AR 25-1
cy. 1

Army Regulation 25–1

Superseded
by
AR 25-1
30 June 2004

Information Management

Army Information Management

Headquarters
Department of the Army
Washington, DC
31 May 2002

UNCLASSIFIED

SUMMARY of CHANGE

AR 25-1
Army Information Management

The revision dated 31 May 2002--

- Includes new policy on Army knowledge management, Army Knowledge Online, e-mail, Web site management, the use of Public Key Infrastructure/Common Access Card (PKI/CAC) for electronic information transmissions, and bandwidth conservation. Operational security for Web sites is included in the regulation's management control checklist.

- On the title page, supersedes the history paragraph and supersession statement.

- After paragraph 1-6, adds a new paragraph 1-7 on Army knowledge management and renumbers paragraphs 1-7, 1-8, and 1-9 as 1-8, 1-9, and 1-10.

- Supersedes paragraph 6-3q.

- Supersedes paragraph 6-3r.

- Supersedes paragraph 6-4f.

- Supersedes paragraph 9-2 introductory text.

- Supersedes paragraph 9-2b.

- In appendix A, section I, adds AR 360-1, Allied Communication Publication (ACP) 123, section 508 of the Rehabilitation Act (29 U.S.C. 794d). Updates changed publication titles throughout appendix A.

- Adds to appendix B, paragraphs B-4d(21) through B-4d(29).

- In the glossary, section I, adds AKM, AKO, GILS, LDAP, OPSEC, PKI, PMO, SSL, and URL.

- In the glossary, section II, adds the terms access control mechanism, authentication, bandwidth, cookie, digital signature, electronic signature, Extranet, infostructure, Intranet, persistent cookies, smart card, third party cookies, URL, Web portals, and Web site.

- The revision dated 15 February 2000--

- Replaces the title 'The Army Information Resources Management Program' with the title 'Army Information Management.'

- Rescinds DD Forms 2054/1 and 2054/2.

- Implements General Orders 23, Transfer of Publications and Printing, 12 June 1997; and General Orders 24, Transfer of Records Management, 12 June 1997.

- Prescribes requirements control symbol (RCS) CSIM-59.

- Omits library policy.

- Eliminates the concepts of the Information Mission Area (IMA) and IMA disciplines. The terms information management and information technology are used instead (chaps 1 through 3).

- Transfers proponency of records management from the DISC4 to the DCSPER. Designates the HQDA DCSPER as the archivist of the Army and the U.S. Army Records Management and Declassification Agency as the operational agency. Assigns oversight responsibility of the records management function to the DISC4, as CIO (chaps 2 and 8).

- Transfers proponency of printing and publishing from the DISC4 to the Administrative Assistant. Updates guidance on electronic publishing support and staffing. Assigns oversight responsibility of the publishing function to the DISC4, as CIO (chaps 2 and 9).

- Implements the Clinger-Cohen Act.

- Defines Chief Information Officer responsibilities. Provides new guidance on strategic planning, business process analysis and improvement, IT capital planning and investment strategy, IT performance measurements, CIO involvement in the PPBES process, CIO assessments, and CIO validation of requirements. Replaces the Major Automated Information System Review Council with the Information Technology Overarching Integrated Process Team (IT OIPT) (chap 3.)

- Prescribes new policy on the Army Enterprise Architecture (AEA) as a corporate framework, the use of associated AEA documents, and the responsibilities for completing the AEA products. Identifies the relationship between the AEA and Defense-level architecture documents and products (chap 4).

- Provides new policy on information assurance (IA), its components, and the management structure of IA (chap 5).

- Prescribes new policies for management and use of technologies such as e-mail, internet, World Wide Web, electronic business/electronic commerce, cellular telephones, satellite telecommunications, and others. Updated and new policies also include IT support for telecommuting, information access to handicapped employees, installation-level processing services, network management, site licenses, leasing of IT assets, IT materiel fielding coordination, post-production software support, use of computer programming languages, excess IT inventory reporting, software copyright protection, interservice and service-level agreements, Defense Messaging System. Prescribes new management control guidelines for use of e-mail, cellular telephones and other telecommunications systems and devices (chap 6).

- Provides new policy on combat camera and the use of the Training Support Automated Management Software - Enhanced (TSAMS-E) (chap 7).

- Updates the Management Control Evaluation Checklists (app B).

- Removes the local reproducible forms from the back of the manuscript and makes them available by electronic media only.

Headquarters
Department of the Army
Washington, DC
31 May 2002

*Army Regulation 25–1

Effective 28 June 2002

Information Management

Army Information Management

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

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

History. This printing publishes a revision of this publication. Changed parts have been listed in the summary of change.

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, and the resources supporting information technology. The regulation implements the Public Law 104-106, Clinger-Cohen Act of 1996 (formerly Division E, Information Technology Management Reform Act, Defense Authorization Act for 1996), and establishes the DISC4 as the Army's Chief Information Officer (CIO). The full scope of CIO 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 (ARNG), and the U.S. Army Reserve (USAR). This publication is in effect during mobilization.

Proponent and exception authority. The proponent of this regulation is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponents may delegate the approval authority, in writing, to a chief under their supervision within the proponent agency who holds the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions in accordance with AR 11-2 and contains checklists for conducting management control reviews at appendix B.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (SAIS-IMC), WASH DC 20310-0107.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA FORM 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (SAIS-IMC), WASH 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, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Recordkeeping requirements • 1–4, *page 1*
Managing information resources and information technology • 1–5, *page 1*
Information as a resource • 1–6, *page 1*
Army knowledge management • 1–7, *page 2*
Information transmission economy • 1–8, *page 2*
Use of IT to improve mission efficiency and effectiveness • 1–9, *page 2*

*This regulation supersedes AR 25-1, dated 15 February 2000.

UNCLASSIFIED

Contents—Continued

User/customer focus and the relationship between the customer and the IT community • 1–10, *page 2*

Chapter 2
Responsibilities, *page 2*
The Director of Information Systems for Command, Control, Communications and Computers (DISC4) • 2–1, *page 2*
Principal HQDA officials • 2–2, *page 5*
The Army Acquisition Executive (AAE) • 2–3, *page 5*
ASA (Financial Management and Comptroller (ASA FM&C) • 2–4, *page 5*
The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT)) • 2–5, *page 6*
The Office of General Counsel (OGC) • 2–6, *page 6*
The Administrative Assistant to the Secretary of the Army (AASA) • 2–7, *page 6*
The Deputy Undersecretary of the Army (International Affairs) (DUSA-IA) • 2–8, *page 7*
The Chief of Public Affairs (CPA) • 2–9, *page 7*
The Director of the Army Staff (DAS) • 2–10, *page 7*
The Deputy Chief of Staff for Intelligence (DCSINT) • 2–11, *page 7*
The Deputy Chief of Staff for Operations and Plans (DCSOPS) • 2–12, *page 7*
The Deputy Chief of Staff for Personnel (DCSPER) • 2–13, *page 8*
Assistant Chief of Staff for Installation Management (ACSIM) • 2–14, *page 8*
The Judge Advocate General (TJAG) • 2–15, *page 8*
MACOM Commanders • 2–16, *page 8*
Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC) • 2–17, *page 9*
Commanding General, U.S. Army Materiel Command (CG, AMC) • 2–18, *page 10*
The Commanding General, U.S. Army Forces Command (CG, FORSCOM) • 2–19, *page 10*
Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM) • 2–20, *page 12*
The Army Surgeon General/Commanding General, U.S. Army Medical Command (CG, MEDCOM) • 2–21, *page 12*
Commanding General, United States Army Corps of Engineers (CG, USACE) • 2–22, *page 12*
Commanders of the Army Components of unified and sub-unified commands • 2–23, *page 12*
U.S. Army Reserve Command and the U.S. Army National Guard • 2–24, *page 13*
Commanders or directors of major subordinate commands (MSC), FOA, separately authorized activities, tenant, and satellite organizations • 2–25, *page 13*
Installation, State Area Command (STARC), or comparable level community commanders • 2–26, *page 13*
Commanders of Army Reserve Support Commands (RSC) • 2–27, *page 13*
Program, Project, and Product Managers (PMs), 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*
Designation of CIO • 3–2, *page 14*
IM/IT resource management • 3–3, *page 14*
Process analysis and business/functional process improvement • 3–4, *page 15*
CIO validation of requirements • 3–5, *page 16*
IT performance measurements • 3–6, *page 17*
Army acquisition and CIO assessment • 3–7, *page 18*
IM/IT personnel proponency • 3–8, *page 18*
Information management organizations below Headquarters, Department of Army • 3–9, *page 18*

Chapter 4
The Army Enterprise Architecture, *page 19*
Introduction • 4–1, *page 19*
General guidance for development and use of the AEA • 4–2, *page 19*
Operational architecture (OA) • 4–3, *page 20*
Technical architecture (TA) • 4–4, *page 20*
Systems architecture • 4–5, *page 20*

Contents—Continued

The Army Data Management and Standards Program (ADMSP) • 4–6, *page 20*
Installation Information Infrastructure Architecture (I3A) • 4–7, *page 21*

Chapter 5
Information Assurance, *page 21*
Mission • 5–1, *page 21*
Management structure for information assurance • 5–2, *page 22*
Information system certification/accreditation • 5–3, *page 22*
Physical security • 5–4, *page 22*
Software security • 5–5, *page 22*
Hardware security • 5–6, *page 23*
Procedural security • 5–7, *page 23*
Personnel security • 5–8, *page 23*
Communications security • 5–9, *page 23*
Risk management • 5–10, *page 23*

Chapter 6
Command, Control, Communications, and Computers/Information Technology (C4/IT) Support and Services, *page 24*
Management concept • 6–1, *page 24*
Automation • 6–2, *page 27*
Telecommunications • 6–3, *page 30*
Long-haul and deployable communications • 6–4, *page 43*
IT support for battlefield systems • 6–5, *page 46*
IT support for military construction (MILCON) • 6–6, *page 46*

Chapter 7
Visual Information, *page 46*
General • 7–1, *page 46*
Combat camera (COMCAM) • 7–2, *page 47*
VI executive agent responsibilities • 7–3, *page 48*
VI activities • 7–4, *page 48*
VI activity operations • 7–5, *page 49*
Automated information management system • 7–6, *page 49*
Equipment and systems • 7–7, *page 49*
Products • 7–8, *page 50*
Services • 7–9, *page 54*
VI records management • 7–10, *page 54*
VI Documentation (VIDOC) Program • 7–11, *page 55*
Restrictions • 7–12, *page 56*

Chapter 8
Records Management Policy, *page 58*
Mission • 8–1, *page 58*
Management concept • 8–2, *page 58*
Life cycle management of records • 8–3, *page 59*
Tenets • 8–4, *page 60*
Major subprograms • 8–5, *page 60*
General policies • 8–6, *page 62*
Record media • 8–7, *page 63*
Electronic records management • 8–8, *page 64*

Chapter 9
Publications and Printing, *page 64*
Management concept • 9–1, *page 64*

Contents—Continued

Central configuration management • 9–2, *page 65*
Statutory restrictions for publications • 9–3, *page 65*
Statutory requirements for printing • 9–4, *page 65*
Requisitioning printing • 9–5, *page 66*

Appendixes

A. References, *page 67*

B. Management Control Evaluation Checklist, *page 73*

Table List

Table 7–1: Types of VI Activities, *page 48*

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 applies to information technology contained in command and control systems, intelligence systems, business systems and national security systems developed or purchased by the Department of Army. It implements the provisions of Public Law 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), DOD Instruction (DODI) 7740.3 and other related DOD directives. It addresses the management of information as an Army resource, the technology supporting information requirements, and the resources supporting Command, Control, Communications, and Computers (C4)/information technology (IT).

1–2. References

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

1–3. Explanation of abbreviations and terms

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

1–4. 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 in AR 25-400-2.

1–5. Managing information resources and information technology

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 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 systems 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.

1–6. Information as a resource

a. Information is a valuable resource that must be managed as any other asset, such as funds, personnel and equipment. The cost to the Army of collecting, processing, distributing and storing information makes it impossible to view information as a free commodity. Except where restricted for reasons of national security, privacy, sensitivity, or proprietary rights, information will be managed as a shared resource which will be made available to all those needing it to accomplish their mission and functions. Requirements for information and the supporting technology will be carefully planned. This supporting IT and related investments will be evaluated in terms of their support of Army 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 380-19. It is either routinely made available to the public or provided upon public request with or without charge. It may be freely shared among Army users without restriction. Non-public data or information is both personally identifiable and subject to the Privacy Act, or classified according to the National Security Act, subject to a FOIA exemption, or sensitive. Unclassified FOIA exempt information or data is non-public 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. Refer to AR 25-55 for further information on the Army FOIA Program and to AR 340-21 on the Army Privacy Program.

c. The responsible functional proponents will maintain Army data and ensure that it is readily accessible to whomever requires it. This practice promotes economic 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.

d. Information will be managed through centralized control and decentralized execution. Approved DOD-wide methods, approaches, models, tools, data, IT and information services will be used.

1–7. Army knowledge management

Army knowledge management (AKM) is the Army's strategy to transform itself into a network-centric, knowledge-based force and is an integral part of the Army's transformation to achieve its objective 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. The goals are—

- Adopt governance and cultural changes to become a knowledge-based organization.
- Integrate knowledge management and best business practices into Army processes.
- Manage the infostructure at the enterprise level.
- Scale Army Knowledge Online as the enterprise portal.
- Harness human capital for the knowledge organization.

1–8. Information transmission economy

Originators of record communications will use the most operationally and cost-effective means of transmission. This determination is made from an analysis of the perishability, classification, urgency, and transmission means available.

1–9. Use of IT to improve mission efficiency and effectiveness

a. IT provides capabilities that can 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 IT. When appropriate and cost-effective, IT will be used to support Army processes.

b. Information in 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. Integration of information systems throughout the organization generally reaps dividends in the form of increased efficiency resulting from better coordination among functional areas and the availability of consistent information.

1–10. 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. These capabilities and services are not an end 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 its support role, the IT community must maintain a constant focus on the needs of its users and customers.

b. This focus should include awareness of the current requirements for support, the quantity and quality of support provided, future customer requirements, and emerging IT capabilities which can benefit the customer. The Army's increasing employment of IT dictates a robust relationship between the IT community and users, in which both the user and the service provider take responsibility for communicating with each other. Each organization's IT management process must foster this 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. Customers must be sensitive to the IT community's need to be involved in seemingly unrelated management issues because of potential IT impacts. 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. Service and accountability to the customer will be incorporated in the analysis to outsource or consolidate and will be included in agreements and contracts for IT support capabilities.

Chapter 2
Responsibilities

2–1. The Director of Information Systems for Command, Control, Communications and Computers (DISC4)

The DISC4 will-

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

b. Provide functional policy and guidance on C4/IT systems (to include Internet and Web site management).

c. Serve as Chief Information Officer (CIO) for the Army. The responsibilities are:

(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; freedom of information; 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 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 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 and Defense Chief Information Officers Councils.

(10) Manage the Army segment of the Office of the Secretary of Defense-mandated information assurance program.

(11) Provide oversight for National Security Systems (NSS), i.e., all systems which have IT/C4I requirements and include such functions as requirements review, prioritization, resource management, and acquisition.

d. Implement the policy and procedures mandated by:

(1) 44 U.S. Code, chapter 35, Coordination of Federal Information Policy (P.L. 104-13 (Paperwork Reduction Act of 1995)).

(2) 47 U.S. Code §§ 151, 157, 158, 201, 203, 552, 553, 571-73 (P.L. 104-104 (Telecommunication Act of 1996)).

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

(4) 40 U.S. Code § 759 (P.L. 100-235 (Computer Security Act of 1987))

(5) Executive Order 13011, Federal Information Technology.

(6) Executive Order 13103, Computer Software Piracy.

e. Provide oversight and direction for implementation of the policies and procedures in:

(1) 44 U.S. Code, chapter 31, Records Management by Agencies

(2) 44 U.S. Code § 211, chapters 29, 31, and 33 (P.L. 94-575, Federal Records Management).

(3) P.L. 97-375 (Congressional Reports Elimination Act of 1982).

(4) 44 U.S. Code § 3502 (Public Printing and Documents).

(5) 5 U.S. Code § 552 (Freedom of Information Act).

(6) 5 U.S.Code § 552a (Privacy Act of 1974).

(7) P.L. 96-470 (Congressional Reports Elimination Act of 1980).

(8) P.L. 97-375 (Congressional Reports Elimination Act of 1982).

(9) Executive Order 12600, Pre-disclosure Notification Procedures for Confidential Commercial Information.

f. Support the Army Acquisition Executive (AAE) for the acquisition of information systems (IS) and on aspects of other major systems to include:

(1) Serve as the military deputy for C4/IT to the AAE.

(2) Serve as Chairman of the Army IT Overarching Integrated Product Team (OIPT).

(3) Serve as member of the Office of the Secretary Defense (OSD) IT OIPT or similar committee.

(4) Serve as member of the Army Systems Acquisition Review Council (ASARC) or similar committee.

(5) Work Army Acquisition Corps (AAC) IT issues through the Acquisition Career Management Office..

(6) Serve as member of Test Schedule and Review Committee (TSARC).

(7) Serve as chairman of C4 ASARC program Integrated Product Team (IPT).

g. Assist the Assistant Secretary of the Army (ASA) for Acquisition, Logistics and Technology (ALT) and the AAE in the day-to-day interface with Program Executive Officers (PEO) and Program Managers (PM) for those systems that pertain to IT.

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

(2) Act as the Army Software Executive official and serve as the Army focal point for all software acquisition activities.

h. In the assigned role of Army Enterprise Architect (AEA):

(1) Integrate Army-wide architectures per the AEA Guidance Document (AEAGD). Review Operational Architectures (OAs), Systems Architectures (SAs), and Technical Architectures (TAs) developed by major commands (MACOMs), PEOs, developers and HQDA staff proponents.

(2) Serve as the Army Systems Architect (SA) to integrate, maintain, and control the Army Systems Architecture.

(3) Develop and maintain the AEA Framework Document (AEAFD).

(4) Develop and maintain the AEAGD.

(5) Develop and maintain the AEA Master Plan (AEAMP).

(6) Assist the AAE, as assigned, in the development and enforcement of the Joint Technical Architecture-Army (JTA-A).

(7) Lead and manage the Army Data Management and Standards Program (ADMSP) and serve as the Army Component Data Administrator (CDAd) under the DOD Data Administration Program. (See also paragraph 4-6).

i. Serve as senior policy official for the Army Electronic Business/Electronic Commerce Program and associated electronic business/electronic commerce activities, initiatives, and solutions.

j. Manage and execute the Army Electronic Business/Electronic Commerce Program, including review, approval, and general oversight of electronic business/electronic commerce activities, initiatives, and solutions.

k. Serve as senior authority for telecommunications programs, to include the following:

(1) Joint Chiefs of Staff (JCS)-controlled mobile/transportable telecommunications assets.

(2) Allied communications publications (ACP) and Joint Army-Navy-Air Force Publications (JANAP).

(3) The Spectrum Certification Program.

(4) Compatibility and interoperability of tactical Command, Control, Communications (C3) and Intelligence (C3I) systems.

(5) Test and evaluation for the Joint Tactical Communications Program.

(6) Oversight for the executive agents for Tactical Switched Systems and Joint Network Management.

(7) Voting member of the Military Communications-Electronics Board (MCEB) and participate in MCEB activities. Refer military communications-electronics matters to the MCEB for decision.

(8) Member of the National Security Telecommunications and Information Systems Committee.

l. Serve as senior authority for Army visual information (VI) and manage non-tactical VI and multimedia products per OMB Cir A-130, DODD 5040.2, DODI 5040.4, DODI 5040.5, OMB Cir A-76, and 36 Code of Federal Regulation (CFR). These programs include:

(1) Department of Army Visual Information (VI) Production and Distribution Program (DAVIPDP).

(2) VI Systems Program (VISP).

(3) VI Documentation Program (VIDOC).

(4) VI Authorization Program.

(5) Representation to the Defense Visual Information Steering Committee (DVISC).

(6) Chair the Army Visual Information Steering Committee (AVISC).

(7) Serve as functional proponent representative for commercial activities General Functional Code (GFC) T807 (Visual Information).

(8) Provide oversight of the Army Joint Visual Information Service (JVIS) functions.

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

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

(2) Serve as Chief Signal Corps Officer of the Army.

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

n. As the HQDA staff agency 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; receives, coordinates, and integrates these issues; and ensures 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 System (PPBES) decision groups.

(3) Promulgate C4/IT system policy; ensures program conformance to the approved JTA-A, OA, and SA; coordinates and supports the priorities within C4/IT for information system development related activities; and secures adequate resource support.

(4) Operate the Strategic and Advanced Computing Center to promote the application of proven artificial intelligence (AI) techniques, procedures and methodologies across the Army's corporate management processes and their associated information systems.

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

(6) Coordinate resource requirements for C4/IT support activities within HQDA on behalf of the Training and Doctrine Command (TRADOC), the Army Materiel Command (AMC), other MACOMs and Army components, and the field operating agencies (FOA) of HQDA, and appropriate PEOs and PMs.

(7) Prepare and coordinate OA data with TRADOC as input to Army-wide OA for warfighting requirements.

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

(9) Ensure interoperability among command and control systems and coordinate Army survival, recovery and reconstitution system and Continuity of Operations Plans (COOP) support requirements. Ensure that essential information services in support of DA COOP are available to alternates of HQDA agencies and MACOMs, major subordinate commands and installations.

(10) Serve as the Director, Defense Metropolitan Area Telephone System (DMATS), responsible for the management, operation, and support of assigned DMATS.

(11) Direct, monitor, plan and program for the Army spectrum management program.

(12) As member of the C2 Protect Triad made up of DISC4, DCSINT, and DCSOPS, manage the Army Information Assurance Program.

(13) In conjunction with the ODCSPER, ensure that records management requirements are included in the life cycle of information systems beginning at milestone 0.

o. Provide consultation and advice to the Administrative Assistant of the Secretary of the Army in the operation of the Defense Telecommunications Service-Washington.

2–2. Principal HQDA officials

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

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

(1) As required, participate in the Army IT OIPT and Army Systems Acquisition Review Council (ASARC) processes.

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

(3) Participate collectively with other Army C4I/IT stakeholders in the CIO capital planning and investment strategy process. (Refer to Section 3-3.)

(4) 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 PPBES process.

(5) Develop AEA architectures (OA, TA, and SA) respective to their functional areas and act as the integrator for systems of systems under their purview and coordinate with DISC4 per the AEAGD.

(6) Develop and coordinate OA data with TRADOC as input to Army-wide OA.

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

c. Ensure outsourcing is considered for all non-core/priority mission functions. See paragraph 3-4a. for more details.

d. Appoint in writing a records manager to manage the internal records of the organization and act as a point of contact for recordkeeping requirements of the respective functional area. Provide a copy of the appointment to the U.S. Army Records Management and Declassification Agency. (See address at paragraph 8-5b(1)(d)).

2–3. The Army Acquisition Executive (AAE)

General acquisition responsibilities for the AAE are defined in AR 70-1. Those responsibilities unique to C4/IT are listed below:

a. Review and approve, for Acquisition Category (ACAT) ID and ACAT IAM programs, the Army position at each decision milestone before the Defense Acquisition Board (DAB) or DOD IT OIPT review. This includes the review and approval of Acquisition Program Baselines (APB). (See DODD 5000.1 for further clarification on ACAT programs.)

b. Serve as the Milestone Decision Authority (MDA) for Army ACAT IC and ACAT II programs.

c. As the Army Technical Architect:

(1) Develop and approve the JTA-A.

(2) Act on requests for waivers to the application of the JTA-A.

