disciplined, structured, comprehensive, and integrated methodology and framework that encompasses all Army information requirements, technical standards, and systems descriptions regardless of the information system's use. The AEA transforms operational visions and associated required capabilities of the warfighters into a blueprint for an integrated and interoperable set of information systems that implements horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA is the combined total of all the Army's Operational, Technical, and System Architectures.

Army Knowledge Management
The Army-wide effort to transform the Army into a net-centric self-learning organization that will improve operational and mission performance.

Army Recordkeeping Systems Management
Cost-effective organization of Army files and records contained in any media so that records are readily retrievable; ensures that records are complete, facilitates the selection and retention of permanent records, and accomplishes the prompt disposition of noncurrent records in accordance with National Archives and Records Administration approved schedules.

Army 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, combat camera, combat and training development, doctrine, and other related issues.

Army Web Risk Assessment Cell
A team of information assurance 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.

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 (BOD)
Construction complete, user move-in dates.

Broadcast
The transmission of radio, television, and data signals through the air waves or fiber optic cable.

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 (GAO BPR Assessment Guide, 1997). (See also DODD 8000.1.)

Business process re-engineering (BPR)
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 only part of what is necessary in the radical change of processes; it refers specifically to the design of a new process (DODD 8000.1.)

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 PBX or CENTREX 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, and subordinate systems (CCS2)
Part of the Army command and control system, which encompass all intrinsic subsystems of the five battlefield functional areas at corps and below, representing the battlefield command and control architecture.

Command, control, communications, and intelligence (C3I)
One of the four domains used to manage Architecture configurations in the ASA. It includes all systems involved in command, control, and communications (C3) and intelligence.

Command, control, communications and computer (C4) systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations.

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. Communications security 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 community of practice (CoP) is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice. CoPs cut across formal organizational structures and increase individual and organizational agility and responsiveness by enabling faster learning, problem solving, and competence building; greater reach to expertise across the force; and quicker development and diffusion of best practices. CoP structures range from informal to formal and may also be referred to as structured professional forums, knowledge networks, or collaborative environments.

Compatibility
The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

Compliance
A system that meets, or is implementing an approved plan to meet, all applicable Technical Architecture (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 3–15 year time frame.

Configuration
An expression in functional terms (that is, expected performance) and in physical terms (that is, appearance and composition).

Connection fee
The charge, if any, imposed on a subscriber by the cable television (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 inter-related 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 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.

Copying
See *duplicating/copying.*

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 JCS 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 community of interest (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 enterprise-wide storing, viewing, and reusing architectures, data models, business rules, and other artifacts associated with functional Army systems.

Data standards
Metadata expressed as authoritative data sources (ADSs), information exchange standards specifications (IESSs), enterprise identifiers (EIDs), and eXtensible Markup Language (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 (DTS)
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 policy developed 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.

Domain
An area of common operational and functional requirements. Currently, there are four domains: command, control, communications, and intelligence (C3I); weapon systems; modeling and simulation; and sustainment.

Duplicating/copying
Production of not more than 5,000 units of a single page or not more than 25,000 units in the aggregate of multiple pages produced utilizing automatic copy-processing or copier-duplicating machines employing electrostatic, thermal, or other copying processes.

Electronic Army (e-Army)
The strategic employment of IT to provide products, services, or knowledge to intended users—whether they are customers, constituents, internal operations employees, information providers, or business partners—that results in

enhanced value to the user. E–Army encompasses the full range of self-service applications available on AKO, Web services; enterprise resource planning systems; e-content, e-record, and e-pubs programs; e-commerce activities; digital signature; and automated processes that facilitate knowledge exchange.

Electronic business (e-business)
A means of performing enterprise activities that involves the use of electronic technologies, including such techniques as facsimile, e-mail, World Wide Web software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

Electronic government (e-government)
The use by government of information technologies that have the ability to transform relations with citizens, employees, businesses partners, and other government organizations. Analogous to e-commerce, which allows businesses to transact with each other more efficiently and brings customers closer to businesses, e-government aims to make the interaction between government and citizens, government and business enterprises, and interagency relationships more friendly, convenient, transparent, and inexpensive.

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
The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise Architecture
The explicit description of the current and desired relationships among business and management processes and IT. An enterprise architecture describes the "target" situation that the agency wishes to create and maintain by managing its IT portfolio.

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.

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 morale, welfare, and recreation (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 nonappropriated fund 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 an Intranet, an extranet includes outside vendors and uses Web technology to facilitate interbusiness transactions, such as placing and checking orders, tracking merchandise, and making payments.