(3) Act as final decision authority to resolve conflicts among TA profiles.

d. Approve and assign software reuse domains and domain management responsibility based on recommendations from the DISC4.

e. Provide acquisition life cycle and funding support to the Army Software Reuse program and ensure that software reuse is included in the acquisition strategy.

2–4. ASA (Financial Management and Comptroller (ASA FM&C)

In addition to duties listed in 2-2 above, the ASA (FM & C) is responsible for gathering and reporting IT data required in the program objective memorandum (POM) and the Exhibit 43 (Information Technology Systems Budget).

2–5. The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT))

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

a. Serve as the Source Selection Authority or delegate Source Selection Authority for acquisition of all IT.

b. Direct and review communications, command, control, and intelligence systems, target acquisition systems, and tactical IT requiring significant 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 selected tactical information systems required for strategic and tactical purposes.

d. Coordinate the C4/IT modified integrated program summaries.

e. Formulate and execute the RDT&E and procurement portions of C4/IT programs and budgets.

f. Manage the C4/IT technology base.

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

2–6. The Office of General Counsel (OGC)

The OGC will, in addition to duties listed in 2-2 above, notify the Deputy Chief of Staff for Personnel when certain records are required for litigation and may not be destroyed.

2–7. The Administrative Assistant to the Secretary of the Army (AASA)

The AASA will, in addition to duties listed in 2-2 above:

a. Implement the Army Publishing and Printing Program (APPP) to include:

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

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

(3) Serve as HQDA point of contact on policy issues with the chairman of the Joint Committee on Printing (JCP), the Public Printer, GPO, the Director of Bureau of Engraving and Printing, and the Administrator of General Services Administration (GSA).

b. Serve as the authenticating official for all Departmental publications except policy publications which are authenticated by the Secretary of the Army.

c. Operate and maintain the U.S. Army Visual Information Center (USAVIC) as a Joint VI service in support of OSD, JCS, Army activities, other Defense components, and Federal agencies, as required, with USAVIC managing VI for the internal use of the HQDA as a MACOM.

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

(2) Provide a central visual information office for the execution of DISC4 VI programs and functions:

(a) DA VI Production, Multimedia and Distribution Program (DAVIPDP).

(b) Recommend changes to VI activity authorization documents per table 7-1.

(c) Manage the Army portion of the Defense Automated VI System (DAVIS).

(d) Recommend validation to ODISC4 of requirements for VI equipment and systems VI Systems Program (VISP) projects.

(e) Provide alternate representation to DOD VI workgroups.

(3) Act as a Component Accessioning Point (CAP) for the accessioning ofArmy VI record material into Defense VI Center (DVIC).

(4) Serve as sole Army organization authorized to execute the Joint VI service mission of contracting for productions in their entirety for the Army, Defense agencies and other components and Federal agencies, as required.

(5) Provide data entry support of T-ASA contract commitments and obligations into DOD finance database.

d. Manage IT for the internal use of HQDA. The AASA is assisted in the execution of the information management (IM) function by the HQDA Information Manager (HQIM). The HQIM performs the role of the Deputy Chief of Staff for Information Management (DCSIM) for HQDA as a MACOM. The AASA will also:

(1) Ensure that HQDA staff elements accomplish their assigned internal HQDA 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.

(4) Provide policy, guidance and direction for implementation of internal HQDA IM.

(5) Ensure operational information support and the supporting Director of Information Management (DOIM) provides services to HQDA.

(6) Provide a HQDA evaluation to the DISC4 of the Army IM/IT strategic plan.

(7) Serve as the Information Management Officer (IMO) for the Office of the Secretary of the Army (OSA); Office of the Chief of Staff of the Army (OCSA), and supported activities.

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

2–8. The Deputy Undersecretary of the Army (International Affairs) (DUSA-IA)

Serves as the principal focal point for the Army concerning Multinational Force Compatibility (MFC), to include C4/IT issues. MFC is the ability of the Army and its forces to operate effectively as a member of a multinational coalition or alliance across the full spectrum of military missions and to support the ability of the Regional Commanders in Chief to employ U.S. forces as part of a multinational coalition or alliance. The DUSA (IA) will, in addition to duties listed in 2-2 above:

a. Promulgate general MFC policy guidance for all MFC forums, including those that address C4/IT issues (NATO Army Armaments Group Land Groups, NATO Military Agency for Standardization Working Parties, American-British-Canadian-Australian Quadripartite Working Groups, and Senior National Representative (Army) forums, and others).

b. Oversee Army participation in MFC forums, including those that address C4/IT interoperability issues.

c. Coordinate HQDA approval of the positions proposed by Army Heads of Delegation to major MFC forums.

d. Coordinate Army policy related actions on the proposal, ratification, implementation, and evaluation of all MFC agreements involving the Army.

2–9. The Chief of Public Affairs (CPA)

The CPA will, in addition to duties listed in 2-2 above, provide general staff supervision and approval for the release of Army VI products to the public.

2–10. The Director of the Army Staff (DAS)

The DAS will accomplish all the responsibilities assigned to the principal HQDA officials for the Office of the Chief of Staff of the Army (OCSA) (see 2-2).

2–11. The Deputy Chief of Staff for Intelligence (DCSINT)

The DCSINT will, in addition to duties listed in 2-2 above:

a. Provide policy to the DISC4 for the IM activities of the intelligence community and advise the DISC4 accordingly.

b. Represent for the CIO the National Foreign Intelligence Program (NFIP)-funded IT/C4I efforts under the Defense Agency NFIP Program Manager's CIO programs. Any IT/C4I NFIP 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 ISS efforts.

d. Provide functional oversight and management for Army-managed DOD Intelligence IT purchases, systems and leases (other than single source logistic support management).

e. Serve as staff proponent for a Sensitive Compartmented Information (SCI) Information Assurance (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.

2–12. The Deputy Chief of Staff for Operations and Plans (DCSOPS)

The DCSOPS will, in addition to duties listed in 2-2 above-

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 requirement 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 requirements.

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

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

i. Validate and resource Army DAVIPDP and multimedia production, replication, and distribution requirements. Validation responsibility may be delegated.

2–13. The Deputy Chief of Staff for Personnel (DCSPER)

The DCSPER, in addition to the responsibilities in 2-2, also serves as Archivist of the Army and senior policy official for the Army Records Management Program. As Archivist of the Army:

a. Develops and maintains the Army Information Collection required by Title 44, United States Code, and chapter 8.

b. Establishes policy to identify DA permanent records and ensure their transfer to the National Archives.

c. Advises the Secretary of the Army concerning the destruction of records in his legal custody in an Army repository outside the continental US (OCONUS) during a state of war between the U.S. and another nation or when hostile action (by a foreign power, terrorist agents or public demonstrators) seems imminent.

d. Administers the Army Management of Information Requirements Program.

e. Establishes Army-wide policy and procedures for managing manual and electronic records to include:

(1) Developing records retention schedules for Army manual and electronic records.

(2) Developing provisions for a clearing-house for the sharing of electronic record-keeping information among all appropriate Army offices.

(3) Developing standardized procedures for the external and internal identification of the contents of electronic records.

f. Executes the official mail and distribution management program for the Army.

g. Coordinates DOD-wide mail distribution issues with the Military Postal Service Agency.

h. Executes the Correspondence Management Program for the Army.

i. Executes the Privacy Act Systems Notices Program for the Army.

j. Executes the Freedom of Information Act Program.

k. Executes the Vital Records Program for the Army.

l. Executes the Modern Army Record Keeping System (MARKS).

m. Executes the periodic Army evaluations of the records management program.

n. Manages the Army-wide Record Collections from selected Army operations.

2–14. Assistant Chief of Staff for Installation Management (ACSIM)

The ACSIM will, in addition to duties listed in 2-2 above-

a. Exercise HQDA proponency for the IM architecture of Real Property Management Activities

b. Provide HQDA oversight of the IM activities of Real Property Management Activities.

c. Provide HQDA oversight of the U.S. Army Community and Family Support Center (USACFSC), which serves as the proponent and focal point for matters concerning Army Morale, Welfare, and Recreation (MWR) information technology systems.

2–15. The Judge Advocate General (TJAG)

TJAG will, in addition to duties listed in 2-2 above-

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 (e.g., DCSIM, CIO, or equivalent) who has the sole responsibility to implement the command's IM/IT program. MACOM DCSIMs will directly supervise the information management staff activities and related programs and activities.

b. Develop and maintain internal headquarters and MACOM-wide IM/IT procedures to provide required guidance and direction to subordinate organizations.

c. Identify the MACOM IM/IT requirements. Ensure that these requirements are validated, coordinated, and integrated per AR 71-9.

d. Manage the MACOM information management requirements throughout their life cycle, including those which are for MACOM organizations that are tenants on other MACOM installations. See paragraph 3-5(a) for more detail.

e. Take appropriate action to obtain resources to support information requirements through the PPBES process.

f. Coordinate IT plans, programs and requirements with appropriate information systems security managers (ISSM) per AR 380-19.

g. Assess all assigned programs prior to their Milestone Reviews, and based on the MACOM CIO assessments, recommend programs to be continued, modified, or terminated, as part of the Milestone Reviews for milestones I, II, and III.

h. Develop and maintain the MACOM IT architecture.

i. Develop appropriate procedures to ensure compliance with applicable software copyright laws and license agreements.

j. Develop AEA architectures (OA, TA and SA) for respective command functions and act as the integrator for systems of systems under their purview. Coordinate with DISC4 as required by the AEAGD.

k. Assist DISC4 in ensuring JTA-A compliance for designated systems.

l. Implement the Army data management and standards program as guided by the Army Component Data Administrator (CDAd).

m. Maintain current systems architecture for assigned installations.

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

o. Ensure that all non-core/priority mission functions are accomplished effectively, efficiently and at the lowest cost. See paragraph 3-4a for more detail.

p. Appoint a command records administrator. This individual is responsible for overseeing the Records Management Program throughout the command.

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

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

s. Designate a MACOM VI manager. Staff proponency and placement is at the commander's preference. If VI is not managed by the senior information management official, the VI manager will ensure coordination with the former for planning requirements and compliance with Federal, DOD, and Army VI policy; prepare directives implementing VI policy and procedures; and provide management direction to VI activities, including annual on-site visits. Each MACOM VI Manager will-

(1) Develop a 6-year VI Systems Acquisition Plan and submit the investment portion of the plan and annual updates to ODISC4 (VI) for Program Objective Memorandum (POM) development.

(2) Validate, consolidate, and submit VI investment system requirements for the Visual Information Systems Program (VISP), RCS CSGPO-344.

(3) Approve and/or validate VI production multimedia requirements, maintain production registers, and submit requirements for the annual Department of the Army Visual Information Production and Distribution Program (DAVIPDP), (RCS DD-PA (AR) 1381).

(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 (RCS-CSIM-59).

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

(7) Serve as the MACOM representative to the Army VI Steering Committee.

(8) Manage VI non-tactical documentation quarterly submissions to the VIDOC program.

(9) Ensure life cycle management of multimedia products.

t. Implement policy for integrated logistics support of IM systems/equipment during its life cycle.

u. Implement DA policy regarding property accountability of IT.

v. Appoint and assign a frequency manager.

w. Identify information systems and communication systems functional requirements for all Army Military Construction (MILCON) projects, to include VI systems.

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

y. Administer the MACOM-level IT component of the Army IT Metrics Program.

2–17. Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC)

The CG, TRADOC will, in addition to duties listed in 2-16 above-

a. Formulate IM/IT doctrine for the Army.

b. As Army Operational Architect, will-

(1) Develop, approve and integrate the OA for all Army requirements.

(2) Coordinate with DISC4 per the AEAGD.

c. In coordination with the DISC4 and materiel developers, identify and analyze IM/IT training requirements and, when appropriate, update existing courseware.

d. Conduct warfighting experiments; participate in warfighting experiments conducted by others to support the development of requirements for IT.

e. Review materiel development actions for warfighting information systems and technology to ensure integration with related combat developments. This includes supporting and advising DISC4 on Joint and Army documents supporting unified, specified, combined, and service component commands.

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

g. Ensure spectrum management precepts contained in AR 5-12 are considered and included, where appropriate, in publications and formal training courses dealing with concepts, doctrine, operation and maintenance of C4/C3 countermeasures equipment, components and systems.

h. Provide electromagnetic spectrum impact consideration in the formulation of Army C4/C3 countermeasures concepts and doctrine.

i. Advise and support modeling and simulation programs in the establishment of standards, technical architecture, and master planning.

2–18. Commanding General, U.S. Army Materiel Command (CG, AMC)

The CG, AMC, will, in addition to duties listed in 2-16 above-

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

b. Maintain an inventory of C4/IT materiel systems.

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

d. Ensure that C4/IT component systems meet all interoperability requirements of the OA and standards of the JTA-A, U.S. Message Text Formats, Global Command and Control System (GCCS), North Atlantic Treaty Organization (NATO), international, and other joint or combined programs.

e. Operate and maintain the Army Operational Data Repository.

f. Establish and maintain configuration management of the C4/IT materiel component systems based on top-level, functional and operational sub-system and interface specifications.

g. 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.

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

i. Validate information systems technical requirements and associated cost estimates for all Army MILCON projects except for those projects specifically designated to FORSCOM as materiel developer.

j. Provide users at all levels with necessary technical support, assistance, and advice regarding information systems.

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

l. Plan, program, and conduct new equipment training for assigned systems and recommend required training to TRADOC, Medical Command (MEDCOM), the Judge Advocate General (TJAG), and the Chaplain Corps, for inclusion in their Army schools program.

m. Provide technical support and evaluation to DISC4 during requirements validation for IT.

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

o. Coordinate C4/IT systems designs with TRADOC.

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

q. Perform system engineering for the combat service support battlefield functional area (BFA) of the Command, Control, and Subordinate Systems (CCS2).

r. 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.

2–19. The Commanding General, U.S. Army Forces Command (CG, FORSCOM)

The CG, FORSCOM, in addition to duties performed in 2-16 above, will exercise command and control of the Army Signal Command (ASC) in its performance of its information technology (IT) mission. ASC will-

a. Identify IT system requirements and associated cost estimates for OCONUS Army MILCON projects.

b. Provide products and associated services for assigned IT responsibilities.

c. As assigned, provide users at all levels with necessary technical support, assistance, and advice regarding Army communication systems.

d. Develop and acquire technical solutions for communication systems for which USASC is the assigned materiel developer.

e. Develop operational procedures for C4/IT as assigned by the DISC4.

f. Provide technical support and evaluation to DISC4 during requirements processing for communication systems.

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

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

i. Operate and maintain 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.

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

k. 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. Draft agreements will be forwarded to HQDA for staffing and approval.

l. Provide an information systems 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.

m. In support of the information requirements of the Joint Staff (JS):

(1) Maintain ASC communications assets designated as part of the Joint Communications Support Element (JCSE).

(2) Provide reports on JCS-controlled USASC communications assets to the JCS as required.

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

(4) Develop and maintain plans in support of JCS requirements.

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

(1) Participate in all negotiations concerning recognized requirements.

(2) Serve as executive agent for all memorandums of understanding, letters of agreement, or similar documents, based on the guidelines provided by JCS and DOD policy (DODD 5530.3).

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

(4) 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.

(5) Provide, operate, and maintain equipment, facilities, and systems (or services) required supporting U.S., NATO-U.S., and NATO member communications objectives as assigned.

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

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

p. Service unofficial telephones furnished by the Army, including those installed in public quarters and other military and civilian personnel housing.

q. Manage the administration and operation of Army Military Affiliate Radio System (MARS) programs, including acquisition, storage, distribution, and accounting for equipment.

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

s. Develop near-term and long-term communications security and survivability programs.

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

u. Provide an assessment of progress per National Security Decision Directive 42, National Policy on Telecommunications and Automated Information Systems Security, and Section IV of National Telecommunications and Information Systems Security Directive 900, Governing Procedures of the National Telecommunications and Information Systems Security Committee.

v. Ensure Army compliance with DISA telecommunications report procedures as published in DISA Circular 310-130-1 and DOD policy for video teleconferencing (VTC) Management, Acquisition, and Standards, 26 October 1993.

w. Serve as Executive Agent for operating and maintaining designated Defense Red Switch Network, Defense Satellite Communications, Defense Information Infrastructure (Microwave and Fiber Optic Cable Systems), NIPRNET and SIPRNET Routers, Defense Messaging System operational requirements, Defense Switch Network, and operational requirements for National Command Authority/Commander in Chief (NCA/CINC) communications teams in support of the Army.

x. Establish and execute a program to unify the Army's network and systems management and information and

information systems security functions to enhance the protection, availability, confidentiality, and integrity of sensitive but unclassified and secret sustaining base networks and information systems.

y. Exercise configuration management of the integrated hardware and software solutions for the Army's wide area network and systems security infrastructure.

z. Serve as the Army's focal point for the development of formal intelligence production requirements and other exploitation of the DOD Intelligence Production Program (DODIPP) for identification and analysis of information operations threats to Army networks and systems.

aa. Manage the "army.mil" Internet domain and the assignment of sub-domains requested by other Army organizations.

2–20. Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM)

The CG, INSCOM will, in addition to the duties performed in 2-16 above-

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. Provide OA input to TRADOC, as required.

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

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

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

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

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

2–21. The Army Surgeon General/Commanding General, U.S. Army Medical Command (CG, MEDCOM)

The CG, MEDCOM, will, in addition to the duties performed in 2-16 above:

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 combat camera documentation support by ensuring applicability to internal command operational plans and rapid response to wartime, contingencies, joint exercises, and natural disasters.

2–22. Commanding General, United States Army Corps of Engineers (CG, USACE)

The CG USACE will, in addition to the duties performed in 2-16 above-

a. Implement an IT Architecture incorporating all engineering functions that require interface between the Civil Works program, the Army Military Construction (MILCON) program/implementation and management of common assets.

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

c. Provide guidance, data, and detailed assistance to the Army on the use of Computer Aided Design and Drafting hardware and software.

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

2–23. Commanders of the Army Components of unified and sub-unified 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 initiated by the MACOM/AC/FOA to TRADOC as required.

c. Coordinate with TRADOC, AMC, and FORSCOM on matters pertaining to C4/IT combat and materiel developments.

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

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

f. Integrate tactical visual information (Combat Camera) 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.

2–24. U.S. Army Reserve Command and the U.S. Army National Guard

The U.S. Army Reserve Command and the U.S. Army National Guard are responsible for the same responsibilities as specified in 2-16.

2–25. Commanders or directors of major subordinate commands (MSC), FOA, separately authorized activities, tenant, and satellite organizations

Commanders or directors of major subordinate commands (MSC), FOA, separately authorized activities, tenant, and satellite organizations will, based on guidance of their parent organization, accomplish the same information management responsibilities as their parent organization commensurate with their mission, size, responsibilities, and location.

a. Commanders of MSCs will designate a DCSIM or equivalent senior IM official who will have the same staff responsibility for the supported MSC as the DCSIM at MACOM level.

b. FOAs and other organizations will, as a minimum, establish/appoint an information management office/officer to plan and/or supervise the execution of information management.

c. Coordinate information systems requirements with the installation or area DOIM.

d. Designate a MSC or FOA VI manager. If VI is managed outside of the DCSIM review chain, the VI manager will coordinate (copy furnished) with the DCSIM on VI plans, strategies, and resourcing. VI responsibilities include functions outlined in paragraph 2-16.

2–26. Installation, State Area Command (STARC), or comparable level community commanders

Installation, State Area Command (STARC), 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 telephone, voice, and data network management functions for the installation, to include installation, operations, and maintenance, and configuration management of common user component devices.

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

(3) Validate TA compliance for all IT-related developments or acquisitions initiated within the installation level.

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

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

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

b. Appoint a record manager who will carry out records management program responsibilities.

c. Appoint a single installation Visual Information Manager. Commanders will ensure that the installation VI manager and activity is functionally aligned to reflect MACOM organizational structure. VI responsibilities include functions outlined in paragraph (see Commanders of Army Major Commands (MACOM)), and others, as assigned by the MACOM VI manager.

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

e. Establish and maintain an Information Management Support Council (IMSC).

f. Commanders or directors of organizations comparable to an installation where there is no DOIM will implement procedures comparable to those managed by DOIMs.

2–27. Commanders of Army Reserve Support Commands (RSC)

Commanders of Army Reserve Support Commands (RSC) will accomplish the same information management responsibilities as the U.S. Army Reserve Command (USARC), commensurate with their mission, size, responsibilities, and location.

2–28. Program, Project, and Product Managers (PMs), and IT materiel developers

Program, Project, and Product Managers (PMs), and IT materiel developers, will-

a. Prepare and submit timely and accurate periodic program performance reports, as required.

b. 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 per the AEAGD.

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

(3) Coordinate TA profile, OA and SA products for their systems with the PEO and management official of gaining commands and installations.

(4) Coordinate their systems architectures with MACOMs and DOIMs prior to fielding systems to installations within the MACOM.

c. Coordinate fielding plans for their systems with senior information management officials of gaining commands and installations to ensure compatibility with existing systems and IT support structure.

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

2–29. PEOs and direct-reporting PMs

PEOs and direct-reporting PMs will-

a. Develop AEA architectures (OA, TA and SA) and act as the integrator for systems of systems under their purview and coordinate with DISC4 per the AEAGD.

b. Develop and coordinate OA data with TRADOC as input to Army-wide OA for requirements.

Chapter 3
CIO Management

3–1. General

Executive Order (EO) 13011 mandates that federal executive agencies promote the effective design and operation of all major information resources management (IRM) processes with oversight by a Chief Information Officer (CIO). CIO management focuses on those policies, processes, and organizational responsibilities necessary to accomplish the mission defined primary in governing legislation and other guidance. Such responsibilities include strategic planning, business process analysis and improvement, assessment of proposed systems, resource management (to include investment strategy), performance measurements, IT acquisition, and training. This chapter covers the required participation of HQDA, MACOMs, installations, and other Army activities in executing the IRM management process and assisting the CIO. All statements regarding the CIO refer to the Army-level CIO unless otherwise indicated.

a. Mission. A CIO's primary responsibility is Information Resource Management (IRM). Executive Order 13011 mandates the establishment of a CIO at the executive agency level. The Army, as a military department, is an executive agency. The CIO provides advice to the Chief Executive Officer (Secretary of the Army) and other senior management personnel to ensure that IT is acquired and information resources are managed, consistent with established priorities. The full spectrum of CIO responsibilities (including IT/IM and National Security Systems (or Command, Control, Communications, Computers, and Intelligence) (C4I)) are delineated throughout this regulation.

b. 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 paragraph 2-1, the Secretary of the Army directed other duties. These include validating warfighting requirements and undertaking the resourcing and prioritization of individual programs in coordination with the DCSOPS, subject to the oversight, review and approval of the ASA (FM&C).

c. The CIO process will not routinely address IT systems that are funded under the NFIP or other intelligence programs. The DCSINT will represent Army NFIP-funded IT/C4I under the DOD and NFIP Program Manager's CIO programs. DCSINT will bring any IT NFIP concerns to the CIO's attention.

3–2. Designation of CIO

DISC4, as the CIO, is the only federally mandated CIO for the Army. Subordinate organizations below HQDA may, at their discretion, designate a "Chief Information Officer" and establish supporting offices within their organization. Any subordinate CIO may also serve as the DCSIM or equivalent position. 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. A designated CIO will have the following responsibilities and authorities:

a. Provide management oversight for IT investments to achieve expected levels of performance.

b. To the extent possible, serve as the senior IM official with duties similar to those of the Army CIO. The CIO duties are further delineated in this chapter and in chap 2.

3–3. IM/IT resource management

a. Planning.

(1) Strategic Planning is conducted at many levels. At the highest level, National Military Strategy is derived from the National Security Strategy, which emanates from the President through the National Security Council. The DOD Defense Planning Guidance translates National Military Strategy for the Military Departments and Defense Agencies to develop their own strategic plans and eventually their POMs. At HQDA, The Army Plan (TAP) is the Army's Strategic Plan.