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.

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).

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 JCS 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 communities of interest.

Information management
Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

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 system
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of 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. (Ref. Clinger–Cohen Act of 1996.)

Infostructure
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 Clinger–Cohen Act of 1996.

Infrastructure
The term is used with different contextual meanings. It most generally relates to and has a hardware orientation, but it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

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)
A 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 World Wide Web 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.

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, based on the recommendation of the Central Technical Support Facility (CTSF) Director, 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.

A private Internet operating on an organization's internal network; an information utility that makes organizational and departmental information accessible via the standards of the Internet: e-mail (SMTP), WWW, file transfer protocol, and other Internet services.

IT Architecture
An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic and information resources management goals.

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 IT management 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.

Joint Technical Architecture-Army (JTA–A)
The complete set of rules derived from the JTA that prescribe the technical standards for Army IT systems and enable interoperability among joint systems.

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)
An 8-year package of dollars and manpower to support a given program or function. The BIP is the first 3 budget and execution years of the MDEP, and the PDIP is the 5 program years following.

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 enterprise-wide 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)
Record 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 critical (MC) 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 war fighter operations or direct mission support of war fighter operations.

Mission Essential (ME) 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 MACOM 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.

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 command and control 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 Clinger–Cohen Act of 1996).

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 appropriated funds (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 Freedom of Information Act exemption, or sensitive.

Objectives
Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.

Operational Architecture
Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.

Operational View (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 National Archives and Records Administration 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.

Photojournalism
Conveying a story, through still photography, of a significant DOD event, normally to support the news media or internal DOD publications.

Planning, Programming, Budgeting, and Execution (PPBE) process
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Printing
The processes of composition, platemaking, presswork, and binding, including micropublishing, for the production of publications.

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, MACOMs, 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 material 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 World Wide Web
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 Department of the Army 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.

a. Federal records centers: records centers operated by the National Archives and Records Administration.

b. Army records centers: Army-maintained records centers for intelligence, criminal investigation, and similar records.

Records management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with information creation, information maintenance and use, and information disposition in order to achieve adequate and proper documentation of the policies, transactions, and effective and economical management of DA operations.

Records management program
A program that includes elements concerned with the life-cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information Act and the Privacy Act.

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 satellite communication space systems that use Government frequency bands, and commercial satellite communication systems provided by commercial entities using commercial frequency bands. SATCOM is further defined to include DOD's use of other allied and civilian satellite communications resources as appropriate (See CJCSI 6250.01). SATCOM includes Defense Satellite Communications System (DSCS), DOD Teleport integration of C, Ku, Ka, UHF, EHF, advanced EHF and Mobile User Objective System (MUOS), MILSTAR, Teleport, Wideband Gapfiller System (WGS), and Defense Information Infrastructure.

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 COMINT 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" mail.

Standard
Within the context of the Army Enterprise Architecture, 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 nonappropriated fund activity that procures services made available pursuant to the terms of the franchise agreement.

Support agreement
An agreement to provide recurring BASOPS support to another DOD or non-DOD federal activity.

Synchronization
Coordinating and aligning the development of the Army Enterprise Architectures in both timing and direction for mutual reinforcement and support.

System
An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JCS 1–02). Within the context of the Army Enterprise Architecture, 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).

Synchronization
See data synchronization.

Systems Architect
Responsible for integration and oversight of all Army information systems.

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
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 control (TECHCON)
The authority for one organization or command to issue and enforce policy and authoritative direction concerning the use of techniques, procedures, standards, configurations, designs, devices, and systems to another specified organization to accomplish a specific mission. It does not include command authority or administrative control for logistics or matters of administration, discipline, internal organization, or unit training. NETCOM will exercise TECHCON over all organizations that operate and maintain portions of the AEI.

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.

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.

URL (uniform resource locator)
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
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 of 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 visual information (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. VIDOC encompasses combat documentation (COMDOC), operational documentation (OPDOC), and technical documentation (TECDOC).

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 a NETCOM/9th ASC region, FOA, or other management level established to prescribe and require compliance with 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
VI documentation 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.

VI Support Center (VISC)
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.

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 222

PIN:	058039–000
DATE:	07-14-05
TIME:	06:40:13
PAGES SET:	126
DATA FILE:	C:\wincomp\r25-1.fil
DOCUMENT:	AR 25–1
SECURITY:	UNCLASSIFIED
DOC STATUS:	REVISION