(a) . HQDA C4/IT Strategic Planning. The broadest strategic C4/IT perspective for the Army is in the Army Enterprise Vision and Army Enterprise Implementation Plan. To better incorporate the elements of Joint Vision 2010 and Army Vision 2010, Army Enterprise XXI will provide an updated strategic path to the future in the C4/IT arena. On a more near-term basis, and tied to the Planning, Programming, Budgeting, and Execution System (PPBES), the ASA (ALT) and the DCSOPS will publish the Army's Modernization Plan (AMP), which provides specific information on and direction for battlefield and supporting systems. This includes the C4/IT modernization plans that are embedded in the AMP annexes.

(b) MACOMs will develop their own strategic plans, using the guidance from higher headquarters strategic plans. Except when specifically requested by the CIO, MACOM C4/IT strategic plans will not be submitted to HQDA, but will be used for internal MACOM planning and execution. 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 should describe how the vision and goals support the Army strategic vision, missions, and goals; any architectural developments and how these and other existing or ongoing efforts comply with the Army Enterprise Architecture. They should also include any new business processing improvement efforts that may result in an IT investment; performance measurements in conjunction with organizational processes; and new systems partnerships with other organizations. Other areas for consideration are the organization's investment strategy, a modular contract strategy for individual systems, and information systems security prerequisites. C4/IT planning guidance at organizations below MACOM level is at the direction of the MACOM DCSIM or functional proponent.

(2) IT Capital Planning and Investment Strategy.

(a) The CIO's Investment Strategy, together with other acquisition documents, such as the acquisition strategy and program baselines, will form the basis for the Army's IT capital plan. This strategy will evaluate and establish priorities for IT investments throughout the PPBES and acquisition processes. The capital planning process, which is not appropriation unique, begins with the formulation of an IT investment strategy, developed according to selected criteria determined by the CIO and other senior management, and continues during program and budget development. The purpose of a capital planning process and investment strategy is to assess the value and manage the risks of the Army's IT acquisitions. To ensure that this mandate is followed, certain criteria such as return on investment, results of performance metrics and measures, contribution to military operations, improved efficiency, or support of revised business processes will be used throughout the acquisition process. These criteria will be used to help determine whether to continue, modify or terminate a program or project (Clinger-Cohen Act).

(b) MACOM senior IM officials should also develop an IT investment strategy to assist in funding decisions.

b. Programming.

(1) CIO representatives at the colonel/GS-15 level will participate as members in Program Evaluation Groups (PEG) meetings. These representatives will advise the PEG members on the IT investment strategy, technical implications, architectural compliance requirements, and other factors used in the PEG decision-making process. PEGs will include the CIO representatives in any matters dealing with C4/IT programs such as funding issues (bills, billpayers, and movement of dollars) and affected Management Decision Evaluation Package (MDEP) changes.

(2) CIO C4/IT PEG representatives will ensure that each new and revised POM and unfunded requirement (UFR) submission for an IT system (costing $2M or more in a fiscal year, or $30M or more total life cycle) contains a statement on accomplishing process analysis and revision. A summary of the process analysis and revision may also be provided, as appropriate.

(3) The CIO may raise selective issues that cannot be resolved within the PEG to the next level of the PPBES process. The CIO will participate in all PPBES decision-making bodies except the Army Resources Board.

c. Reporting of Capital and Other IT Expenditures. The CIO will review and validate the Information Technology Systems Budget submission on IT obligations after final budget decisions have been made. IT capital investments and other anticipated IT expenditures are submitted in the Tab G report to OSD as part of the normal POM process. Specific instructions are published in the Resource Formulation Guidance. See also DOD 7000.14-R, Vol. 2B, chap 18.

d. MACOMs and below.

(1) Senior IM officials below the Army level will participate in a similar process for PPBES decisions.

(2) For POM and UFR submissions, MACOMs will identify whether process analysis and appropriate revision have been accomplished or are planned for IT systems or systems with a C4/IT impact that cost $2M or more in a fiscal year, or $30M or more total life cycle. These systems will be accepted in POM or UFR submissions as long as process analysis and revision are accomplished prior to the budget year or prior to systems selection, whichever comes first. If process analysis and revision, as appropriate, are not accomplished, programmed funds will be removed at the beginning of the budget year.

(3) MACOMs will use the C4/IT portions of the AMP as a guideline to develop their Execution Plans.

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, e.g., another MACOM 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 reengineering (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 $2M or more in a fiscal year, or $30M or more total life cycle cost. However, any process will be assessed, as mission needs change. Process analysis and appropriate revision 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) Reduced cycle time.

(5) Elimination of non-value added activities.

(6) Streamlined high-cost activities.

(7) Increased product quality.

(8) Lowering costs of providing services.

(9) Moving to a "fee-for-service" mode of operation.

(10) Adapting to changing technology and information systems.

(11) Integrating duplicative information across processes.

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

(1) Validate the organization's mission, goals, and objectives as they relate to the process to be analyzed.

(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. Describe how it is deficient. If there is no current process, describe the situation that is 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 in the mission needs statement (MNS) and operational requirements document (ORD). The doctrine, training, leader development, organizational design, materiel, and soldiers (DTLOMS) requirements methodology will be used. See AR 71-9 and TRADOC Pamphlet 71-9 for information on the requirements generation process. Process analysis and revision will be accomplished before submitting a MNS or ORD.

g. Process analyses, improvements, and reengineering of mission-related and administrative work processes will be documented in a CIO database on the CIO Web site (http://www.army.mil/ciog6/cio/). All Army organizations will provide information and data on improvement initiatives for the database.

h. Prior to beginning any process improvement initiative, the activity proposing the initiative will search the database. Justification is required for a proposed improvement project that is comparable to one that is just beginning, ongoing, or completed. ODISC4 will review the justification and provide written approval/disapproval to duplicate an existing initiative.

i. 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 $100,000, replacement parts for existing systems, and routine replacement or upgrade of office automation equipment, e.g., upgrading a local area network or replacing office computers.

3–5. CIO validation of requirements

a. For warfighting processes, the CIO will validate all warfighting requirements through the review of appropriate requirement documents, per AR 71-9. For certain warfighting requirements, e.g., joint, DCSOPS may require a SES/general officer signature. Validation criteria will include:

(1) Determination that non-materiel alternatives were judged to be inadequate per AR 71-9 and a process analysis (or DTLOMS analysis) has been completed to make this determination.

(2) A statement that any materiel solution must be Joint Technical Architecture-Army compliant and have the ability to be interoperable.

(3) Evaluation of emerging technologies.

(4) Inclusion of outcome-oriented performance measurements.

(5) Compliance with information security requirements.

(6) Inclusion of spectrum management criteria.

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

(8) Other criteria as appropriate.

b. For mission-related and administrative work processes, the process associated with the mission need will be evaluated to determine whether it can be outsourced.

(1) The functional proponent must validate and/or approve the process analysis and revision (if appropriate) if the revision will result in an IT system costing $2M or more in a fiscal year, or $30M or more total life cycle.

(2) The functional proponent must be informed of process analysis and revision (if appropriate) if the revision will result in an IT system costing less than $2M.

c. CIO validation will be completed at the colonel/GS-15 level.

d. MACOMs will follow a like process for requirements, which has been delegated to them under AR 71-9.

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.

(1) Measures of effectiveness demonstrate that an organization is doing the right things.

(2) Measures of efficiency demonstrate that an organization is doing things optimally.

b. Measuring IT investments. Performance measures will be developed for each IT investment which supports organizational missions before execution or fielding of that investment. The performance measures will:

(1) Gauge the value-added contribution of the IT investment to missions, goals, and objectives.

(2) Be the critical few measures that provide a clear basis for assessing accomplishment, aiding decision-making, and assigning accountability at each management level.

c. Performance measurements in requirement documents. Performance measures in support of warfighting materiel requirements with an IT/C4 impact will be included in the appropriate requirement document per AR 71-9.

d. 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.

(1) Enterprise-level IT performance measures will assess Army-wide mission accomplishment and will generate outcomes that guide policy direction and strategies. IT performance measures at the Army Enterprise level will ensure that:

(a) Investments are synchronized with overall DOD/Army mission priorities. All functional strategic plans are explicitly linked to enterprise level plans.

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

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

(2) IT performance measures at the functional level will assess functional mission outcomes relative to strategic objectives of the next higher organization. Functional managers, e.g., the functional proponent or those at the MACOM, 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.

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

(b) Performance will be customer-oriented.

(3) Performance measures at the program/project level will assess progress towards accomplishing expected functional mission outcomes and results of C4/IT investments by collecting information, i.e., 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:

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

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

e. 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.army.mil/itmetrics. Compiled IT metrics data will be used to identify mission capability shortfalls and to re-allocate IT investment resources.

f. A cost-benefit analysis must be applied against any proposed performance measurement system. If the cost of

collecting and analyzing the required data exceeds benefit to the organization, a measure will not be used unless directed by higher authority.

3–7. Army acquisition and CIO assessment

The acquisition process begins at the point when an organization's C4/IT needs are established in the appropriate requirement document per AR 71-9. The acquisition process also involves the description of requirements to satisfy the needs, how 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 process of fulfilling the needs by contract.

a. The CIO will ensure that 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). MACOMs will establish the materiel requirements document format and compliance procedures for IT equipment and systems under $10 million.

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 acquisition categories (ACAT) I and II programs. PM's of ACAT I and II programs will provide a self-assessment of compliance for every program to the CIO. See AR 70-1 and DOD 5000.2-R for additional information on acquisition program categories.

(2) Non-ACAT investments for IT services will also be assessed for any programs that cost $2 million or more in a single year or with a total life cycle cost of $30 million or more. The Milestone Decision Authority will perform these assessments.

(3) MACOM information management officials will evaluate ACAT III and IV programs (with IT expenditures $2 million or more in a single year or with a total life cycle cost of $30 million or more). MACOMs will follow a like process as defined in AR 70-1.

3–8. IM/IT personnel proponency

a. The CIO will define IM/IT competencies and establish professional development standards and practices for Army personnel in IM/IT career areas.

b. The CIO will provide guidance on education, training, and professional development opportunities for Army personnel to support their effective acquisition, management, and use of IT resources.

c. The CIO will develop plans, strategies, and initiatives for hiring, training, and developing civilian personnel in IM/IT areas.

d. IM/IT competencies will be integrated into Army institutional training as appropriate and published as part of the Army Civilian Training, Education, and Development System (ACTEDS) Plan.

e. The CIO is responsible for the policy, oversight, and management of CP-34.

3–9. Information management organizations below Headquarters, Department of Army

a. MACOMs. Every MACOM will have a senior information management official as a principal staff officer with CIO-like duties. The MACOM IM staff officer responsible for IM may be designated the Deputy Chief of Staff for Information Management (DCSIM), CIO, G-6, or other title as directed by the commander.

b. Major Subordinate Commands (MSC) will establish a DCSIM or equivalent IM official with the same staff responsibilities as a MACOM DCSIM.

c. Installations.

(1) The installation information manager is designated the DOIM. There will be only one DOIM at an installation designated by the host command or activity. This DOIM will be the focal point for providing IT support for the entire installation, including all its tenants. Other activities on an installation will not establish a DOIM but may have an Information Management Officer (IMO) or other technical personnel to accomplish internal IT services. Where no post, camp, or station installation configuration exists, the host command or activity will ensure IT support.

(2) Staff proponency and placement of VI activities, records management, and printing and publications is at the Commander's preference.

(3) National Guard.

(a) The State Area Command (STARC) is equivalent to an installation. These responsibilities include the development and maintenance of the installation IM resources, the direct management and supervision of the information management staff, operational activities, and related programs and activities except where they have been exempted by HQDA.

(b) The United States Property and Fiscal Office (USPFO) will man and operate a Data Processing Facility to perform statutory accountability functions. The STARC DOIM will provide information management services and support for the State, to include the USPFO.

d. Other. Tenant and satellite organizations, separately authorized activities, Government-owned/contractor-operated

facilities, regional support activities, field operating activities, and major staff entities, which are not directly supported by a DOIM or DCSIM, will designate an IMO. The IMOs will operate and maintain the organization's IM resources. Other responsibilities are at the direction of the activity manager. Tenant activities on installations will provide their organization's information requirements to their parent MACOM and furnish a copy of their input to the installation DOIM. The DOIM will identify the tenant requirements to be satisfied by sharing installation resources and the impact on the installation resources and architecture

Chapter 4
The Army Enterprise Architecture

4–1. Introduction

The Army Enterprise Architecture (AEA) is the Army's corporate framework and management process for developing and maintaining a comprehensive, integrated IT systems blueprint. The Army's information technology systems blueprint will be developed per section 5125 (b) (2) of 1996 Clinger/Cohen Act and will translate Army operational patterns into discrete warfighter capabilities needed to achieve the common goals of the Army and DOD. The AEA is fundamental to achieving information dominance by linking military strategy and doctrine to the employment of information technology used in executing military operations.

a. This chapter provides policy to implement IT-related guidance and applies to the development, promulgation, implementation, management and maintenance of the AEA. Detailed procedures implementing this policy are provided in the AEA Guidance Document (AEAGD). The AEAGD is located at http://arch-odisc4.army.mil/.

b. AEA is composed of three architecture views: Operational Architecture (OA), Technical Architecture (TA), and Systems Architecture (SA), as defined in the Joint Technical Architecture-Army (JTA-A).

c. The following enterprise-level documents, in addition to the AEAFD, are used to develop, manage, and facilitate the implementation of the AEA:

(1) The AEA Guidance Document (AEAGD) will be used Army-wide to ensure that Army architectural efforts are inter-relatable and integratable across the Army and joint/combined organizational/functional boundaries. The AEAGD provides detailed procedures on how to design, develop, maintain, and implement Army architectures per Army and DOD policy. AEAGD products will support C4/IT strategic planning requirements per paragraph 3-3a(1)(b).

(2) The AEA Master Plan (AEAMP) will be used Army-wide in planning, programming, budgeting, and execution of AEA strategic goals, objectives, and tasks. The AEAMP provides the Army's corporate strategy, to include priorities, schedules/timelines, tasking, and resource allocations for managing the decentralized and incremental AEA development/maintenance efforts. The AEAMP is located at http://arch-odisc4.army.mil/.

d. The Army will incrementally develop the AEA using decentralized architecture design efforts as outlined in the AEAMP. The AEAMP will be reviewed by the Enterprise Council of Colonels and approved by the Enterprise General Officer Steering Committee. Procedures will be implemented (as guided by the AEAGD) to ensure that the resulting data and products are sufficiently standardized to support required analyses of integrated IT architectures. Each architectural view (i.e., OA, TA, and SA) will be developed to provide information needed for analysis and integration at and across various levels of architectural integration. See the AEAGD for the specific definitions and uses of the various architectural levels of integration.

4–2. General guidance for development and use of the AEA

a. This policy is applicable, Army-wide, to all efforts which plan for, acquire, develop, manage, operate, maintain, and use IT capabilities whether configured as systems of systems, end-systems, or provided as components of other systems. These policies will be applicable to, but not limited to:

(1) Acquisition programs of all types as defined by AR 70-1.

(2) Other efforts not classified as acquisition programs that have IT capabilities except IT embedded in devices with no external interfaces.

b. The AEA Master Plan will define and categorize the specific groups of programs and initiatives to which specific AEA policies will be applicable.

c. The DISC4 will act as the AEA Integrator of the OAs/SAs/TAs for systems of systems architectures at the enterprise level. PEOs and MACOMs will act as the integrator for systems of systems under their purview. PMs and IT developers will act as the integrator for their systems.

d. Architectures are mandated for the development and management of IT capabilities. Organizations (e.g., functional proponents, materiel developers, PEOs, PMs, and IT initiative leaders at the MACOM/agency/installation levels) responsible for developing integrated architectures will follow the procedures provided by the AEAGD.

e. Army data administration policies per DODD 8320.1 will be implemented within the scope of the AEA per the direction in paragraph 4-6 below.

f. Mandatory AEA products cited herein are based on mandates provided by DOD C4I Surveillance and Reconnaissance (C4ISR) Architecture Framework Document.

4–3. Operational architecture (OA)

a. Mandatory OA products and the procedures for their development will be described in the AEAGD.

b. TRADOC, as the Army Operational Architect, will integrate, maintain and control an Army-wide Operational Architecture which integrates lower level OA's per the configuration management procedures in the AEAGD.

c. OAs will be developed by the organizations listed in paragraph 4-2d.

4–4. Technical architecture (TA)

a. The DOD Joint Technical Architecture (JTA) provides the baseline of standards with which Army IT capabilities will conform. The Army Acquisition Executive (AAE), as the Army Technical Architect, will develop and approve the Army-specific refinements or extensions to the JTA, which are promulgated in the JTA-A. MACOMs and PEOs may further refine and extend these standards in a TA Profile used within their domains, provided that such refinements and extensions do not reduce overall interoperability capabilities with systems developed in accordance with the JTA-A.

b. All Army IT developers and PMs will:

(1) Design or acquire systems within the constraints imposed by the JTA-A.

(2) Develop a TA profile(s) for their assigned system(s) per guidance provided by the AEAGD.

(3) Include JTA-A usage, as appropriate, in requirements, program management and contractual documents.

(4) Apply data standards and data standardization guidance (in compliance with DODD 8320.1), when applicable for information systems, as directed by Section 4 of the JTA-A and paragraph 4-6 of this regulation.

c. All existing IT capabilities will comply with the JTA-A by FY 2006.

d. The Army Technical Architect must approve all waivers at any level to the JTA-A. The Army Technical Architect is the final decision authority for conflicts among TA profiles that cannot be resolved at lower levels.

e. The IT materiel developer will manage configuration control of the content of the TA profile for a system. As JTA-A standards and guidance evolve, the IT materiel developer will determine which standards in JTA-A guidance are applicable to a specific IT capability or acquisition.

4–5. Systems architecture

a. The DISC4, as the Army Systems Architect, will integrate, maintain and control an Army Systems Architecture (Army SA) which integrates lower level SAs per the configuration management procedures in the AEAGD. The Army SA will be based on the multiple levels of architectural configurations as described in paragraph 4-1d. The Army Systems Architect will identify and document Army SA rules, constraints, and common IT solutions in the AEAGD.

b. SAs will be developed by the organizations listed in paragraph 4-2d.

c. Mandatory SA products and the procedures for their development are described in the AEAGD.

4–6. The Army Data Management and Standards Program (ADMSP)

a. The Army Data Management and Standards Program (ADMSP) establishes information about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data used in the Army.

(1) The ADMSP facilitates the dissemination and exchange of information among organizations and information systems throughout not only the Army but also the Department of Defense and the Federal Government. The ADMSP implements DODD 8320.1 and the information standards portion of the JTA-A.

(2) The ADMSP manages information requirements from data models and business rules down to data-element and data-value levels of detail, within the policies of the AEA and by use of the procedures of the AEAGD.

(3) The ADMSP facilitates internal, joint, and combined interoperability through the standardization and use of common data elements.

(4) The ADMSP improves data quality and accuracy, and minimizes the cost of data production and data maintenance.

(5) ADMSP procedural guidance will be developed by the CDAd.

b. Per DODD 8320.1 Army information is a Government resource and will be shared unless specifically limited by law, regulation, need-to-know, security, or privacy restrictions.

c. Data standards (as provided by the JTA-A) will be used to guide all data exchanges. Data management requirements will be included in IT planning documents.

d. The Army Operational Data Repository (AODR) is a centralized, meta-data repository used for the procedural storing, universal viewing, and selective re-use of (all, or parts of) architectures of functional Army systems. The functionality of the AODR promotes interoperability, between Army systems, by allowing the Army Data Management Group (ADMG) to perform technical reviews of all proposed architectures (models) and to assist in the harmonization of the functional requirements with the DOD data standardization requirements. Information about Army data (meta-

data) will be maintained and controlled in the AODR and will be included as part of the standard data element documentation.

(1) Databases and information systems will use standard data elements.

(2) Information systems design documentation will use standard data element documentation from the AODR.

(3) Standard data elements will be used in newly developed and redesigned applications and, when feasible, in existing systems.

(4) Candidate standard data elements will be submitted for standardization as early in the information system life cycle as possible.

(5) Candidate standard data elements will undergo functional review by the appropriate CFDAd and technical review by the Army Data Management Group.

(6) All data elements in data requirement documents will be standardized in accordance with DOD 8320.1-M-1 and the AEAGD.

e. All data will be protected per AR 380-19 and AR 380-5.

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

(2) Continuity of operation (COOP) analyses will be conducted for data and meta-data per DOD and Army Data Administration Strategic Plans.

f. As CDAd, the DISC4 establishes Component Functional Data Administrators (CFDAds), who are responsible for standardizing data in their functional areas.

g. CFDAds will identify data administrators to carry out data management and standards actions for the organization and serve as liaisons between functional experts and technical personnel.

h. Only organizations identified by CFDAds will create or update data values exchanged with or disseminated to any other organization.

(1) Data synchronization requirements will be identified and documented as part of the standard data element documentation.

(2) Data synchronization requirements will consider information flows and data elements (including data transfers, system run cycles, management decision cycles, timeliness, and accuracy).

i. PEOs, PMs, MACOMs, and agencies will ensure its materiel developers comply with Army and DOD data requirements by developing and maintaining a Program Data Administration Strategic Plan and a Program Data Performance Plan.

j. Each PM/materiel developer will develop and maintain a fully attributed system data model in IDEF1X format per JTA-A, and submit data standards proposal packages for review through respective chains.

k. The CFDAd will review the data structure of assigned data elements in the Army Operational Data Repository at each milestone and at five-year increments after system deployment.

l. The materiel developer is responsible for integration of COTS software and ensuring interoperability with existing data models and architectures.

4–7. Installation Information Infrastructure Architecture (I3A)

The I3A is a synchronization tool encompassing major Army automation and communications programs, thus supporting the Sustaining Base of the JTA-A. It is used for designing target system architectures and cost models for Army installations worldwide.

a. Army organizations must comply with I3A guidelines for modernizing IT infrastructures from the installation gateway to the end user boundary.

b. I3A includes all components of the office installation communications capabilities. It addresses the details of the common user facilities providing the transport capability for voice, data and imagery and the appropriate information assurance thereof. The I3A also addresses the components that are required to provide connectivity from the installation long-haul point of presence to the end user device, supporting the warfighter.

Chapter 5
Information Assurance

5–1. Mission

As promulgated by DOD, information assurance (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 architecture 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, command and control (C2), physical, software, hardware, procedural, personnel, network, communications (COMSEC), operational, and intelligence. Information Assurance Vulnerability Alert (IAVA) is a process within the command and control 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, base operations, and force protection. See also AR 380-19 for more guidance on information assurance.

a. 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.

b. IA seeks to maintain effective C2 of friendly forces by protecting critical information infrastructures from unauthorized users, detecting attempts to obtain or alter the information, and reacting to unauthorized attempts to obtain access to or change information. These measures focus on the integrity, confidentiality, availability, authentication, verification, protection, non-repudiation of the infrastructures and the information contained within.

5–2. Management structure for information assurance

An appropriate management structure will be established at all levels to implement the Information Systems Security Program (ISSP) and the IAVA for the protection of critical information infrastructures. See AR 380-19, chapter 1, for more information on the ISSP management structure. In addition, commanders will appoint, as appropriate, personnel who are responsible for enforcing the IAVA process.

a. Each MACOM will appoint an information assurance officer to protect MACOM-level critical information infrastructures. The IA officer will develop, establish, implement, manage, coordinate, and assess IA policies and programs within that command. The IA officer will be the commander's representative with the Army IA office. The IA officer will be responsible for administration of those areas directly related to the security of electronic data.

b. Activities below MACOM level will appoint an IA officer. The IA officer will establish and implement the IA program for all information infrastructures within that command or activity. This includes posts, installations and installation equivalents.

c. An IA officer will be appointed in environments where personal computers, workstations, file servers, local area network, or small systems are oriented toward the functional user as the operator. The IA officer will ensure these systems are secure.

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

e. The IA officer may also serve as the Information Systems Security Program Manager, Information Systems Security Manager, or Information Systems Security Officer at the discretion of the commander.

5–3. Information system certification/accreditation

All information systems and networks will be subjected to an established certification and accreditation process that verifies that the required levels of information assurance are achieved and sustained. Only Army-approved IA products will be used. Information systems and networks will be certified and accredited per DODI 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP). The DITSCAP process 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. MACOM commanders or their designates (not less than lieutenant colonel or GS-14) are the accreditation authorities for sensitive but unclassified systems operating the dedicated or system high mode of operations. The DITSCAP process will be applied to all systems requiring certification and accreditation throughout their life cycle. (See also AR 380-19 and DODI 5200.40.)

5–4. Physical security

Commanders who operate and maintain any information system will provide adequate levels of physical security per AR 380-19, chapter 2, section IV.

5–5. Software security

a. Controls will be implemented to protect system software from compromise, subversion, or tampering. The IA officer, DOIM, and systems administrator must approve all software used on Army networks prior to installation and operation.

b. When data base 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 380-19, chapter 2.)

c. All software packages providing security services will have appropriate evaluation/certification prior to use or be selected from the National Security Agency (NSA) ISS Products and Services Catalog. Other evaluated products may be used based on a valid justification and approval from the designated authority. Agencies responsible for distribution of software security products will ensure their evaluation and certification. (For more information, refer to AR 380-19, chapter 2.)

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, installation (or equivalent) commanders 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 IA officer, who will notify the MACOM-level IA officer. Reporting structure will follow the same structure as in paragraph 5-2. The operator, IA officer, and the DOIM will notify the Regional Computer Response Team (RCERT) 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, advisories, and that corrective measures are taken.

c. Any information system which processes data in a Sensitive Compartmented Information (SCI) environment will ensure its equipment used for processing, handling, and storing is in compliance with Director of Central Intelligence Directive (DCID) 1/16 and AR 380-19.

d. User identification and password systems must support the minimum requirements of accountability, access control, least privilege and data integrity. The DOIM will manage password control which the systems administrator will implement.

5–8. Personnel security

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

a. All individuals who are appointed as IA/ ISSP personnel and systems administrators must complete an Information Systems Security course and other courses, as necessary, equal to the duties assigned to them.

b. All personnel who require access to information system processing classified Defense information to fulfill their duties will possess a security clearance based on the appropriate personnel security investigation per AR 380-67.

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: (1) Risk analysis of resources, controls, vulnerabilities, and threats, and the impact of losing the systems' capabilities on the mission objective; (2) Management decision to implement security countermeasures and to mitigate risk; (3) Implementation of countermeasures; and (4) Periodic review of the risk management program.

Chapter 6
Command, Control, Communications, and Computers/Information Technology (C4/IT) Support and Services

6–1. Management concept

This chapter pertains to automation (computer software, hardware, and peripherals) and telecommunications (networks, long-haul and deployable communications), support for battlefield systems, and IT support for military construction. These policies promote decentralized execution of IT programs while maintaining Army-wide interoperability of capabilities required for supporting the warfighter.

a. Information transmission economy and systems discipline. MACOM commanders and agency directors will develop and implement policies and procedures to promote optimum, responsive, cost-effective use of all types of DOD information systems/services, and ensure the application of sound management practices in accomplishing information systems/services economy and discipline.

(1) Commanders/activity heads will establish an Information Management Support Council (IMSC) composed of primary staff to advise the commander on the development and implementation of C4/IT policies, procedures and priorities. The IMSC will also review and evaluate the economic and disciplined use of IT systems as part of its information resources.

(2) Local economy and discipline procedures will be consistent with guidance in this regulation. Commanders/activity heads will establish procedures to ensure:

(a) Personnel are familiar with the types and purpose of available communications, services and systems. Special emphasis will be placed on economy and discipline in use of long distance communications to include the use of the Defense Information Systems Network (DISN).

(b) 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 (business lines/flat rate). The use of a personal identification number (PIN) process for telephone control is authorized and recommended.

(c) Information managers review and revalidate all common-user Army information services, Government and commercial, regardless of user. The appropriate information manager will review dedicated information services and facilities at least every two years. Review will consist of toll-free numbers (purpose and traffic volume), calling cards (assignment and how and from where used), cellular phone and pagers (assignment, and how and when used). For further procedures, see also DA Pamphlet 25-1-1.

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, plans for the protection of critical records and files, and the provision of minimum essential operational capabilities and the relocation facility. HQDA staff agencies, MACOMs, and other organizations subordinate to HQDA are required to maintain a COOP consistent with AR 500-3. Each command, control, communications, computer, or information system deemed critical to essential HQDA missions or functions must also be supported by its own COOP that ensures its continuous operation under all conditions. All COOPs must be tested at least biannually. See also paragraph 8-5.

c. Electronic Commerce (EC). Army activities will use EC technologies to the maximum extent practicable to promote the goal of a paper-free (or near paper-free) business environment within the Army. The Army objective is to achieve a paperless acquisition process. Records created during electronic business/electronic commerce and maintained on electronic business/electronic commerce technologies will be preserved per retention schedules in AR 25-400-2.

d. Official and authorized uses of telecommunications and computing systems.

(1) The use of DOD and other Government telephone systems, 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. The DODD 5500.7-R, 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 to avoid disruptions of Army communications systems.

(2) All communications users must be aware of security issues and their consent to monitoring for all lawful purposes, of restrictions on transmitting classified information over unsecured communications systems, of prohibitions regarding release of access information such as passwords, and of the need for care when transmitting other sensitive information. See paragraph 6-3u for additional information on communications monitoring.

(3) Commanders recover toll charges, as practical, for unofficial/unauthorized personal telephone calls placed on official telephones by personnel in their organizations. Persons making unauthorized unofficial telephone calls may be subject to disciplinary action as well as charged for the calls.

(4) Official business calls and e-mail messages are defined as those that are 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. The installation or 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 only be made during non-peak, non-duty hours and must not exceed 5 minutes. Emergency calls may exceed this limit.

(6) Authorized uses of communications systems. Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DOD employee's usual work place 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 that they:

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

(b) 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).

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

(d) In the case of long distance (toll) calls, are:

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

2. Made to a toll-free number.

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

4. Charged to a personal telephone credit card.

(e) Serve 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).

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

(a) Use of communications systems in a way that would reflect adversely on DOD or the Army (such as uses involving pornography or access to pornography Web sites; chain e-mail messages; unofficial advertising, soliciting or selling via e-mail; and other uses that are incompatible with public service).

(b) 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, 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.

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

(d) Misuse. Both 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.

(e) Interference. 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:

1. Create, download, store, copy, transmit, or broadcast chain letters.

2. "Spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

3. Send a "letter-bomb," that is, to re-send the same email message repeatedly to one or more recipients, to interfere with the recipient's use of email.

4. Broadcast unsubstantiated virus warnings from sources other than systems administrators.

5. Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations.

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

7. Abuse of DOD and Army telecommunications systems, to include telephone, e-mail systems, or the Internet, may result in disciplinary action.

e. Use of privately owned assets. Employee-owned IT hardware or software may be used by Army personnel to process Army related work off the Government work site. Use of employee-owned IT hardware or software at the work site must be approved by the commander or designated official, after technical review and approval by the systems administrator. The products of Army-related work are the property of the U.S. Government, regardless of the

ownership of the automation hardware or software. Privately owned property should be properly registered as present at a Government location via the use of hand receipts and the owner must agree to sign a release from liability in case of theft, damage or malfunction.

f. IT Support Agreements. Army activities may provide IT support services to other Army, DOD or non-DOD activities on a reimbursable basis.

(1) Army activities, e.g., installation tenants, requiring IT support from other Army activities will coordinate with the supporting DOIM. Support agreements are normally not required for specifying IT support between two Army activities. The quality of IT support provided to other Army activities will be equivalent to the quality of support the supplier furnishes for its own mission, unless otherwise arranged. The DOIM is the primary source for IT contract support. Consideration may also be given to using contract capabilities available from other DoD and Federal activities.

(2) Army activities 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 United States Government, and the head of the supplying activity determines capabilities exist to provide the support without jeopardizing assigned missions. The quality of IT support provided will be equivalent to the quality of support the supplier furnishes to its own mission, unless otherwise agreed. An interservice support agreement (ISA) with associated service level agreement (SLA) will be negotiated to specify the services and basis for reimbursement. The supporting DOIM must be a participant in the ISA coordination. Depending upon the scope of the ISA, the MACOM DCSIM may be included as a third party.

(3) 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.

g. MWR Activities and Non-Appropriated Fund Instrumentalities (NAFI).

(1) Use of appropriated funds on a non-reimbursable basis is authorized to provide communications and data automation support to:

(a) MWR activities as outlined in AR 215-1 (Appendix 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).

(b) All other NAFI(s) as outlined in DODD 1015.6 (AAFES, Civilian Welfare and Restaurant Funds, etc.). 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 NAF. NAFI requiring DOIM-provided IT support will comply with this regulation and those policies promulgated by the installation DOIM or equivalent.

h. IT support for telecommuting.

(1) Telecommuting is defined as working from an alternative site via use of electronic means. Alternate sites may be the employee's home, a remote or outlying office, or a mobile site.

(2) Use of Government IT resources (such as computers, facsimile machines, modems, etc.) for telecommuting are authorized under certain conditions, which will vary greatly from one installation or activity to another. Army agencies at all levels are empowered to make the best possible choices for their missions and functions, relative to local conditions and resource constraints. Coordination with local legal offices is required in developing IT support agreements for telecommuting to ensure consideration of liability issues and the feasibility of IT support and services. (Telecommuting resources are not intended for individuals who occasionally check e-mail from their residences.)

i. Information access for the handicapped. 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 to 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 (CAP) , 5111 Leesburg Pike, Suite 810, Falls Church, VA 22041-3206, provides assistive technology accommodations and services to persons with disabilities at the Department of Defense (DOD), at no cost to individual activities. CAP operates a Technology Evaluation Center to match people with specific technologies. Funding is available to provide such things as interpreters, readers, personal assistants, telecommunications devices for the deaf (TDD), telephone amplifiers, listening devices, closed captioned decoders, and visual signaling devices for those with hearing problems.

j. Installation-level technical support and service.

(1) Help-desk operations. 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 point of contact for IT and networking problems. Help desks normally will determine the type of reported system problem within defined response times; 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, automatic data processing accountability support, hardware exchange, and repair service support.

(2) Since DOIMs cannot provide equal technical support, e.g., trouble shooting 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 be so restrictive as to preclude the use of the common infrastructure of any JTA-A compliant IS. The lists will not be used as the justification for eliminating

competition in contracting. Supported organizations and IT fielding organizations that rely on common network capabilities may deviate from supported product lists on an exception basis only.

k. Year 2000 (Y2K) Compliance. All C4/IT systems must be Y2K compliant.

6–2. Automation

a. DOD provided processing services. This paragraph pertains to Army use of DOD-provided centralized information processing services, e.g., DISA's Defense Megacenters, which are available to all military departments and services on a fee-for-service basis.

(1) The fee-for-service rates will be coordinated between DISC4 and the DOD providers for service provided to Army activities. Army activities will be assisted by the DISC4 in resolving issues with provision of, and funding for, services from DOD providers.

(2) MACOMs, installations, and activities are permitted to coordinate directly with DOD-providers to establish, maintain and reimburse for the specific set of services they require. See DODI 4000.19, Interservice and Intraservice Governmental Support, 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.

b. 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 mainframe processors and/or mini-computers, which generally operate on raised computer room floors and require controlled environmental conditions. Facilities (e.g., functional offices) that merely support local area networks, 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 data processing alternatives by conducting benefit/cost analysis studies per AR 5-20 to determine whether services should be consolidated, outsourced to the private sector or another federal agency (e.g., Defense megacenters), or retained within the agency. Significant change in mission or funds warrants conducting benefit/cost analysis studies. Any agency planning to consolidate its in-house operations or outsource its data processing services will provide the results of its analysis and planned milestones per AR 5-20, with advance coordination copy to DISC4. Any agency requiring an exception to this policy will coordinate with DISC4 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 deemed economical. TRADOC will determine the organization of processing services in the TOE force.

c. Office automation.

(1) *Office equipment.* This office equipment includes desktop personal computers, laptop computers, notebook computers, hand-held computers, and personal digital assistants. Peripheral devices include any device designed for use with PCs to facilitate data input, output, storage, transfer, or support functions such as power, security or diagnostics. System software includes software required for PCs operations, e.g., operating systems. PC office automation applications include word processing, spreadsheets, electronic mail, task management, graphics, and databases that do not require the greater computational power of workstations.

(2) *Site licenses.* Local software site licenses will be acquired based on a business case, considering the availability of Army- and MACOM-wide contracts, user requirements, economic benefit, maintenance and training requirements, piracy control and the potential to reduce the proliferation of locally unsupported products. As appropriate, DOIMs will recommend site licenses to the installation commander or local IMSC and will act as the users' representative in specifying the requirements and seeking approvals for installation-wide site licenses. Privately owned computers or equipment will not be included in site licenses without prior approval from the DISC4.

(3) *Software control.* See paragraph 5-5 for COTS software installation approvals. Users will not install new software packages, software upgrades, free software, freeware, shareware, etc., without the authorization of their systems administrator. Unauthorized software may contain harmful viruses or defects which can result in the loss of data or system failure. In addition, the use of such software may create configuration management problems, violate software copyrights or licensing agreements, or cause other difficulties.

(4) *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.

(5) *Personal Digital Assistants (PDA).* 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 will be managed and accounted for as computers.

d. 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 Executive Order 12845, Requiring Agencies to Purchase Energy Efficient Computer Equipment.

e. Standard software applications. Army activities will minimize the proliferation of software applications that provide similar sets of operational capabilities. Army activities will maximize the use of selected software applications across all forces. Selected applications will be recorded in the Army systems architecture. The following policies promote the use of standard software applications.

(1) DISC4 will provide notice to Army activities of the common/standard Army software applications/modules that are Army or OSD-approved. DISC4 will also announce 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.

(2) All organizations that represent the users (e.g., 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. TRADOC and other requirement approval authorities will seek and exploit opportunities for standardizing the use of software applications across all forces and recommend standardization opportunities to the DISC4. DISC4 will coordinate with the Army staff and MACOMs before designating base operations (BASOPS) software applications for standardized use.

(3) Software applications will not be developed or acquired which satisfy substantially the same set of operational requirements as that of approved standard applications, unless approved by the Army Systems Architect. Opportunities to eliminate duplication of development and acquisition effort will be a factor in decisions regarding software applications.

(4) COTS products or existing Government-off-the-shelf (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 system life span.

(5) Software applications will be reviewed at system milestone reviews and 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, they 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 non-local data.

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

(e) Use standard data formats as approved for use by the DOD Data Administration Program described in DOD Directive 8320.1 and chapter 4 of this regulation.

(6) Software components will be engineered for reuse in all applicable systems. Determination for software reuse will be based on cost/benefits analysis from a total Army perspective. Software reuse and plans will be assessed at program milestone reviews of the IT OIPT and ASARC per AR 70-1.

(7) The policy of total package fielding (TPF), per AR 700-142, will apply when fielding software applications to multiple MACOMs for standardized use in TDA organizations. To implement TPF 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 (e.g., communications, computer platforms, system software) are fully supportable and interoperable.

(b) IT materiel developers and gaining MACOMs/activities will coordinate the development of a materiel fielding plan (MFP) to negotiate the conditions 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 MACOM's senior IM officials. The MFP will be coordinated with MACOMs prior to scheduling or executing any fielding actions within a MACOM and in time 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 six months prior to the receipt of the new system.

(c) MFPs will be developed per DA Pamphlet 700-142, appendix F.

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

(9) IT materiel developers with responsibility for the development of a multi-MACOM software application will initiate its post-production 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 IPRs, as applicable.

(10) Software applications, whether combined with hardware or as separate end items, are subject to the same procedures regarding modifications as are 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 a specific 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.

f. Authorization and requisitioning. Automation equipment authorized in Common Table of Allowances (CTA) 50-909 and listed in Supply Bulletin (SB) 700-20, applicable MTOE, TDA, or other appropriate authorization documentation, may be requisitioned within authorized allowances without submission of any IT specific planning or acquisition documentation to HQDA. 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.

g. Property book accountability. Hardware will be accounted for by using appropriate supply regulations addressing property book accountability. Software is treated as a durable item. Although it does not require property book accountability, software will be controlled by the using organization's IMO.

h. Defense Automation Resources Management Program (DARMP). DARMP is the DOD-wide program for asset visibility, resource sharing and asset redistribution. DISA is the executive agent of DARMP for DOD. Army activities will participate in the DARMP and comply with its policies and procedures contained in the DOD Information Technology Asset Management Deskbook. The primary functions of the DARMP are to provide visibility of the DOD-wide inventory of automation assets; to redistribute excess; and to oversee DOD donation of excess IT equipment through the Federal Donation Program and DISA's Educational Institution Partnership Program (EIPP)

(1) The Defense Information Technology Management System (DITMS) provides automated support for the DARMP. DISC4 will be the Army DITMS focal point. Each CONUS MACOM will appoint a DITMS focal point and inform the DISC4. Installation Property Book Officers are designated IT asset managers. Authorization and user documentation for on-line access to DITMS is obtained by contacting the Army focal point at Web site http://www.disa.mil/cio/darmp/focalpt.html#army.

(2) Army activities in CONUS use DITMS to manage excess IT equipment. DODD 7950.1, AR 710-2 and DA Pamphlet 25-1-1 provide guidelines for reporting excess automation equipment. Prior to disposing of excess hardware or COTS software, activities will request disposition instructions from DISA's DARMP Division via DITMS. Disposition instructions may include transferring to other Government or private sector organizations, or destruction. COTS software licenses that are no longer needed for their originally acquired purpose must be reported for internal DOD redistribution screening unless redistribution is an infringement of the licensing agreement.

(3) Excess automation hardware for which the Army DITMS focal point cannot identify a DOD recipient may be made available to the nation's schools through the EIPP. The gaining organization is responsible for the cost of shipping excess equipment. This initiative supports Executive Order 12999, Educational Technology: Ensuring Opportunity for all Children in the Next Century.

(4) COTS software for which DARMP cannot identify a recipient will be destroyed at the installation where it is employed. If the vendor provides for donation to a charitable, educational or other non-profit organization, the software can be provided to such organizations through the vendor's program. COTS software subject to an upgrade is normally not eligible for redistribution. When in doubt about the licensing agreement, Army activities should consult the appropriate contracting officer.

i. 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 Section 117, Title 17 United States Code. Also see paragraph 7-8. Army's private sector service providers are subject to software copyright laws and may be required to provide written assurances of compliance.

j. Life cycle depreciation. In planning life cycle requirements and calculating economic benefits of automation IT, five years from the initial date of installation will be used as the metric for obsolescence. 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 support, or incorporation of alternative products or technologies when such changes are justifiable and cost-effective.

k. Domain specific guidance. A common set of life-cycle management policies will be used for all types of materiel systems, including all types and combinations of automation. This chapter provides guidance that is specific to automation, and that supplements or amplifies the common life-cycle management policies provided in other regulations. The policies in this chapter apply to all types of automation, including models and simulations (M&S), artificial intelligence (AI), and digitization.

(1) M&S, per AR 5-11, promulgate a unique management structure and policies that govern developing and maintaining automation within the M&S domain. M&S' unique standardization requirements, e.g., High Level Architecture (HLA), for M&S confederations, will be promulgated as a separate domain appendix in the JTA-A.

(2) Digitization is the collective name for Army programs that provide warfighters a horizontally and vertically integrated digital information network to support warfighting systems and to assure command and control decision cycle superiority. No unique regulations apply, but a unique management structure will be used to oversee and coordinate the integration of digitization activities. The Army Digitization Office (ADO) provides guidance and direction of the integration of digitization across the force.

(3) Artificial intelligence (AI) is the collective name for capabilities that perform functions normally associated with human intelligence. No unique regulations apply, but the Army will use a unique management structure for AI integration.

6–3. Telecommunications

Telecommunications provide the ability to gather and disseminate information through the transmission, emission and reception of information of any nature by audio, visual, electro-optical, or electromagnetic systems. This section pertains to data networks, telephones (including cellular), pagers, radios, satellites, facsimile, video teleconferencing, cable television, and others. These services provide the warfighter and installation users the telecommunications technology needed to achieve their operational objectives. Long-haul telecommunications are covered in Paragraph 6-4.

a. Network Management. The DOIM is responsible for the overall management of an installation's or assigned area's networks, to include those supporting DOD, DA, and MACOM initiatives.

(1) Network management incorporates all support functions associated with providing customer access to the installation classified and unclassified data, voice, and video network(s) which, in turn, are connected to remote sites, DOD enterprise networks and the Internet. Physical networking equipment includes, but is not limited to, hubs; routers; switched networking devices; asynchronous transfer mode (ATM) switches; inside and outside cable and fiber optic plant; network servers; Studio and Desktop Video Teleconferencing (DVTC) devices; Wide Area Network (WAN) and Local Area Network (LAN) connectivity items; remote dial-in configurations; and wireless networking configurations. Network management also involves the preparation, submission, and tracking of procurement actions for network-related items.

(2) Inter-installation/regional networks. Defense Information Systems Agency (DISA) manages networks external to the installation that enable installations to communicate with each other. In addition, DISA manages the hardware and software that control inter-installation telecommunications. The DOIMs will coordinate closely with DISA regarding components that affect their supported organizations

(3) Installation network management. The installation DOIM will manage the logical and physical structures of all networks on its installation including local network device hardware and software configuration, installation, testing, implementation, follow-on maintenance contracting, and problem resolution. Network management involves direct interface with DISA and other higher HQ network implementers to include DOD Enterprise networks connectivity established on the installation. Installation DOIM network management includes planning for appropriate network hardware and software technology upgrades/replacements to ensure customer demands are met. Customer coordination and support may require formal ISAs and SLAs to adequately define network management roles, responsibilities, and authorities. SLAs which include network support will, as a minimum, define configuration change procedures, support requirements, escalation procedures, and security management procedures; and where appropriate, address reimbursement for service above existing levels of support.

(4) 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 include: file server management which includes operating systems; application software interfacing; metering and virus scanning software; server backup; contingency planning and disaster recovery for managed LANs; and providing technical assistance to functional system administrators who provide support from their servers to their end-user workstations.

(5) Network management information sharing. Network managers will work together to support the warfighter and all operational contingencies. Network management "lessons learned" and innovative ideas will be shared among all network managers through e-mail, online bulletin boards, and World Wide Web pages. At a minimum, network management information will be shared between all parties of an ISA or SLA. The resolution of reported problems will

be shared with all impacted to avoid future occurrences of the circumstances. Network management information will also be shared with the MACOM DCSIM.

b. 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 will be the preferred telecommunications means for command and control users. However, if DSN cannot be used in a timely manner, or if the called party does not have access to DSN service, other long-distance calling means may be used. The Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6215.01 provides the policies for DSN on- and off-net calling.

(2) *Federal Telecommunications System (FTS 2000/2001).* FTS will be used for non-command and control administrative voice services instead of the Defense Switched Network (DSN). 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.

(3) *International Direct Distance Dialing (ID3).* ID3 service will be used for non-command and control administrative international voice services instead of the Defense Switched Network (DSN). However, use of this service is not compulsory.

(4) *Defense Metropolitan Area Telephone System (DMATS).* The DMATS provides consolidated nonsecure voice and dial-up switching telecommunications service to its subscribers. Telephone service from the DMATS is provided on a full-cost or fair-market value recovery basis. Unless specifically exempted by the DISC4, all Army subscribers currently assigned to a DMATS will obtain their telephone equipment and service through the DMATS, to include common user services considered appropriate by the DMATS manager. In DMATS, centralized attendants will not be used to manually pass calls that the subscribers can access by direct dial, provided the system has a means whereby the local telephone managers can control telephone abuse, such as user reports rendered from an automated central accounting system. If practical, telecommunications service authorizations will be processed by the local office of acquisition. If practical, financial activities of the DMATS will be processed by the local accounting and finance office. Tactical telephone equipment and facilities in command posts or emergency action centers are not included in the coverage of this section.

(5) *Telecommunications services in the National Capitol Region (NCR).* The Telephone Management Project Office (TEMPO), 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.

c. 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). 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 telephone lines accessing central offices, toll trunks (local, FTS, international), DSN, and Government telephone systems/services (i.e., 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) 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 will normally not be subdivided. Class C telephone lines are for transacting official Government business on Army installations. Class C service does not provide direct-dial access to off-base trunk lines (toll trunks (FTS or commercial, international or DSN). Class C 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. Class D service will normally be subdivided as follows:

(a) Class D1. Fire alarm service.

(b) Class D2. Security alarms (JCIDS or ICIDS) and camera circuits.

(c) Class D3. Other special services/alarms. (Data circuits, energy management circuits, special circuits, etc.)

(4) *Unofficial telephone service-Class B.* The subscriber pays all charges associated with this service according to 10 US Code (USC) 2481, DOD criteria, and this regulation. Class B service is only provided 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 these categories:

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

(b) Class B2. Telephone lines at a military location for activities such as public schools, ARC, motion picture services, exchanges, credit unions, noncommissioned officers' and officers' open messes, Boy Scouts, Girl Scouts, nurseries, thrift shops, commercial contractors, service clubs, concessionaires, and other businesses operating on behalf of DOD if they are on or near a DOD installation.

d. Requesting telephone and telephone-related service.

(1) Unless exempted, DOIMs will request a Communications Service Authorization (CSA) be awarded through the USASC in areas where the local public utility commission requires tariffed or regulated services (for example, central office trunking, business lines, Foreign Exchange (FX) service.) The CSA will be based upon competitive bids for tariffed service from all interested service providers in the local area. For untariffed and unregulated services, competitive bids must be obtained through the USASC. USASC will determine whether a CSA will be initiated or modified and whether a competitive bid will be required.

(2) DD Form 1367 (Commercial Communications Work Order (CCWO)) will be placed against an existing competitively awarded Communications Service Authorization (CSA) when acquiring tariffed telecommunications services. The limit for each DD Form 1367 will be based upon the current limit for micro-purchases. The current limit is $2,500.00 per purchase. However, any contracting office is authorized to award a CSA for tariffed telecommunications services exempted by USASC. Because the Federal Acquisition Regulation (FAR) specifies that only a warranted contracting officer can obligate the Government, any DD Form 1367 must be preceded by a modification through the contract office that awarded the original CSA.

e. Long distance calling.

(1) Callers will place long-distance telephone calls directly, without assistance from the post switchboard operator (i.e., direct dial capability), when telephone switching systems have either a call detail reporting capability or an automatic telephone number call data identification system.

(2) Callers at Army installations without either a call detail reporting capability or an automatic identification system must use some type of locally developed control and accounting system to manage use of the 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) Defense Switched Network (DSN). See 6-3.b(1) above.

(5) FTS-2000/FTS-2001 and International Direct Distance Dialing (ID3). See 6-3.b(2) and (3) above.

(6) A flat rate, long-distance, non-reimbursable telephone service may be provided to tenants authorized Class A service, as a BASOPS service, if the host installation also uses this service. When the host installation does not require flat-rate long-distance service, such a service is a special requirement and the tenant must pay for it.

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

f. Billing for telephone services.

(1) *Verifying Bills.* Federal statutes require the Secretary of the Army 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 a 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 (example repetitive one-time service bills for installation, removal, or relocation of instruments) as official.

(2) *FTS-2000 and ID3 verification.* The DOIM will use a judgment sampling to verify bills for FTS-2000 and ID3. The General Service Administration (GSA) is the Government's contracting agency for FTS-2000 and the ID3. The DOIM will credit the amount collected to the account that originally paid the bill.

(3) *Billing and paying.* 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 a tariff or contract does not show a due date.

g. Use of calling cards includes credit cards and International Direct Distance Dialing.

(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, fraudulent and unofficial use.

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

h. Official telecommunications (e.g., Voice (Telephone), Data, and Video) services in personal quarters. Official voice, data, and video service is authorized for key personnel whose duties require immediate response or have a direct bearing on the timely execution of critical actions. Key personnel will be designated based on functional position and mission impact. Official service installed in quarters of key personnel will meet, as a minimum, the following conditions and arrangements:

(1) 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 (i.e., 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 Government official business for command and control or tactical purposes except as specified in paragraph 6-1d.

(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) The installation commander has the authority to approve and administer the installation and use of official telecommunications service within cited restrictions and to designate personnel who occupy key official positions. This authority will not be delegated. The servicing DOIM will maintain on file written approval from the installation commander for each individual authorized official service in their quarters. This approval will be retained for as long as the service is installed.

i. Single line service. The Army subscribes to the single-line telephone concept and minimized retention of key systems. The standard single line telephone is the Dual Tone Multiple Frequency (DTMF), type 2500/2554. Key telephone systems may be used until the installation infrastructure is available to support the single line concept. The DOIM will certify the requirement of every key system due to limited infrastructure. This certification will remain on file until the key system is removed and single line service installed. The DOIM will revalidate the need for each key system every five (5) years. Key systems will normally only be installed in command or administrative areas at the battalion level (or equivalent) and above.

j. Secure Telephone Unit (STU) and Secure Telephone Equipment (STE). Secure phones are critical to most agencies and units, and should be used as needed to assure voice and data communications security. STU/STE can be used with International Maritime Satellites (INMARSAT), PC's, and unclassified fax machines to provide security that is not present in those unsecured devices.

(1) STU/STE may not be left operating in unattended environments except for specific circumstances allowed by AR 380-40 (i.e., approved vaults and SCIFs).

(2) Earlier STU-III phones are now being complemented by STU-1900/1910 versions. STU-1900's are voice STE and STU-1910's are data-only STE without keyboards or handsets.

(3) Only NSA-approved secure cellular telephone adapters will be used to encrypt data from portable computers through any cellular telephone network. Commercial cellular phones, alleged to be secure, are not authorized for classified or sensitive communications. NSA-approved adapters will be used for secure voice cellular telephone service. Tactical units will use the Army's Tactical Cellular Phone network in lieu of commercial devices.

k. When voice mail service is used, it will be installed as part of a dial central office switch. Stand-alone voice mail service or voice mail service attached to key systems will no longer be authorized and existing systems will be phased out of service. Voice mail will be considered a special service. MACOMs and DOIMs will determine if the service will be reimbursed by the using units/activities and the rate of reimbursement.

l. Automated service attendant. MACOMs and DOIMs 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 MACOM.

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

n. Telecommunications services for specific installation activities.

(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 base operations (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.

(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.

(3) *Reserve Officer Training Corps (ROTC).* Local voice and data services for senior and junior ROTC detachments are normally provided by the supported education institution. The supporting area DOIM may approve requests from

detachments to reimburse the supporting education institution for long distance service provided funding is available for these services. Also, the supporting DOIM may approve requests for special services, to include local telephone company service, FTS-2000 service, toll-free service, calling card service, and on/off net service from a nearby Army post. All special services will be subject to reimbursement by the requesting ROTC detachment. All available services, including FTS-2000, and equivalent service, should be considered prior to approving commercial service Direct Distance Dialing (DDD).

(4) *Army morale, welfare, and recreation (MWR) programs and nonappropriated funded 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 non-reimbursable basis for the conduct of Executive Control and Essential Command Supervision (ECECS) and Command and Control/Management functions, providing 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 plant will be provided per paragraph 6-3p(1) on an as-needed basis. Access to other data services may be provided if the capacity exists and it does not inhibit Army command and control functions. If the existing telecommunications and network systems do not have the capacity to allow MWR traffic, MACOMs and DOIMs will plan for 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.

(5) *Defense commissary stores.* 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. Class A-4 telephone service is installed in locations where only cashier personnel have access to the service.

(c) 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.

(d) 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. This agreement may be between the DOIM and the commissary officer or the area commissary field director, depending on the source of reimbursement.

(e) Official common user communications services are authorized for use by commissary stores overseas, including Alaska, Puerto Rico, Hawaii and Panama, on a non-reimbursable basis.

(f) If the existing telecommunications and network systems do not have the capacity or would otherwise be adversely impacted by DCS 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 DCS facilities.

(6) *Army and Air Force Exchange Services (AAFES).* AAFES Headquarters, 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 non-reimbursable basis for the conduct of command management functions which constitute official business. 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, which require data transfer. This is on an as-needed basis, provided the capacity exists and it does not inhibit Army command and control 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.

(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 will normally only be provided proximity access to intra-post class C service necessary for coordinating local support and for fire and safety reasons. Contractors will not normally 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 appropriated fund type support may receive official 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 if tariff rates are excessive, 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 give official Government telephone calling cards to contractors. The procedures for authorizing, controlling, and recording long-distance service also apply to official collect telephone calls that contractor personnel place or receive.

(e) The agency funding the contract reimburses the host installation for telephone charges that the contractor incurs. CJCSI 6215.01 provides guidance on when U.S. civilian contractor personnel can use the DSN.

(8) *Field Operating Activities (FOA).* FOAs located on an Army installation, or through mutual agreement when stationed nearby, may be provided the following telephone services:

(a) Class A-1 service, when the FOA is performing a military function, to include medical.

(b) Class A-2 service, when the FOA is performing a civil works function.

(c) A mix of class A-1 and A-2 service when the FOA is performing both a military and a civil works function. The distribution of type of service is mutually determined at the local level.

(d) Access to data services and networks are furnished FOA provided the capacity exists and it does not inhibit Army command and control functions already on the network.

(9) *Department of Defense Dependent Schools (DODDS).* Provide Class A2 and Class C telephone service to Government operated school facilities of military dependents on an Army installation. Access to other voice and data services is dependent upon local agreements.

(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.

(11) *Army lodging TDY facilities.* The Comptroller General has ruled that "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:

(a) Host MACOMs will 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) MACOMs may authorize direct access 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) When providing telephone service to transient personnel, undertake the responsibilities detailed in the Telephone Operator Consumer Service Improvement Act (Public Law 101-435, codified in 47 USC 226).

(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 unless the installation DOIM approves a higher class of service or special features.

(13) *Private telephone service for hospital patients.* The hospital administrator will coordinate with the installation DOIM for infrastructure in order for the local telephone company to provide private unofficial telephone service to hospital patients who request it. 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.

(14) *Nonprofit organizations.* The commander or commanding officer who exercises command authority or the military officer or appropriate Department of the Army 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.

(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.

(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.

(17) *Civilian post offices on military installations.* When requested, provide reimbursable voice and data service to on-base civilian post offices, branches, or stations. The extent of services is dependent upon local agreements.

(18) *Soldiers in the barracks.* All private telephone service for soldiers in the barracks will be through AAFES. MACOMs and installations will not establish telephone service for soldiers in the barracks outside of the AAFES contract. Access to other voice and data services is dependent upon local agreements.

(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 (e.g. DSN, FTS-2000, and ID3) through local operations centers or installation telephone operators and as long as such communications support the appropriated fund command support functions. 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.

o. Pay (coinless or coinbox) telephones. Contracting for pay telephone service will use NAF procedures and contractor fee payments per these contracts are NAFs and will be paid to the NAF instrumentality. AAFES is the sole activity authorized to contract for pay telephone and other unofficial telecommunications requirements, e.g., barracks telephone, cellular telephone, internet, telephone calling cards. Any requirements for such unofficial telecommunications services will be referred through command channels to HQ, AAFES, for appropriate contracting action. Per the MOA, contractor fee payments to AAFES are shared through the Army MWR Fund with local installation MWR funds.

p. Data networking. To support its mission and organization, the Army's infrastructure of networks must provide a robust foundation of telecommunications capabilities for implementing common network services (e.g., e-mail) and mission specific applications. Network infrastructures must enable IT insertion to support new applications.

(1) Army activities will use installation-wide networks (sometimes called campus area networks or metropolitan area networks) and local area networks to interconnect their computers as required to efficiently execute mission requirements. No further justification beyond this policy is required to gain approval for connectivity. However, subject to the guidance in the AEA, chapter 4, networking is not mandatory. Mission requirements and trade-off factors, e.g., high cost, security, mobility, will be used to decide specific requirements implementation.

(2) Networks will be installed and managed using a common user approach that can provide bandwidth on demand, rather than the stovepipe approach that dedicates an asset to one application or set of users. Installation commanders and activity heads will determine local policies, procedures and responsibilities for managing the devices that constitute the common user and specific functional user portions of local area networks.

(3) As DOIMs determine necessary, they will analyze alternatives for implementing common user network capabilities and recommend the required system architecture to their installation commanders. DOIMs will implement and maintain common user network segments as funded by the installation commander.

(4) IT materiel developers will coordinate with appropriate levels of information management activities concerning insertion of their systems into local networking environments to ensure interoperability at the required level for executing the operational concept. Refer to paragraph 6-2e(7) for guidance.

(5) A continuous contractual source of network devices will be made available to information managers and materiel developers. The assigned contract manager will ensure the available devices remain technologically current and interoperable with devices used by centralized Army programs for network modernization. Use of centralized contracts by installations and activities is a business decision that must consider required capabilities and services, cost, and schedule against the benefits offered by existing contracts.

q. Electronic mail (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, down to the secretary/clerical level, as required, to efficiently execute mission requirements. No further justification beyond this policy is required to gain approval for e-mail or other electronic services.

(2) Public Key Infrastructure (PKI) will be used for e-mail transmissions in unclassified environments within the Department of Defense when it becomes available. The standard DOD PKI will be used to digitally sign and encrypt e-mail messages that are created and sent from any Department of Army e-mail system other than the Defense Message System (DMS). E-mail applications, to include Web mail applications, will support both digital signature and encryption services, contingent upon advances in browser-based e-mail technology to support this requirement.

(3) Soldiers, civilians, and contractors who are authorized e-mail accounts in the Defense network are required to also have Army Knowledge Online (AKO) Web mail. To register, log on to https://www.us.army.mil. Follow the instructions under "I'm A New User." 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.

(4) 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. See also paragraph 6–3*p* above for related direction on the common user approach to managing bandwidth.

(5) 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. The practice of posting documents to a Web site is preferable to distributing documents by e-mail to a large number of people. Install access-control mechanisms, as required. See paragraph 6–3*r* below for prohibitions on posting information on public Web sites.

(6) 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. Commanders/activity heads 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 points of contact will manage the office's organizational e-mail account 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.

(7) 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.

(8) 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.

(9) Refer to paragraph 6-4f for policy on Defense Message System (DMS).

r. 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 can 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. In addition, the following Army policies apply:

(1) Access to all forms of nets is authorized for all personnel as deemed reasonable by respective managers. Access may be implemented without further justification than this regulation.

(2) The AKO at www.us.army.mil is the primary portal for Army unclassified intranets and the NIPRNET. The AKO-S is the primary portal for classified intranets and the SIPRNET.

(a) As of July 2002, Army Web-enabled business applications will 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) 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.

(3) FORSCOM (Army Signal Command) manages the ".army.mil" Web site assignment of sub-domains requested by other Army organizations. FORSCOM promulgates procedures for Army sub-domain 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 PAO, and other appropriate designee(s) (for example, command counsel, force protection, intelligence, etc.) have properly cleared information posted to the WWW. 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 B, paragraph B–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 or restricted distribution information.

(b) For Official Use Only (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 but unclassified information such as proprietary information, pre-decisional documents, and information that must be protected under legal conditions such as the Privacy Act.

(e) FOIA exempt information. This includes a prohibition of lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization or office in the Department of Army. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties, such as flag/general officers and senior executives, public affairs officers, or other personnel designated as official command spokespersons, is permitted.

(f) Draft publications. See also paragraph 9–2.

(5) The Army CIO will provide policies, procedures, and format conventions for Web sites and will promulgate such guidance in this regulation and on the Army Web site 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 register the site with the Government Information Locator Service (GILS) at http://sites.defenselink.mil/. GILS is used to identify public information resources throughout the U.S. Federal Government.

(8) Organizations maintaining private Web sites (for example, intranets, extranets) must register them with the Army Networks and Systems Operations Center (ANSOC) and assure that the Secure Sockets Layer (SSL) is enabled and that PKI encryption certificates are loaded. PKI Web server certificates may be obtained from the Army Network Systems Operations Center (ANSOC), Army Signal Command (ASC) of U.S. Army Forces Command (FORSCOM).

(a) All Web applications will support client authentication to the applicable private Web server at a minimum.

(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 that is 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 limiting access to link(s) to limited access site(s) (and not the information resources).

(9) Every Army organization that maintains a public Web site must observe Federal, Defense, and Army policies on protecting personal privacy on official Army Web sites and 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 non-user identifying information may be gathered for the purposes of assessing usefulness of information, determining technical design specifications, and identifying system performance or problem areas.

(c) Persistent "cookies," that is, those cookies that can be used to track users over time and across different Web sites to collect personal information, are prohibited. The use of any other automated means to collect personally identifying information without the express permission of the user is prohibited. Requests for exceptions must be forwarded to the Army CIO.

(d) Third party cookies will be identified and purged from official Web sites.

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

(11) Possible risks must be judged and weighed against potential benefits prior to posting any Army information on the WWW. (See also para 5–10.)

(12) Web masters/maintainers will provide a re-direct 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. Refer to section 508 standards on Web-based, Intranet, and Internet information and applications at http://www.section508.gov/. This site offers free online training to assist Web

developers in how to design Web sites for 508 compliance. See also paragraph 6-1*i* on information access for the handicapped.

(14) Web sites published by Army commands but hosted on commercial servers (servers other than "army.mil") are considered official sites and remain 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 informational needs of personnel and their families, mission-related needs, and public communications and community relations objectives.

s. Internet Service Providers (ISP). The only authorized access from DOD computers, systems, and networks to the Internet is via the NIPRNet. Any Army computer, system, or network that accesses the NIPRNet must receive access to the Internet only via Army or DOD-owned circuits that connect to the Internet through Defense Information Systems Agency (DISA) controlled NIPRNet gateways. Select situations may exist where organizations connected to the NIPRNet also may require direct connection to the Internet, e.g., through an ISP. However, these situations must be protected per OSD security requirements. Additionally, the organization must submit a waiver request for validation by HQDA (SAIS-IAS), which then transmits the waiver request to the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) for final approval. The DSAWG represents the DISN Designated Approving Authorities and is the OSD approval authority. (See Web site http://cap.nipr.mil for additional information).

(1) Army organizations may acquire commercial Internet service, e.g., 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. Organizations must also make these "stand-alone" ISP connections known to HQDA and OSD via the waiver process.

(2) Internet connections for educational (off duty or non duty related) or morale, welfare, and recreational 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 (e.g., for communicating with family support groups in the sustaining base) using unit funds established and managed per AR 215-1, Section IV. AR 215-4 governs IT supplies and services acquired with NAF. Such use will be coordinated with the supporting Signal unit(s) or other designated communications unit.

(3) If due to mission requirements, local Internet access is not available, unit commanders may authorize the use of unit funds (NAF) to establish ISP accounts per OSD 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 (e.g., key command personnel with a genuine need for service at any/all hours, etc) and OSD guidelines are adhered to.

(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).

t. Video teleconferencing (VTC). This policy applies to all Army VTC activities and capabilities (including videophones, desktop, and PC-based devices). VTC facilities will be managed by the installation DOIM, unless otherwise determined by the installation commander. The MACOM DCSIM is responsible for VTC policy, procedures and guidelines. The DOIM or other designate will approve all VTC systems. All items will meet FIPS 178 standards and DISA policies. 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 a command responsibility. 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.

(1) VTC fixed (permanent) facilities costing over the OPA threshold will be validated by the requesting DOIM, approved by the chain of command, prioritized by the MACOM/FOA Commander, and funded by ODISC4. VTC investment items are DA-controlled with a cost threshold established by Congress.

(2) DOIMs will plan for expense and investment VTC systems to meet their current and projected needs. Requirements for investment equipment will be developed and forwarded annually, along with the requirement identified in paragraph 6-3 above, by each DOIM. This plan 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 MACOM/FOA Program Objective Memorandum (POM) submissions to MDEP MU1M. All requirements for VTC systems (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). See DA Pamphlet 25-91 for instructions on form completion.

(3) Video teleconferencing program. The 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 1st quarter of each FY for the next FY. As functional proponent for the VTC program, the ODISC4 establishes acquisition priority numbers for all investment VTC systems.

u. 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 Army Regulation (i.e., AR 380-53 and AR 380-19 for information systems security monitoring; AR 190-53 for law enforcement purposes; AR 380-10 for electronic surveillance; AR 381-14 for technical counterintelligence; and AR 381-3 for signals intelligence. 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. Unauthorized use of DOD computer systems may subject users to administrative, criminal, or other adverse action.

v. 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 a telephone/ information systems directory at least annually. When the telephone exchange serves several installations, the main installation publishes the directory and includes listing for the sub-installations. Installations may publish directories separately, as a subsection of the local community telephone directory (published by the local telephone company) or as a subsection of a local installation guide (published by public affairs office). Directories will contain the mandatory warning banner per AR 380-53 and AR 380-19. 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 may also be placed on an Army Intranet or the WWW, per Army WWW guidance and MACOM and local procedures for the public release of the information in the specific directory. See also paragraph 6-3r.

(2) *Releasing telephone/information systems directories to the public.* All installation directories will be unclassified. Installation telephone/information systems directories may be released to contractors through the Government procuring or administrative contracting officer. Directories containing names and duty addresses of those assigned overseas, classified, sensitive, and routinely deployable units or home addresses and telephone numbers will not be released to the public or placed on an unrestricted Web site. See also DA Pamphlet 25-1-1 for further guidance on format and content of directories.

w. 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 non-appropriated fund instrumentality (NAFI) to be the franchising authority. Overall staff management of CATV is the responsibility of the DISC4 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 Morale, Welfare and Recreation 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 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 Federal Acquisition Regulation 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) are 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 (CI) 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 Public Affairs Officer 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 (CCTV), cable television (CATV), or other systems for internal public affairs purposes.

x. Master Antenna Television (M/CATV) systems. Existing Government-owned Master Antenna Television (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 nonappropriated fund activities or individual persons is not authorized unless such M/CATV expenditures are justified under provisions of AR 415-15.

y. Commercial Satellite Television Services (CSTS) 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.

z. Global Broadcast Service (GBS) will provide a CINC-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 command and control, and intelligence dissemination, the GBS also serves to deliver training and morale/welfare information services. Such services include the Armed Forces Radio and Television System, commercial cable news/weather services and other desired broadcast services for deployed units. User reception of broadcast information will be issued via GBS receiver terminals.

aa. Other telecommunications devices. Commanders and IT organizations at all levels of the Army are empowered to employ telecommunications devices consistent with mission requirements, security considerations, operational constraints and funding. DOIMs must apply sound principles of security, operational necessity and management controls to the provision of other IT used for communications.

(1) *Portable, mobile, and cellular telephones.* These types of telephones will not be used in lieu of established "wired" telecommunications networks. These devices are to be used for official business only and may be approved for handheld portable use and/or installed in Government vehicles. 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. Cellular telephones without encryption provide no privacy or security and are easily monitored by third parties. MACOM 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 periodically to identify and switch to plans that cover the organization's needs at the lowest overall cost. DOIMs will work with cellular telephone service providers to implement use of Personal Identification Numbers (PINs) for each account holder. 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 (a prime indicator that cellular telephone integrity has been compromised). For maximum security, DOIMs need to look at digital technology to replace older analog cellular telephones as digital cellular telephone coverage expands to all of CONUS, Hawaii and Alaska.

(a) Examples of appropriate applications for these telephones are as follows:

1. Emergency management and emergency restoration situations which may be required as fixed station back up to an external or internal telephone system experiencing difficulties.

2. Specifically designated projects and/or mission unique requirement, e.g., work being performed in geographically remote areas, or work where continuous communication is required.

3. When safety of personnel, unit or organization security considerations are paramount.

4. When placed in Fly-Away or Drive-Away kits/sets for contingency purposes.

(b) Cellular telephones have proven useful during emergencies, but should not be considered a total or primary

solution to emergency communications requirements due to inherent vulnerabilities and limitations of cellular technology. Examples of such vulnerabilities are as follows:

1. Damage to or displacement of cells (the actual broadcast/rebroadcast towers and systems that are the underlying enabling support for this technology).

2. Cellular system overload, and/or overloading of the Public Switched Network.

3. Analog-type cellular telephones numbers can be intercepted by simple scanners and resold on the black market for use by persons seeking to avoid paying long-distance toll charges.

4. Cellular telephones may be used with PCMCIA data adapters; greatly enhancing the ability of remote or mobile users to pass data files to/from home stations. However, the adapters do not provide any security or encryption. Users need to be educated to prevent security violations.

5. Geographic limitations on areas served and signal strength.

(c) Tactical units. Tactical units will use only the Army's tactical cell systems, which are encrypted for security.

(2) *Beepers and/or pagers.* When beeper/pager functions are part of the features of a cellular telephone, the item will be managed the same as a cellular telephone. (See paragraph 6-3aa(1).) Unit commanders in conjunction with the supporting DOIM will determine the most economical service type based upon mission requirements. Beepers/pagers will be authorized service based upon the following service areas.

(a) Local. The area directly adjunct to an Army installation for facility.

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

(c) Continental United States (CONUS). The geographical region of the CONUS.

(d) World-Wide. The service will reach any country in the world.

(3) *Facsimile (Fax) Machines.* Plain paper faxes will be used to the maximum extent practicable. Since quality fax machines cost as much as desktop PCs, information managers will pro-actively seek solutions, such as integrated fax servers, that maximize service to customers while minimizing costs. Further, efforts should be made in conjunction with users to reduce or eliminate the need for hard copy materials, with fax servers and other means (such as Internet and Intranet homepages) applied to this end. 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.

(4) *International Maritime Satellite (INMARSAT).* This technology is a commercial international satellite system owned and operated by a consortium of 82 member countries. It provides global mobile satellite communications for commercial, emergency, and safety applications on land, at sea, and in the air. COMSAT is a private US corporation designated by law as the US representative within the INMARSAT consortium membership. COMSAT is the exclusive US source of access to INMARSAT services for voice, fax, and data transmission. By international treaty, INMARSAT use is limited to uses "exclusively for peaceful purposes." Army's use of INMARSAT is allowable for emergency communications in support of disaster relief, humanitarian, and peacekeeping missions. COMSAT, a regulated monopoly, operates as a consortium sanctioned by global governmental agreements. The use of INMARSAT terminals in any theater of operation will be guided by the policy of the theater Commander in Chief of Unified or Specified Command (CINC). Primary communications should be via DISA/Joint/CINC/Army networks and devices, with INMARSAT filling voids when primary communications providers are not available.

(a) Procurement of INMARSAT equipment. MACOMs/DOIMs are responsible to fund INMARSAT terminal acquisition and airtime. MACOMs/DOIMs will submit their requirements to DCSOPS, ATTN: DAMO-FDR, for approval. MACOMs/DOIMs will submit a Request for Service (RFS) to Defense Information Technology Contracting Office (DITCO) for acquisition and airtime. MACOMs/DOIMs are responsible for arranging the commissioning of Army INMARSAT terminals into satellite access operation by arrangement through the US Army Communications-Electronics Services Office (USACESO). USACESO, an element of HQDA ODISC4, is the only designated Army office authorized by HQDA to coordinate commissioning of terminals directly with COMSAT.

(b) Operation of INMARSAT equipment. MACOMs/J-6/G-6's will ensure field operators configure INMARSAT units to a COMSAT Land Earth Station (LES). MACOMs/J-6/G-6 may use INMARSAT terminals during deployments and exercises. Upon the establishment of communications by the supporting signal unit's, INMARSAT terminals will become a backup means for communications. MACOMs/J-6/G-6's will ensure National Security Agency approved or endorsed encryption devices are used when required by the Commander in Chief (CINC) responsible for the theater of operations. MACOMs/J-6/G-6's will ensure INMARSAT terminals are not used for personal phone calls except in cases of emergency where commanders determine it is in the best interest of the military to do so. Personal calls are to be made on commercial telephone systems or the Military Affiliated Radio Service (MARS) high frequency radio equipment provided for this purpose.

(c) Equipment readiness. MACOMs/J-6/G-6s are responsible for testing INMARSAT terminals to ensure devices are in proper working order. Diagnostics test will be performed in accordance with operator's manual.

ab. Army management of electromagnetic spectrum. AR 5-12 governs Army-wide spectrum management. The DISC4 designates the Army Spectrum Manager, who is responsible for promulgating spectrum policy and planning guidance for Army operations, training and acquisition.

ac. Radio System Support Services.

(1) Requirements for entry into existing networks will be identified to the installation DOIM. Installation support

radio comprises non-tactical, user-operated, radio-networks, systems, facilities, equipment, and information services required supporting host and tenanting 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 system support services will be justified based upon operational necessities and on economic analysis. Commercial off-the-shelf equipment available on contracts negotiated by AMC 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 380-19. See also chapter 5 of this regulation.

(3) Military Affiliate Radio System (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.

(4) Amateur and citizen band radio operations are addressed in AR 105-70.

ad. Leasing of Government-owned telecommunications assets. 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 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.

(1) Compensation paid by telephone/radio companies for lease of any Government-owned appropriated-funded facilities (cable pairs, equipment, manholes, antenna space, etc.) will be in the form of a check payable to the FAO and may not be used to support NAF activities. Terms of the reciprocal lease agreement will provide that the Government may, according to its needs, reacquire any leased asset.

(2) The revenue from the lease of non-appropriated funded telecommunications assets will be deposited into the NAF activity's fund.

(3) 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.

(4) OCONUS leasing activities will follow this practice in negotiating for new or in revising existing services or facility leases and in negotiating new or re-negotiating 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.

(5) Existing leases, status of forces, or other pertinent intergovernmental agreements need not be re-negotiated for the sole purpose of compliance with this policy.

6–4. Long-haul and deployable communications

This section provides Army policies on the use of long-haul communications, or 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 non-secure data, voice and video information.

(1) All Army activities requiring telecommunications services will use the DISN when those services are available and are technically and economically feasible to the Army. Requirements will be processed per DODI 4640.14 and the supporting Army activity's procedures.

(2) Army activities will continuously assess the impact of mission and operational concepts on their long-haul communications requirements. Army activities that require long-haul common-user services will submit validated requirements to DISA for DISN planning purposes. DOIMs will validate operational requirements before requesting connection approval from DISA to ensure DISN is the best solution for the requirements considering the bandwidth, security, connectivity and other technical issues. An interservice support agreement (ISA) with associated service level agreement (SLA) should be negotiated between DISA and the installation DOIM to ensure both understand their roles and responsibilities to provide end-to-end customer communication capabilities. See Para 6-1 on support agreements.

(3) MACOMs and Army activities will:

(a) Review long-haul common-user transmission requirements and forward all requirements not needing unified and specified command, Joint Staff, or OSD approval to DISA 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 CINC, requirements for service with the information prescribed in DISAC 310-13-4.

(c) Program, budget, fund, and provide support for assigned portions of the DISN through the PPBES, including approved contractor and foreign Government systems.

(d) Provide sufficient local distribution capability to meet the CINC's 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 meet the requirements of 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 unified command. Conflicting views among the requesting activity, DISA, and the concerned commander of a unified command 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. Army MACOMs and activities will provide representatives to joint, 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 (POPs) located on their respective posts, installations, or equivalent.

(j) Manage DISN subnetworks when authorized by the Director, J-6, Joint Staff.

(k) Provide information, as requested, to DISC4 and DISA for billing, management and inventory purposes.

(l) Identify representatives to the DISN requirements committee and its subcommittees, as required.

b. Defense Switched Network (DSN). DSN is the DOD preferred means of providing voice communications for command and control.

(1) DSN may be used to transmit unclassified facsimile traffic without a STU-III.

(2) Defense Red Switch Network (DRSN) services.

(a) The CINCs 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 for the DRSN logistics support, sustainment, training, DRSN-related equipment and special interface trunks as may be required by the CINC or supported command for which they are responsible.

(b) Unique requirements will be forwarded through the MACOM to HQDA, ODISC4, ATTN: SAIS-PAC for coordination and validation. 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 ODISC4 before approval of funding availability will be certified.

c. Federal Telecommunications System-2000/2001 (FTS-2000/2001). FTS-2000/FTS-2001 is the preferred network for administrative long distance voice communications in CONUS.

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 C4ISR structure that includes the C4ISR architectures and systems of the CINCs, and Defense agencies. Army SATCOM terminal systems include military developed and acquired terminal systems (including Army-owned commercial off-the-shelf (COTS) terminals (such as INMARSAT terminals and Iridium handsets). SATCOM systems are considered a constrained resource of the DOD. Access to SATCOM systems is based on CJCS-validated and prioritized requirements, approved priorities for day-to-day operations for the execution of operational plans, and as directed by the CJCS and National Command Authority.

(2) The CJCSI 6250.01 establishes operational policy and procedures and provides guidance for the planning, management, employment, and use of SATCOM systems. The space segments of all SATCOM systems are controlled as joint assets to meet CJCS approved requirements. Joint Staff certification, through the Joint Interoperability Test Center (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 CJCS approved requirement.

(a) Army is assigned Planning, Programming, and Budgeting System (PPBS) responsibility for the payload and network control systems of the Defense Satellite Communications System, the Wideband Gapfiller System, and the Advanced Wideband System.

(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 Global Broadcast Service (GBS) Primary Injection Point (PIP) terminals).

(3) AR 70-1 and AR 71-9 govern the requirement, development, and acquisition of Army SATCOM Systems.

e. Global Positioning Services (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 JPO (Joint Program Office). Army PPS users will employ PPS user equipment incorporating both Selective Availability and Anti-spoofing features to support combat operations. The Army Acquisition Executive (AAE) can submit waiver requests to OSD for use of Standard Positioning System (SPS) user equipment in specific platforms or application categories, which do not involve combat operations and which do not require direct PPS accuracy.

(2) Except for Congressional exemptions (range instrumentation, advanced technology, mapping, Special Forces, and classified applications) the global positioning system (GPS) Joint Program Office (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 Department of Defense record messaging system. DMS is the replacement for AUTODIN. The DMS will be implemented in all environments. All Army activities that require the use of official organizational messaging will migrate to the DMS. DMS migration will be accomplished through centralized fielding by the Army DMS Project Manager.

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

(3) Refer to the Army DMS Program Management Office (PMO) Web site (http://dmsweb.belvoir.army.mil/) concerning compliance standards, certification, and waivers.

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 Chairman Joint Chiefs of Staff Instruction (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 DISC4 when unique Army specifications are a major impediment to adoption of an otherwise cost-effective allied system.

(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-those wholly owned, operated, and maintained by the U.S. Government, or U.S. commercial enterprises, or a combination thereof, to 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. needs.

i. Compatibility and Interoperability of Tactical Command, Control, Communications, and Intelligence (C3I) Systems.

(1) The Army will develop, acquire, and deploy tactical C3I systems that meet operational needs of U.S. tactical forces and are compatible/interoperable with allied tactical and non-tactical C3I systems. The goal is to develop common, interoperable systems within NATO. The number of devices necessary to achieve interoperability will be minimized by the acquisition of common 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 non-tactical C4I systems that support joint or combined operations, the J-2, Joint Staff, will assist in making defense intelligence communication acquisition requirements support military forces and achieving joint and multinational interoperability. Intelligence warfighting needs are examined for solutions and ensure compliance with DOD directives and joint directives.

(4) The J-6, Joint Staff, is the approving authority that will determine the basis for joint or combined communications system prior to initiation of system development. Duplication of development effort will be avoided. Established joint interface standards and operational procedures is the standard practice for tactical Army C4 systems. Requirements for new Army funded joint or combined tactical C4I systems will be validated by the DISC4.

(5) The basis for U.S. and Allied compatibility and interoperability of tactical C4I systems will be those agreements between the U.S., NATO countries or alliances as specified in requirements documents and Allied standardization agreements.

(6) Testing and evaluation to ensure interoperability of tactical C3I systems will be performed during the acquisition process. Test and evaluation 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 being developed. Critical issues, test objectives, and evaluation criteria related to mission needs will be established before tests begin. Developers of performance measurements (i.e., functional proponents, PMs) will use these performance measurements to ascertain performance and results-based management of C3I systems.

6–5. IT support for battlefield systems

It is Army policy to standardize its management and operational concepts and to integrate its regulatory guidance for all types of systems, specifically including IT. IT is a critical enabler for the capabilities of battlefield systems. HQDA staff proponents for all aspects of life cycle management, e.g., total package fielding, integrated logistics support, and materiel change management, will ensure IT is addressed in official guidance. Army organizations responsible for the life cycle management and operation of battlefield systems will ensure IT components are supported and managed as an integral part of systems, both on the battlefield and in garrison. The ADO oversees migration of all Army battlefield IT programs to ensure compliance with the JTA-A.

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 local DOIM will provide oversight on the IT support for MILCON. The DOIM must maintain a close and continuous coordination with the Department of Public Works (DPW) 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 for inclusion in the Corps of Engineers' statement of work for construction. If this expertise is not available, the DOIM should request MACOM assistance 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 DOIM will ensure that IT cost estimates are identified for each component supporting MILCON facilities. 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. MACOMs and separate supporting commands will ensure the IT requirements identified in the DD Form 1391 are submitted to the POM manager.

c. Host and tenant relationships. Interservice and/or interagency support agreements (ISA) will include IT support for MILCON.

d. Installation Information Infrastructure. MILCON IT requirements include information system connectivity for both voice and data.

(1) Local Area Networks (LANs) are the preferred solution to satisfy data requirements. They 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.

(3) 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 aspect of IT that pertains to the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery and multimedia, with or without sound, linear or non-linear, 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 National Command Authority, Secretary of Defense, JS, military departments, and Army commanders with combat camera (COMCAM) and record documentation, multimedia/VI products, and services to satisfy official requirements. These requirements may include, but are not limited to, support for command and control, 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. Related VI Policy and Guidance. This chapter implements National Archives and Records Administration 36, Code of Federal Regulation (CFR); American Disabilities Act of 1992; Titles 17, 18 and 44 U.S. Code; OMB Circular A-76, Performance of Commercial Activities, and Circular A-130, Management of Federal Information Resources; DODD 5040.2, Visual Information; DODD 5040.4, Joint Combat Camera Operations; DODD 5040.5, Alteration of Official DOD Imagery; and DODI 1322.20, Development and Management of Interactive Courseware (ICW) for Military Training.

c. Exclusions. The following are excluded from provisions of this chapter except as otherwise noted.

(1) All video teleconferencing (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) VI 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 Armed Forces Radio and Television Service (AFRTS). Products or productions acquired and distributed exclusively for AFRTS overseas use.

(6) VI commercial entertainment productions and equipment acquired and distributed by the Army and Air Force Exchange Service (AAFES) and the Navy Motion Picture Service (NMPS).

(7) VI 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) VI equipment and products acquired with non-appropriated funds.

(9) Organizations using still camera equipment for the purpose of generating identification or security badges.

(10) At the choice of the MACOM commander, 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 paragraph 7-12).

(11) Non-VI activities using COTS office business graphic software (such as Power Point) 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 funded civil works and non-DOD agency missions.

(14) Multimedia products developed within the printing and publications policy and procedures guidelines.

(15) VI library materials and equipment acquired for use in Army libraries.

d. 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 this regulation.

7–2. Combat camera (COMCAM)

a. Army VI COMCAM teams will be maintained to provide rapid VI support to CINCs for military operations, emergencies, and field exercises. Each MACOM, CINC, and ODISC4 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 requests and taskings. Requirements for COMCAM support will be identified to FORSCOM.

d. Corps COMCAM teams are organic to specific Corps units and will 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 Chief, Joint Staff, (CJS) and CINCs have the authority to task joint service COMCAM teams. (Also see DODD 5040.4).

f. COMCAM capabilities will be maintained by the MACOM/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 executive agent responsibilities

OSD (Public Affairs), American Forces Information Services (AFIS), Defense Visual Information (DVI) assigns JVIS responsibilities to the Military Departments to provide VI support to more than one DOD component. DISC4 will inform DOD of any proposed changes to JVIS missions, organizational structure, level of support, or funding prior to implementation. Army executive agency responsibilities are:

a. The U.S. Army VI Center (USAVIC) will provide a central capability to rent, lease, procure, or produce multimedia/VI productions in support of Army, DOD, other military department and Government agency requirements as requested. USAVIC is the only authorized Army activity to issue production procurement contracts exceeding the 49-percent limit for support services (see paragraph 7-8a(8)). USAVIC will also provide support to OSD, JS, and other Army MACOM, DOD and Federal agencies in the National Capital Region, excluding Ft. Belvoir, Virginia.

b. 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.

7–4. VI activities

a. A VI activity is any organization that 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 services or products without authorization unless separately excluded. See exclusions in paragraph 7-1c. VI activities are authorized and managed within the context of this regulation. The types of Army VI activity authorizations are at table 7-1. The MACOM/FOA VI manager, DOD, or ODISC4, as delineated in table 7-1 authorizes either the establishment, change of capability, or disestablishment of VI activities.

b. VI activities are classified as industrial operations (General Functional Area (GFA) T-807) and are subject to OMB Circular No. A-76 studies, except for VI management, combat, and combat support (combat camera) elements. Curtailment of commercial activities is appropriate to re-establish combat and combat support elements or rotational positions to support war plans.

c. Authorization. Authorized VI activities will be assigned a Department of Defense Visual Information Activity Number (DVIAN) by the MACOM VI Manager, in coordination with the U.S. Army VI Center (USAVIC), and DISC4. DA Form 5697 will be used to assign the DVIAN and to identify the VI activity's authorized capabilities. DA Form 5697 is available on the USAPA 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. These managers will maintain close liaison with the information manager (if the VI activity is not managed by the information manager) and other installation staffs to ensure timely, effective support and efficient operations. 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 its 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 Pamphlet 25-91).

f. Resourcing. All installation VI managers will plan, program and budget for future 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 capabilities for which they are resourced. Requirements above this standard level and/or support to customers will be satisfied on a reimbursable basis in accordance with current Army reimbursable policy or will be referred to the MACOM VI manager for support. The following exceptions apply:

(a) Cadet Command reimburses only for above standard level of support.

(b) Army off post customers operating under shop smart will not reimburse for military personnel file photographs, as required by AR 640-30, or the loan of training aids and devices when within the standard level of support.

(2) VI activities may be authorized to fabricate and/or manage training devices. These functions will be resourced separately.

(3) Fee-for-service or industrially funded VI activities will recover their full cost of support.

(4) VI activities will establish and maintain a list of current charges for standard products and services. All customers that pay for VI products and services will use this list of charges as a basis for payment.

(5) A TDA rotational base for TOE/MTOE (Modified Table of Organization and Equipment) COMCAM personnel will be maintained. VI military personnel will be authorized.

g. Media loans will be recorded on DA Form 4103, Visual Information Product Loan Order. DA Form 3903, Visual

Information 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 USAPA Web site and the Army Electronic Library (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.	MACOM (FOAs must be authorized by ODISC4)
		NOTE: Activities should list their specific capabilities here, e.g., still photography, motion picture, linear and/or digital video, audio recording, graphic equipment loan, maintenance, presentation support, art, VI media and/or digital photography, chemical processing, etc.)	
B	VI Production (Local)	Includes production, reproduction and distribution of local multimedia/VI productions to support an individual organization, installation or a defined geographic area.	MACOM
C	VI Production (Non-local)	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.	ODISC4
D	VI Production (Contracting)	Provides commercial contracting, purchase, or rental of VI productions.	ODISC4
E	VI Records Centers	Central management and storage facility for VI products.	OASD(PA)
F	Component Accessioning Point	Central point for VI imagery screening and for forwarding imagery to the VI Records Center	ODISC4
H	VI Documentation	Recording of technical and non-technical events.	ODISC4
		NOTE: Activities should list their specific types of VIDOC being recorded here.	
I	Product Distribution	Central VI product distribution activity.	OASD(PA)
J	VI Mgt	Includes staff functions and management and administration of VI activities.	
1	HQDA		OASD(PA)
2	MACOM or FOA		ODISC4
3	Common Spt		MACOM
4	Dedicated		MACOM
K	VI Support Center (Dedicated)	Provides VI support to a specific organization or organizational element only (also see Type A above).	ODISC4 or MACOM
		NOTE: Activities should list their specific capabilities here, e.g., 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, etc.)	
Q	Broadcast	Includes closed-circuit television support to a defined area. NOTE: Activities should specify their type of broadcast capability (e.g., CCTV, master/community antenna, command channel(s), etc.)	MACOM
R	Regional VI activities	Provides VI support to a specifically designated region. NOTE: Activities should list the specific types of regional support being provided, e.g., chemical processing, VI production (videotape and/or multimedia), etc.	ODISC4
S	Public affairs	Includes photojournalism, HQDA journalism, electronic photojournalism, and other VI media to support public affairs (command information, news gathering, and community relations) for TOE/MTOE public affairs units only.	ODISC4

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 non-profit organizations meeting on Government property will be at the discretion of the local commander.

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 standard operating procedures (SOP) which will be included as part of the customer Standard Level of Support document.

e. Procedures, reports, and formats for the management and operation of VI activities are contained in DA Pamphlet 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

Use of the Training Support Automated Management Software-Enhanced (TSAMS-E) by all VI activities is mandatory. Each VI activity will maintain TSAMS-E data for the current year plus 2 previous years (FY+2). ODISC4 is the TSAMS-E functional proponent, with FORSCOM acting as the executive agent. A Configuration Control Board (CCB), established by the Army VI Steering Committee (AVISC), will validate, approve and prioritize all requested application changes.

7–7. Equipment and systems

a. VI equipment and systems are items of a non-expendable 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), 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 of VI management. 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 must be obtained from the appropriate level of VI management. (Ref AR 25-30).

b. 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 MACOM/FOA VI manager and approved and funded by ODISC4 (MDEP MU1M). Television-Audio Support Activity (T-ASA), an OSD organization, is the item commodity manager for the acquisition of commercially available VI investment equipment. COTS, non-tactical VI equipment and systems costing $50,000 or more will be procured by the T-ASA. MACOM/FOAs may provide supplemental investment funds for the acquisition of DISC4-approved requirements. Local procurement authority may be granted by T-ASA. Expense items of equipment costing less that $50,000 may be procured locally upon approval of the MACOM/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 MACOM/FOA VI manager in a consolidated 6-year plan. This plan is the basis for establishing annual funding increments for equipment replacement. MACOM/FOA VI managers will also submit investment VI equipment requirements for inclusion in the MACOM/FOA Program Objective Memorandum (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 (RCS: CSIM-46). DA Form 5695 is available on the USAPA Web site and the Army Electronic Library (AEL) CD-ROM. See DA Pamphlet 25-91 for instruction on form completion.

(a) Type Classified Items. ODISC4 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 (GOCO) VI activities that use Government-furnished equipment will be acquired through the Visual Information Systems Program (VISP), and consistent with the terms of the contract, only to support contractor services provided to the Government.

(2) MACOM commanders may designate specific non-production, 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.

(d) User/owners will not acquire, lease or rent professional quality VI production equipment.

(e) 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 are turned in for disposal. Repair parts may be procured locally by VI managers.

(5) Maintenance of VI equipment will be performed and managed in accordance with AR 750-1, Section IX. Preventive maintenance on VI equipment will be performed in accordance with manufacturers prescribed scheduled maintenance.

d. Certification of assets.

(1) VI equipment and systems must be certified JTA-A-compliant prior to acquisition by the Army.

(2) The DISC4 is the delegation authority for certifying VI assets between $100,000 (or the OPA threshold-) and $2.5M. Equipment and systems between $100,000 and $900,000 are certified through the MACOM VI manager and DISC4, and the VI Systems Program (VISP). Proof of certification exists when a HQDA VISP acquisition priority number is assigned to a specific VI requirement.

(3) Equipment and systems under $100,000 (or the OPA threshold, whichever is higher) are certified by the MACOM commander or delegated to the MACOM VI manager. Certification authority may be delegated to the lowest level that assures 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 $100,000.

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. DISC4 is the functional proponent for the VISP. The program executor is USAVIC. Project management and engineering is the responsibility of T-ASA. (See also DA Pamphlet 25-91.)

f. Investment VI equipment and systems are normally funded with Other Procurement, Army (OPA)-2 dollars. Operations and Maintenance, Army (OMA) funds support expense items.

g. VI activities which are supported by funding other than procurement dollars, e.g., Army Industrial Funds , civil works, intelligence, etc., will procure VI equipment with those resources which support their operation. MACOM/FOA VI managers will ensure that only authorized VI activities with established DVIANs purchase VI equipment and that it is compliant with the JTA-A.

7–8. Products

a. Multimedia/VI Productions. Multimedia/VI productions are usually stand-alone, organized and unified presentations that are developed according to a plan or script. When multimedia/VI productions meet the criteria stated in this section, they will be managed per the DAVIPDP.

(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 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 (e.g., 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) Not all multimedia productions are considered VI. Productions containing predominantly textual information are considered electronic publications and are governed by printing and publishing policies.

(4) The recording, duplicating and/or use of copyrighted material in a VI production is prohibited by law (Title 17, Copyrights (1998)) unless prior permission from the copyright owner is obtained in writing. Also see paragraph 7-12d.

(5) The following VI products are exempt from the provisions of this paragraph.

(a) Graphic art, electronic and/or digital images, still photographs, motion picture photography, and video and audio recordings which are not used in multimedia/VI productions.

(b) VI report content that is obsolete within a year and is not for public release. VI reports, include technical, intelligence, maintenance reports, video reports, videos of briefings, seminars, conferences, or classroom instruction (talking heads), or commanders' messages to their troops that are for short-term immediate use and do not require life cycle management. Also see paragraph 7-8e.

(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 Department of the Army VI Production and Distribution Program (DAVIPDP).

(6) All multimedia/VI production requirements will be processed per DODD 5040.2 using DD Form 1995 (Visual Information (VI) Production Request and Report), (RCS-DD-PA (AR) 1381). See DA Pamphlet 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 Defense Automated Visual Information System (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) and other similar activities.

5. A Production Authorization Number (PAN) will be assigned to each local production. (Ref DA Pamphlet 25-91, chapter 6).

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

(b) Non-Local productions. These productions are for multi-installation, MACOM/FOA, Army or DOD-wide use.

1. These productions, regardless of cost or format (e.g., videotape or multimedia), will be certified by ODISC4.

2. Non-local productions will be assigned a Production Identification Number (PIN). A PIN register or log will be maintained to ensure control and accountability of non-local multimedia/VI productions. See DA Pamphlet 25-91 for format.

3. Joint VI Service Distribution Activity (JVISDA) will distribute these 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. Non-local multimedia/VI productions (in-house and COTS) will be reviewed by functional proponents for obsolescence within five years of their initial distribution and every three years thereafter. Multimedia/VI productions are obsolete when they no longer reflect current information and will be removed from the inventory. Obsolete multimedia/VI productions may be declared historical when they no longer reflect current policies and procedures, but accurately reflect past events that are considered historically significant. (See DA Pamphlet 25-91 for further information.)

(7) COTS productions may be procured to support the needs of an installation or individual requestor. These products will be reviewed for currency three years after purchase and every two years thereafter. Each acquisition (purchase, lease, or rental) will not exceed five copies per title, and the total cost may not exceed $2,500 or $500 per copy without MACOM/FOA VI manager approval. Acquisition of master materials or duplication rights will be processed the same as a non-local production.

(8) The DAVIPDP provides for the annual identification, funding, and acquisition of multimedia/VI production and distribution requirements. All Army organizations will identify their requirements for non-local multimedia/VI productions and forward their requests to their supporting MACOM/FOA VI manager for validation. MACOM/FOA VI managers will forward valid requirements to ODISC4 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. The ODISC4 will certify all non-local productions.

(9) $100K Review. All production requirements whose estimated production cost exceeds $100,000 will be forwarded through command channels to ODISC4 for review by AFIS/DVI. The VI manager will obtain the signature of the proponent General Officer or SES on the DD Form 1995 or by memorandum, acknowledging the production cost, prior to forwarding the requirement to DISC4. This includes all productions that are provisions of contracts for research and development of tactical systems or new equipment training materiel contracts (that is, new equipment, paper-based training, and similar costs) and mixed-media contracts.

(10) Captioning for Hearing-Impaired. In the design, development, production, presentation, and distribution of multimedia/VI productions, MACOM/FOA proponents will consider the intended audience as required by the American with Disabilities Act of 1990. All multimedia/VI productions developed for general audiences (such as, Privacy Act, AIDS, family support, drug/alcohol abuse, or equal opportunity) will be open or closed captioned for the hearing impaired. Remastering of existing multimedia/VI productions will be accomplished if requested by the proponent and funding is available. Requests and funding for remastering of productions will be submitted through MACOM/FOA VI managers to ODISC4. Production activities will provide a transcript of the "as recorded" audio with the submitted production master.

(11) 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.

(a) Functional proponents will validate requests only for multimedia/VI productions which are legitimate requirements, that are essential, and adequately defined, and for which all other prerequisites have been met.

(b) Before validating a request for production, procurement or adoption, functional proponent will review information obtained from the DAVIS/DITIS search results and reasonably available commercial production sources to determine if an acceptable product already exists or is planned or is in preparation by another DOD agency. DAVIS/DITIS subject searches are not required for classified productions.

(12) Contracting. Multimedia/VI productions will be acquired in the most cost effective manner possible. The Army will use the Federal Uniform Audiovisual Contracting System for competitive procurement of new multimedia/VI productions as prescribed by DODD 5040.2.

(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 Joint VI service activity (USAVIC Joint VI Activity). MACOMs/FOAs will use JVIS procurement contracts to procure multimedia/VI productions. (see table 7-1.)

(b) Federal Acquisition Regulation (FAR). MACOM/FOA, installation VI managers, JVIS 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 that 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 that are developed for the Army.

(c) The contracted producer of multimedia/VI productions made by a GOCO activity must be listed on the Audiovisual Qualified Producers List (QPL) managed by the AFIS/DVI.

(13) The VI production activity (for in-house production) or the DOD 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.

(14) 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.

(15) 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 OSD (PA) 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 or production or when the production contains copyrighted material.

(16) Reproduction of any Army production in whole or in part is prohibited without the approval of the proponent, MACOM/FOA VI manager, JVISDA, or DISC4. 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.

(17) Foreign Military Sales (FMS) Program. Requests for multimedia/VI productions from or on behalf of foreign sources may be approved provided that:

(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 (USASAC) for clearance.

(c) The sale of multimedia/VI productions under the Foreign Military Sales Program is covered in AR 12-8. If release to a foreign audience is questionable because of production content, the DUSA (IA) will make final determination.

(18) Actions to adopt multimedia/multimedia/VI productions of other US Government agencies (non-DOD) for Army use will be coordinated and certified in the same manner as requirements for COTS multimedia/VI productions.

(19) Audio/video play back or broadcast equipment on which classified information will be transmitted must be installed in accordance with the provisions of AR 380-19 and Federal Standard 222.

(a) Procedures for transmitting classified information are contained in AR 380-19-1.

(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.

(20) Requests to translate or rescore new non-local multimedia/VI productions into a foreign language will be processed in the same manner as all other non-local productions. Requests for rescoring or translating of existing multimedia/VI productions will be approved by DISC4 only if the requestor can provide the necessary funds to defray the cost.

(21) Productions cleared by Army and/or OSD (PA) 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.

(22) All multimedia/VI productions placed on a Web site for viewing or downloading will be validated by the functional proponent and cleared for public release prior to placement on the Web site.

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

b. Video/audio documentation. Recordings of specific types of official events as they occur, e.g., 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 paragraphs 7-9c and 7-12.

c. Images.

(1) 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.

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

(3) The alteration of official imagery by any means or for any purposes other than to establish the image as the most accurate reproduction of an event or object is prohibited. (Also see DODI 5040.5 and DA Pamphlet 25-91.)

(a) Imaging techniques common to traditional darkrooms and digital imaging stations, such as dodging, burning, color balancing, spotting, and contrast adjustment that are used to achieve the accurate reproduction of an event are not considered alterations.

(b) Photographic and video image enhancement, exploitation, and simulation techniques used in support of unique cartography; geodesy; intelligence; medical; RDT&E; and training requirements are authorized, if they do not misrepresent the subject of the original image.

(c) Images that have been duplicated and electronically altered or merged with other electronic images will:

1. Be clearly labeled or marked as such.

2. Be treated as new images and assigned a separate Visual Information Record Identification Number (VIRIN) and caption.

3. Not contain copyrighted material without written consent from the copyright holder. Evidence of this consent will be maintained throughout the life cycle of the image.

(d) The obvious masking of portions of a photographic image in support of specific security or criminal investigation requirements is authorized.

(e) The use of cropping, editing, or enlargement to selectively isolate, link, or display a portion of a photographic or video image is not considered alteration. However, cropping, editing, or image enlargement which has the effect of misrepresenting the facts or circumstances of the event or object as originally recorded constitutes a prohibited alteration.

(f) The digital conversion and compression of graphic, photographic and video images is authorized.

(g) Portions of a photographic image may be used and enhanced within a composite graphics illustration if the resulting illustration does not misrepresent the facts or circumstances of the original event recorded.

(h) Original electronic images from library (electronic clip art) files will not be changed, although electronic copies of them may be altered, or sized as needed within specific documents.

(i) Photographic and video post-production enhancement, including 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. If 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.

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

(k) Only authorized VI activities may process official military personnel file photographs. These photographs will be processed per AR 640-30 and DA Pamphlet 25-91.

d. Video reports. Recordings of official events as they occur, e.g., 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 service on a low priority. These video reports will not be reported as VI productions on the VI Annual Workload and Cost Data Report. See paragraph 7-8b, or DA Pamphlet 25-91.

e. 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 overhead transparencies, 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. DISC4 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, etc.

e. Defense Automated Visual Information System (DAVIS). The DAVIS is a DOD-wide automated catalog system for management of VI products and 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. AFIS/DVI is the data base 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) *Cable television (CATV).* The VI activity will operate only the command channel(s) that is (are) provided as part of the CATV franchise agreement. See chapter 6 of this regulation for CATV policy.

(2) *Closed circuit TV (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 non-local Army multimedia/VI productions and VI products with their associated administrative documentation are controlled as official records throughout their life cycle and disposed of per General Records Schedule 21, this regulation and DA Pamphlet 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 in keeping with the local activity's requirements. Still photographs, motion picture footage, video recordings (excluding those assigned a PAN or PIN), and audio recordings will be assigned a VIRIN before they are submitted as record material. A description of the

required VIRIN elements is provided in DA Pamphlet 25-91. All VI record material will be captioned (DD Form 2537 (Visual Information Caption Sheet)) per procedures outlined in DA Pamphlet 25-91. DD Form 2537 is available on the USAPA Web site and the Army Electronic Library (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 commonly accepted industry practices. For further information, consult the American National Standards Institute (ANSI), Inc., 11 West 42d Street, New York, NY 10036, and the Society of Motion Picture and Television Engineers (SMPTE), 595 West Hartsdale Ave, White Plains, NY 10607.

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 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 DVIC.

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

i. Non-local multimedia/VI productions will be forwarded with production folder upon completion 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). The OSD, Chairman Joint Chiefs of Staff (CJCS), HQDA, and field commands use this information for both command and control (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 these products to keep Army personnel informed and for release to the news media. The VI Documentation Program includes both tactical and non-tactical documentation.

a. Tactical Documentation. Record VI documentation 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 theWeb site http://dodimagery.afis.osd.mil. COMCAM teams will provide original source material through the JCCC to USAVIC for accessioning into the DVIC. (See DA Pamphlet 25-91.)

b. Non-Tactical documentation.

(1) Non tactical (infrastructure) documentation is record documentation of technical, operational, and historical events as they occur during peacetime. This documentation informs about people, places, and things; processes in the fields of medicine, science, logistics, RDT&E and other historical events. (See DA Pamphlet 25-91).

(a) 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 as a high priority by all VI activities.

(b) Non-tactical 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:

1. Readiness posture of units.

2. Significant military operations, campaigns, exercises, or maneuvers.

3. Programs and projects that have an impact on national or Army policy and, therefore, must be retained by the Army.

4. Significant events related to construction of major systems, facilities, and installations within theater of operations.

5. Army participation in disaster relief, civil disturbances control environmental protection, and related subjects of national attention or significance.

6. Construction of major systems, facilities, and installations.

7. Depicts the President of the United States or family member.

8. 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 by the commanders of a division or larger unit; the award of the Medal of Honor, or other events of similar or greater importance.

9. Depicts outstanding examples of military life (e.g., 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 which does not meet the above criteria will be destroyed by the VI activity no later than two years after the date of recording. Earlier destruction is authorized.

(d) Use of chain of command photographs is a MACOM prerogative. Photographs of the President, Secretary of Defense, Secretary of the Army, and the Chief of Staff Army may be obtained by local VI activities from JVISDA.

7–12. Restrictions

a. Recording information by audio or videotape will be limited to essential events or activities that are related to military missions and functions. It will be recorded only if a specific official requirement exists. Civilian activities and social events are not normally considered appropriate subjects for recording. The MACOM VI Manager must approve official requests for these types of recordings.

b. Multimedia/VI productions will not be used to promote installations, MACOMs/FOAs, sales of commercial products or private industries; influence pending legislation; or to provide forums for opinions on broad subjects. (Ref DODD 5040.2.)

c. Prohibited recordings. The photo-optical and electronic recording of the following items is prohibited by Title 18, United States Code. 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, US Army Legal Services Agency, will make final determination. Prohibited items include:

(1) The photographing of 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 (but not for other 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, and if the negatives (original recording material) and plates used are destroyed after the final use for the purpose for which they were made. "Money" is interpreted to mean notes, drafts, bonds, certificates, uncancelled stamps and monetary securities in any form.

(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 (Section 701, Title 18 United States Code (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. Recording and/or use of copyrighted material in the development of any VI product is prohibited by law (Title 17 Copyrights (1998)) 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; therefore, written permission will always 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. Violators are subject to prosecution at all levels of involvement.

e. The editing or modifying of any Army VI production, either in-house or by commercial contract, may have certain 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 DISC4.

f. 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) An official request that the program be recorded is initiated by the Army organization that requires the information.

(3) The information recorded will be destroyed 60 days after recording unless the unit or installation commander has determined 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.

(4) DOD personnel will not use recorded information, as an instructional aid or for general viewing, without the written permission of the copyright owner. Off-air broadcasts may be recorded and used without permission of the copyright owner where the viewing of the recording is for the following purposes.

(a) Law enforcement investigation.

(b) Investigations related to national security.

(c) Civil emergencies, when necessary to accomplish an Army mission.

(d) When consent of the copyright owner cannot be obtained prior to use of the recorded information because of time constraints, written permission from copyright holder will be obtained prior to duplication or distribution.

g. Personnel and equipment.

(1) Army personnel who are on official VI assignments, except when off-duty, are not permitted to engage in VI recordings for personal retention or for any other purposes not directly related to official Army activities. When, either by choice or agreement, personally owned equipment or supplies (such as cameras, film, videotape, and graphic arts material) are used during an official assignment, all VI material recorded or generated while on that assignment becomes Army property; it will be turned in to an authorized VI activity. Army personnel have no personal rights to sell or distribute this type of imagery.

(2) Government personnel will not perform roles which subject them to health or safety hazards not normally encountered in their regular duties.

(3) The following equipment will not be purchased through the VISP:

(a) VI equipment used exclusively for RDT&E (to include user testing).

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

(c) Permanently installed installation public address systems (including bugle-call systems) which are handled as real property or property in place.

(d) Television observation/surveillance and remote viewing systems.

(e) Cable distribution systems external to the actual front-end production and playback equipment.

(f) Intercom systems external to front-end equipment for transmission feed except those designated specifically to control studio productions.

(g) VI equipment items that are part of information system requirements for all MILCON projects.

(i) VI equipment that is a component of a teleconferencing system or desktop VTC.

(j) Manual or electronic typesetters, copiers and laser printers used for printing and publishing.

h. Releases. Releases may be required for the use of personnel, equipment, property, etc., 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 ARs 25-55, 340-21, 360-5, 380-5 and DA Pamphlet 25-91.

i. 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.

j. Public exhibition clearance. VI products produced by the Army (whether in-house or by contract) and cleared for public exhibition will become a part of the public domain. This means that these products, upon completion, will be without legal encumbrances such as copyright, patent, personal property, or performance restrictions. Any contract for the production of VI products will require 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 through HQDA (PA) to OSD (PA).

(3) All cleared still or electronic images or stock footage will be forwarded to USAVIC 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, criteria established for the host country involved and through coordination with the U.S. Embassy. AFRTS stations will not broadcast any VI production not cleared for public release.

k. Legal Reviews. In accordance with 36 CFR § 1232.1 and 44 USC § 3301, any U.S. civilian organization may borrow Army VI products that have been cleared for public exhibition by the HQDA (PA) and/or OSD (PA). 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) The editing or cutting of Army VI products (productions or footage) in whole or in part by or for, organizations to which they are loaned is forbidden. 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.

(2) No admission fees or other 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 date of return.

(4) Failure to accept the conditions listed above or to return the material in good condition will provide a basis for refusing subsequent loan of multimedia/VI productions to the individual or organization concerned.

Chapter 8
Records Management Policy

Note: Per General Order 24, the records management function transferred from the DISC4 to the Deputy Chief of Staff for Personnel. Performance of the missions and functions will continue to be subject to the oversight of the DISC4 in the director's role as CIO.

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. Plans, policies and programs of Records Management provide for the modern, efficient and systematic life cycle management of all recorded information, regardless of media. In doing so, it establishes requirements for agency heads and commanders at all echelons to document the Army's official business in a format that is accessible throughout the lifecycle of the information. In addition, it keeps the DA in compliance with information access laws, and protects both DA's and the individual's rights and interests.

b. This chapter implements the following Department of Defense Directives (DODD) and Instructions (DODI):

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

(2) DODD 5025.12, Standardization of Military Terminology.

(3) DODD 5015.2, Records Management Program.

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

(5) DODD 5400.9, Publication of Proposed and Adopted Regulations Affecting the Public.

(6) DODD 5400.11, DOD Privacy Program.

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

(8) DODI 5330.2, Specifications for DOD Letterheads.

(9) DOD STD 5015.2, DOD Design Criteria Standard for Records Management Application Functional Baseline Requirements.

c. Section 3102 of Title 44, 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 provisions for:

(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 under 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, graphic art.

(2) Machine readable items (such as hard disks, magnetic tapes, punched cards, floppy disks, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical recording media, e-mail, databases, and so forth).

(3) Film slides, overhead transparencies, and motion picture films.

(4) Audio and video recordings.

(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, whatever 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, which is processed and produced by such software, and which may in some instances is 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, 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) Records administrators serve on the MACOM staff and have command-wide records management responsibilities. As such, records administrators will:

(a) Be appointed in writing.

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

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

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

(e) Oversee, survey and appraise the methods and operations of records holding areas 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.

(f) 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.

(g) 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.

(h) 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.

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

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

(2) Records management officers serve on the installation garrison staff and have installation-wide responsibilities. As such, records management officers will-

(a) Be appointed in writing.

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

(c) Survey and appraise the records management program at least once every three years and prescribe and ensure that necessary corrective action is taken.

(d) Manage and provide staff direction for the operation of the records holding area. 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.

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

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

(g) 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.

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

(3) Records coordinators. Records coordinators will be designated at sub-elements as necessary for program execution. Coordinators will perform records management duties as assigned.

8–3. Life cycle management of records

a. Maintaining Army information that becomes records is the responsibility of all military, civilian and contractor

personnel, commanders, and leaders. (See chapter 6, AR 25-400-2, 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 and war.

(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 effectively provide alternatives for storage, retrieval, and use of records.

i. Ensure records are preserved in a manner and on a media which meets all legal and archival requirements.

j. Incorporate standards and technical specifications for the life cycle management of record information in all information systems requirements.

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 and soldiers.

c. Establish proactive control over contingency records.

d. Centralize record collection in theater.

e. Digitize once with multiple access.

f. Ensure appropriate command emphasis.

g. Incorporate into training (exercises, NTC).

8–5. Major subprograms

a. Army recordkeeping systems management. The objectives of Army recordkeeping systems management are to cost-effectively organize Army files contained in any media so needed records can be found rapidly, to ensure that records are complete, to facilitate the selection and retention of permanent records, and to accomplish the prompt disposition of noncurrent records in accordance with NARA approved disposition schedules. (See AR 25-400-2.)

(1) *The Modern Army Recordkeeping System (MARKS).* The MARKS provides procedures for the systematic identification, maintenance, retirement, and destruction of Army information. It provides for establishment and operation of Records Holding Areas and Overseas Command Records Holding Areas, and furnishes the legal authority for destruction of non-permanent Army records by organizational elements.

(2) *Electronic recordkeeping systems.* Life cycle management of information contained in automated information systems to include audio, electronic mail, visual and image information systems utilizing automation.

(3) *Manual recordkeeping systems.* Life cycle management of information contained in manual information systems to include paper, image, audio, and visual information systems.

b. Official mail and distribution management. Official Mail and Distribution Management provides rapid handling and accurate delivery of official mail throughout the Army at minimum cost. To do this and to increase efficiency, processing steps are kept to a necessary minimum, sound principles of work flow 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.)

(1) Office symbols are used to identify originators of correspondence and electronically transmitted messages. 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.

(a) Office symbols should contain no more than nine letters. Hyphens are placed between the fourth and fifth and the seventh and eighth letters. Characters other than letters of the alphabet will not be used in the construction of office symbols. The first two letters of an office symbol normally indicate the organization's primary command. For example, "SA" is used for the OSA or an OSA activity; "DA" for other HQDA staff elements.

(b) Office symbols of HQDA field operating and staff support agencies normally begin with two letters representing the parent staff agency. Exceptions may be granted for HQDA field operating agencies and staff support offices located

in the National Capital Region (NCR). The third and fourth letters of the symbol represent the principal official in the activity or agency. The fifth and sixth letters represent a directorate, a comparable element, or the next organizational element below agency level. The fifth and sixth letters may also represent a certain official in the immediate office of the agency head. The seventh letter represents a staff division, a comparable element, or the next lower organizational element. The eighth letter represents a staff branch, comparable element, or the next lower organizational element if there is no branch or comparable organizational element. The ninth letter represents a section, group, team, or an individual action officer.

(c) The letter "Z" is used in the fifth or seventh position only for the immediate office of the head of the agency, the director of a directorate, or the commander of a field operating or staff support agency. The letter "Z" is normally used with letters "A" through "W" to represent the officials (for example, deputies and assistant deputies) in the immediate office of the activity head. The letter "X" is used in the sixth or eighth position only for the executive, executive officer, or executive assistant of the agency or activity.

(d) The Administrative Assistant to the Secretary of the Army proposes office symbols for the Army Secretariat and ARSTAF activities, including the appropriate subordinate and field operating agencies, and submits them to the U.S. Army Records Management and Declassification Agency, ATTN: TAPC-PDD-R, Stop C 55, 6000 6th Street, Stop C-55, Suite S122, Fort Belvoir, VA 22060-5576. Exceptions to the DA construction method may be granted for HQDA field operating agencies and staff support offices located in the NCR.

(e) The basic office symbol for major commands will be constructed using the HQDA construction method and assigned by the U.S. Army Records Management and Reclassification Agency. The Administrative Assistant to the Secretary of the Army (for the Secretariat and ARSTAF) and major commands will submit their requests for deletions, additions and corrections to the U.S. Army Records Management and Reclassification Agency. Other units and activities will submit to the next higher headquarters.

c. Correspondence management. 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 310-4.)

e. Freedom of Information Act (FOIA) Program Management. The FOIA Program implements the DOD policy that requires that its activities be conducted in open manner consistent with the need for security and adherence to other legal and regulatory requirements. The objectives of the FOIA Program are that only information that is exempt from disclosure by the Act is withheld from the general public and to ensure the release of any exempted information if no legitimate purposes for withholding it exists. (See AR 25-55.)

f. Privacy Act program management. The Privacy Act program protects the privacy of an individual from unwarranted invasion by ensuring that collection and maintenance of recorded information about the individual is necessary, accurate, relevant, timely, and complete. Also, it ensures that these records are described in the Federal Register; are used only for authorized purposes, unless otherwise agreed to by the individual; made available for access at the request of the individual; are subject to amendment, when the individual demonstrates them to be inaccurate; and safeguarded from unauthorized disclosures. (See AR 340-21 and DA Pamphlet 25-51.)

g. Management Information Control Office (MICO). The HQDA MICO objectives are to establish policy, procedures and standards for information management control and prescribe responsibilities for the management and control of external and internal Army information requirements. This includes 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 (RCS). The MICO will evaluate proposed, new or revised public information requirements, prepares the Annual Information Collection Budget, and plan and coordinate periodic reviews of Army information management requirements, IT products, and public information requirements. (See AR 335-15.)

h. Vital Records. This program provides for the selection and protection of vital records required for the Army emergency preparedness programs. It also provides policies and guidance for 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, headquarters, major commands, and certain activities maintain copies of emergency operating records at predesignated relocation and alternate sites. See also paragraph 6-1c.

(2) *Rights and interests records.* These are records essential to the preservation of the legal rights and interests of individual citizens (including service members) and the Army. These records include such groups as retirement records, finance and accounting records, medical records, records from contingency operations, 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. (See also AR 310-25 and AR 310-50.)

(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 DOD elements and NATO member countries.

j. Management of records of defunct Army commands and organizations. These are records that have been transferred into a Federal Records Repository but are still under Army control because legal authority has not yet been transferred to the National Archives.

k. Oversight records administration of joint commands. 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 DCSPER 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 HQDA DCSPER (DAPE-ZXI-RM).

m. Defense Visual Information Centers (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 Joint Visual Information Service and Distribution Activity (JVISDA) or through the Component Accessioning Point (CAP). See also paragraph 7-10.

n. Armed Services Center for Research of Unit Records Program. The program meets current and future Army requirements by locating, analyzing, and extracting pertinent data from unit records created during U.S. military contingency 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 data bases 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, etc., 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. This does not violate any of the prohibitions discussed above. Moreover, such donations create a single source of information on actions accomplished by high officials. The Director of Military History Institute will preserve the integrity of these collections with the identification of the donor, such as the "Wickham Papers," the "Abrams Papers," the "Bradley Papers," and so forth. During the lifetime of the donor, the collection will be open to them for whatever research, reference, or historical inquiry they wish to make. The Director of the Military History Institute will provide archival and librarian assistance to the donor. The donor must meet 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 non-record copy, whose absence creates a gap in the files or impairs the logical sequence of essential documentation.

(7) Records required to transact the official business of the Army and any document which assists in the decision making process.

e. Records identified below may be removed when the individual creating them retires, resigns, or otherwise terminates his or her tenure of office.

(1) All personal and private papers that do not contain references to official business.

(2) 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.

(3) Reference books and other personal items brought from private life.

f. Separation and control of personal papers at the time of creation is the best way to avoid mixing personal papers with official records.

g. 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, outside of the continental United States, 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 Reclassification Agency, ATTN: TAPC-PDD-R, Stop C 55, 6000 6th Street, Suite S122, Fort Belvoir VA 22060-5576, as expeditiously as theater or operational conditions permit.

8–7. Record media

a. Information created within the Army may be recorded on various display media such as paper, microform, other machine-readable format, or presentation media (audio and visual). Approved Army disposition schedules 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 must be selected which best serves the operational needs of the Army and meets statutory scheduling requirements. 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 MARKS records disposition schedule, such as, retention period for the information contained in the system, individual microform or data base. MARKS provide procedures for the systematic identification, maintenance, retirement, and destruction of Army information. Where more than one MARKS 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 per DOD STD 5015.2.

(2) The ability to retrieve the 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 in the physical custody of NARA. Formal accessioning into the National Archives of the United States, however, transfers legal custody from the Army to NARA and the Archivist of the United States.

(3) Federal Records Centers have storage facilities for a record in machine-readable and microform formats; however, they do not possess servicing capability. The retiring activity for servicing, testing, manipulation or data processing must retrieve records in these formats.

(4) Information retained in other than paper format only as the record copy 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 or employees that it affects.

(5) VI original materials are retained in their original format. However, electronic VI media for archival retention is transferred to permanent media such as monochrome motion picture film.

(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 MARKS informational 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 contain permanent MARKS informational series as determined by the Archivist of the United States, special conditions noted in 8-7b.(9) 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 are not retained on the film that will deteriorate the recorded information. In addition to the film test, all microforms produced will conform to quality standards and formats. For guidance about forwarding the film samples to the appropriate testing facility and to ensure quality standards are being met for the microform application relative to format, resolution, density, and testing requirements, contact the U.S. Army Records Management and Reclassification Agency, address at paragraph 8-6g(3), for specific instructions.

(9) 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 as well as the display media.

(a) 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 paper must be provided.

(b) If the appropriate MARKS standard does not contain a dual disposition standard for the conversion of paper to microform, approval for conversion must be requested from the U.S. Army Records Management and Reclassification Agency, address at paragraph 8-6g(3).

(c) Agencies may use optical disk systems 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 into an optical disk without NARA's approval. Requests should be sent to the U.S. Army Records Management and Reclassification Agency, address at paragraph 8-6g(3).

(10) Due to personal health risks, agencies will not destroy CD ROMs by burning, pulverizing, or shredding. CD ROMs will be stored pending development of final disposition instructions. If the volume of stored CD ROMs 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 CDs may be smelted.

8–8. Electronic records management

a. Army records, regardless of media, must follow the disposition instructions identified in AR 25-400-2, Appendix B, and comply with the security requirements of AR 380-19. All electronic information generated by or contained in an information system (IS) or any office automation source, or created during the conduct of electronic business/electronic commerce, must be considered. This includes information contained in Standard Army Management Information Systems, e-mail, command or installation 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 system. The functional value and program needs of electronic records dictate the retention period. The MARKS disposition instructions will be defined during the need justification phase, milestone 0, and reviewed in the revalidation phase of each milestone in the life cycle management of the system.

b. Visual information digital still and motion images are excluded from this paragraph. VI products are managed under the provisions of chapter 7 and DA Pamphlet 25-91.

Chapter 9
Publications and Printing

Note: Per General Order 23, this function transferred from DISC4 to the Administrative Assistant to the Secretary of the Army. Performance of the missions and functions will continue to be subject to the oversight of the DISC4 in the director's role as CIO.

9–1. Management concept

The Administrative Assistant to the Secretary of the Army is the functional proponent for the policy, management and execution of the Army Publishing and Printing Program (APPP). The APPP 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 APPP, and related policies, responsibilities, and mandated procedures are described in AR 25-30. The APPP-

a. Includes all levels of publishing (including printing, duplicating, and copy management) 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 Administrative Assistant to the Secretary of the Army (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 and issuing the CD–ROM Army Electronic Library of departmental administrative publications and forms and DA Pamphlet 25–30, Consolidated Index of Army Publications and Blank Forms.

(3) Maintaining the central official online repository for administrative publications and publications index at http://www.usapa.army.mil. The repository also contains hyperlinks to the official publication Web sites for all other types of departmental publications.

(4) Ensuring that electronic publications maintained in the central official online repository are JTA-A compliant.

b. Only those Web sites approved by the AASA may host Army-wide departmental publications and forms on their Web sites. 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 Web site 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 e-mail or on the Internet. Proponents are encouraged to use file compression when sending large file attachments to multiple addressees via e-mail, especially when file attachments exceed five 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 only be done 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 6-3r 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 non-recurring publication will be printed unless approved by the appropriate department 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.

b. Nonessential publications. A proposed Army publication will be considered nonessential and will not be printed or reproduced in any media, to include electronic, if-

(1) It is not directly needed to effectively, efficiently, and economically conduct official business.

(2) It cannot be produced and distributed in time to fully serve its intended purpose.

(3) It duplicates, beyond the requirements for clarity, material already available to the publication's users.

c. 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 appropriated or non-appropriated funds 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 (including CD-ROM replication) and duplicating 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 USAPA. USAPA will procure this printing through DAPS.

(2) Commands and field activities will not produce or procure departmental printing unless authorized by USAPA under a decentralized printing program.

b. Field printing and duplicating. Every effort must be made to requisition field printing requirements from the 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 DCSIM and DOIM or designated functional manager are authorized to procure printing from commercial sources through the DAPS regional offices.

(3) Effectiveness and economy in accomplishing mission objectives will be considered in determining whether in-house or commercial resources will be used.

(4) 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.

(5) 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), WASH DC 20310-0105.

Appendix A
References

Section I
Required Publications

ACP 123
Common Messaging Strategy and Procedures. (Cited in para 6-4.) Obtain from the Internet at http://www.dtic.mil/jcs/j6/cceb/acps/.

AR 5–20
Commercial Activities Program. (Cited in para(s) 2-16, and 6-2.)

AR 25–30
The Army Integrated Publishing and Printing Program . (Cited in para(s) 7-7, 9-4.)

AR 25–55
The Department of Army Freedom of Information Act Program. (Cited in para(s) 1-6, 7-12, 8-2, 8-5.)

AR 25–400–2
The Modern Army Recordkeeping System (MARKS). (Cited in para(s) 6-3, 7-10, 8-2, 8-3, 8-5, 8-6.)

AR 70–1
Army Acquisition Policy. (Cited in para(s) 2-3, 2-5, 3-7, 6-1, 6-2, 6-4.)

AR 71–9
Materiel Requirements. (Cited in para(s) 2-28, 3-1, 3-4, 3-5, 3-6, 3-7, 6-4, 7-2.)

AR 215–1
Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities. (Cited in para(s) 6-3.)

AR 215–4
Nonappropriated Fund Contracting. (Cited in para(s) 6-3.)

AR 340–21
The Army Privacy Program. (Cited in para(s) 1-6, 7-12, 8-5, 8-6.)

AR 360–1
The Army Public Affairs Program. (Cited in para 6-3.)

AR 380–5
Department of the Army Information Security Program. (Cited in para(s) 7-12, 8-6.)

AR 380–19
Information Systems Security. (Cited in para(s) 1-5, 2-16, 5-1, 5-2, 5-3, 5-4, 5-5, 5-7, 6-3, 7-9, 8-8.)

AR 380–53
Information Systems Security Monitoring. (Cited in para(s) 6-1, 6-3.)

DA Pamphlet 25–1–1
Installation Information Services. (Cited in para(s) 6-1, 6-2, 6-3.)

DA Pamphlet 25–91
Visual Information Procedures. (Cited in para(s) 6-3, 7-4, 7-5, 7-7, 7-8, 7-9, 7-10, 7-11, 7-12.)

DoD Regulation 5000.2–R
Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs. (Cited in para 3-7.)

DoD 5500.7–R
Joint Ethics Regulation (JER). (Cited in para(s) 6-1 and para 6-3.)

DoDD 1015.6
Funding of Morale, Welfare, and Recreation Programs. (Cited in para(s) 6-1.)

DoDD 5000.1
The Defense Acquisition System. (Cited in para(s) 2-3.)

DoDD 5040.2
Visual Information (VI). (Cited in para(s) 2-1, 7-1, 7-7, 7-8, 7-12.)

DoDI 1015.10
Programs for Military Morale, Welfare, and Recreation (MWR). (Cited in para(s) 6-3.)

DoDI 4640.14
Base and Long-Haul Telecommunications Equipment and Services. (Cited in para 6-4.)

DoDI 5200.40
DoD Information Technology Security Certification and Accreditation Process (DITSCAP). (Cited in para 5-3.)

29 U.S.C. 794d
Section 508 of the Rehabilitation Act Amendments of 1998, as amended by section 2405 of the FY 2001 Military Appropriations Act (Public Law 106-246)(29 U.S.C. 794d). (Cited in para 6-3.)

Section II
Related Publications
A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 5–11
Management of Army Models and Simulations

AR 5–12
Army Management of the Electromagnetic Spectrum

AR 10–5
Organization and Functions, Headquarters, Department of the Army

AR 12–8
Security Assistance—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 25–55
The Department of the Army Freedom of Information Act Program

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 310–4
Publication in the Federal Register of Rules Affecting the Public

AR 310–25
Dictionary of United States Army Terms

AR 310–50
Authorized Abbreviations and Brevity Codes

AR 335–15
Management Information Control System

AR 380–10
Foreign Disclosure, Technology Transfer, and Contacts with Foreign Representatives

AR 380–19–1
Control of Compromising Emanations (U)

AR 380–67
The Department of the Army Personnel Security Program

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 700–142
Materiel Release, Fielding, and Transfer

AR 710–2
Inventory Management Supply Policy Below Wholesale Level

AR 750–1
Army Materiel Maintenance Policy and Retail Maintenance Operations

CJCSI 6215.01
Policy for the Defense Switched Network. Obtain from http://www.dtic.mil/doctrine/cjcsidirectives.htm.

CTA 50–909
Field and Garrison Furnishings and Equipment

DA Pamphlet 25–30
Consolidated Index of Army Publications and Blank Forms

DA Pamphlet 25–40
Administrative Publications: Action Officers Guide

DA Pamphlet 25–50
Compilation of Army Addresses

DA Pamphlet 25–51
The Army Privacy Program—System of Records Notices and Exemption Rules

DA Pamphlet 70–3
Army Acquisition Procedures

DA Pamphlet 700–142
Instructions for Materiel Release, Fielding and Transfer

DCID 1/16
Supplement-Security Manual for Uniform Protection of Intelligence Processed in Automated Systems and Networks (U) (SECRET)(This publication may be obtained from DIA(SY-ID), Bolling Air Force Base, Building 6000, Washington, D.C. 20340-0001.

DISA Circular 310–130–1
Submission of Telecommunications Service Requests. Obtain at Web site http://www/disa.mil/pubs.

DoD 5400.7–R
Freedom of Information Act (FOIA) Program

DoDD 1015.2
Military Morale, Welfare, and Recreation (MWR)

DoDD 3020.26
Continuity of Operations (COOP) Policy and Planning

DoD 4525.8–M
Official Mail Manual

DoDD 4640.7
DoD Telecommunications System (DTS) in the National Capitol Region (NCR)

DoDD 5015.2
DOD Records Management Program

DoDD 5025.12
Standardization of Military and Associated Terminology

DoDD 5040.3
Joint Visual Information Services

DoDD 5040.4
Combat Camera (COMCAM) Program

DoDD 5040.5
Alteration of Official DoD Imagery

DoDD 5230.9
Clearance of DoD Information for Public Release

DoDD 5400.9
Publication of Proposed and Adopted Regulations Affecting the Public

DoDD 5400.11
DOD Privacy Program

DoDD 5530.3
International Agreements

DoDD 7950.1
Automated Data Processing Resources Management

DoDD 8000.1
Management of DOD Information Resources and Information Technology

DoDD 8320.1
DoD Data Administration

DoDD 8910.1
Management and Control of Information Requirements

DoDI 4000.19
Interservice and Intragovernmental Support

DoDI 5330.2
Specifications for DoD Letterheads

DoDI 5335.1
Telecommunications Services in the National Capitol Region (NCR)

DoDI 7740.3
DoD Information Resources Management (IRM) Review Program

Federal Acquisition Regulation
Government Printing and Binding Regulations

FIPS 178
Video Teleconferencing Services. Obtain at Web site http://www/itl/nist/gov/fipspubs.

General Order 1997-23
Transfer of Publications and Printing

General Order 1997-24
Transfer of Records Management

OMB Cir A–76
Performance of Commercial Activities. Obtain at Web site http://clinton1.nara.gov/White_House/EOP/OMB/html/circular.html.

OMB Cir A–109
Major Systems Acquisitions. Obtain from the Office ofManagement and Budget, telephone (202) 395–7332.

OMB Cir A–130
Management of Federal Information Resources. Obtain at Web site http://clinton1.nara.gov/White_House/EOP/OMB/html/omb-a130.html.

SB 700–20
Army Adopted/Other Items Selected for Authorizations/List of Reportable Items

5 USC § 552
(Freedom of Information Act)

5 USC § 552a
(The Privacy Act)

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

5 USC, Chapter 6
Regulatory Planning and Review

17 USC § 101, 501
Copyrights

29 USC § 762
(P.L. 101-336 Americans with Disabilities Act of 1990)

31 USC § 1115, 1116
(P.L. 103-62, The Government Performance and Results Act (GPRA))

40 USC § 759
(P.L. 100-235, Computer Security Act of 1987)

40 USC § 762
P.L. 100-542 Telecommunications Accessibility Enhancement Act 1988

41 USC § 413
(P.L. 103-355, The Federal Acquisition Streamlining Act of 1993 (FASA))

44 USC, Chapter 31
Records Management by Agencies

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

44 USC § 3502
Public Printing and Documents

44 USC § 211, Chapters 29, 31, and 33
(P.L. 94-575, Federal Records Management)

44 USC §§ 3501–3520
(P.L. 96-511, Paperwork Reduction Act of 1980)

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

P.L. 104–106
The Clinger-Cohen Act of 1996 (formerly Div E, Information Technology Management Reform Act, Defense Authorization Act of 1996)

Executive Order 12600
Predisclosure Notification Procedures for Confidential Commercial Information

Executive Order 12845
Requiring Agencies to Purchase Energy Efficient Computer Equipment

Executive Order 12999
Educational Technology: Ensuring Opportunity for all Children in the Next Century

Executive Order 13011
Federal Information Technology

Executive Order 13103
Computer Software Piracy

RCS DD–PA (A)–1115
Visual Information Products for Obsolescence

RCS DD–PA (AR)–1381
Visual Information Production Request and Report

RCS GSGPO–344
Visual Information Investment System Requirements for the Visual Information Systems Program

RCS CSIM–59
VI Annual Workload and Cost Data Report

TRADOC Pamphlet 71–9
Requirements Determination

Section III
Prescribed Forms

These forms are available on the USAPA Website and the Army Electronic Library (AEL) CD-ROM.

DA Form 3903
Visual Information Work Order. (Prescribed in para 7-4.)

DA Form 4103
Visual Information Product Loan Order. (Prescribed in para 7-4.)

DA Form 5695
Information Management Requirement/Project Document. (Prescribed in para 7-7.)

DA Form 5697
Army Visual Information Activity Authorization Record. (Prescribed in para 7-4.)

DD Form 1995
Visual Information (VI) Production Request and Report. (Prescribed in para 7-8.)

DD Form 2537
Visual Information Caption Sheet. (Prescribed in para 7-10)

Section IV
Referenced Forms

DD Form 1367
Commercial Communications Work Order

DD 1391
FY ____ Military Construction Project Data

SF 258
Agreement to Transfer Records to the National Archives of the United States.

Appendix B
Management Control Evaluation Checklist

B–1. Function

The functions covered by this checklist are the administration of Army information management and information technology. They include key controls for CIO Management, IT Architecture, Information Assurance, Automation, Telecommunications Management, Visual Information Management, Records Management, and Publishing Management.

B–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.

B–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 five years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2-R (Management Control Evaluation Certification Statement).

B–4. Test questions

a. CIO Management (Chapter 3)

(1) Are the duties and responsibilities of the senior information manager clearly designated in the organization's mission and function? (HQDA, MACOM, FOA)

(2) 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)

(3) Does the organization have a strategic plan that is linked to their mission? Is it periodically updated? (HQDA, MACOM, FOA)

(4) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (MACOM, FOA)

(5) 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, FOA)

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

(b) Can the process be eliminated?

(c) Can the process be accomplished more effectively, efficiently, and at less cost by another Government source, e.g., another MACOM or Federal organization, or the private sector?

(6) 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)

(7) Are exceptions to the IT investment-screening process clearly documented? (HQDA, MACOM, FOA)

(8) Does the organization require that management evaluations for the IT investment screening process, as well as scoring, ranking, and prioritization results, are documented (either manually or through the use of automated applications such as a decision support tool)? (HQDA, MACOM, FOA)

(9) Are IT investment decisions made a part of the organization's integrated capital planning process or are IT projects separated out? (HQDA, MACOM, FOA)

(10) 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)

(11) Does the organization have a process for documenting and disseminating results of this review? (HQDA, MACOM, FOA)

(12) Are process analysis and improvements for warfighter processes documented in the mission needs statement (MNS) and operational requirements document (ORD) using the doctrine, training, leader development, organizational design, materiel, and soldiers (DTLOMS) requirements methodology as defined by the TRADOC-led Army requirements generation process in AR 71-9 and TRADOC Pamphlet 71-9? (HQDA, MACOM, FOA)

(13) Have process analyses, improvements, and reengineering of mission-related and administrative work processes been documented in the process improvement/ reengineering database on the CIO Web site? (HQDA, MACOM, FOA)

(14) Have performance measures been developed for each IT investment which supports organizational mission before execution or fielding that investment? (HQDA, MACOM, FOA, PEO, PM)

(15) Have IT investments been synchronized to overall DOD/Army mission priorities? (HQDA, MACOM, FOA, PEO, PM)

(16) Are performance measures linked to management level goals, objectives, and measures? (All)

b. Army Enterprise Architecture (chapter 4). Has the organization developed the appropriate architectures to comply with the AEA? (All)?

c. Information Assurance (Applies to MACOM, Separate Reporting Activity, Installation, Unit) (Chapter 5)

(1) At each level, has the designated approval authority appointed the appropriate IA personnel?

(2) Are IAVA messages being acted upon in a timely fashion?

(3) Are all information systems and networks accredited and certified? When a new information system is created, does it meet all accreditation and certification standards?

(4) Have the appropriate software controls been implemented to protect system software from compromise, subversion, and/or tampering?

(5) Is only approved software being used on Army networks and stand-alone workstations?

(6) Are database management systems that contain classified defense information protected to the highest security classification of any identifiable database element?

(7) 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?

(8) Have all personnel received the level of training necessary and appropriate to perform their designated information assurance responsibilities?

(9) Are proper password control and procedures being implemented within commands? Are minimum requirements of accountability, access control, least privilege, and data integrity being met?

(10) 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?

(11) 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?

d. C4/IT Support and Services (Chapter 6)

(1) Is a process in place for acquiring IT systems and ensuring all required licensing and registration are accomplished? (MACOM, DOIM)

(2) Is the DOIM the single organization responsible for the oversight and management of installation IT? (MACOM, DOIM)

(3) Are periodic reviews being conducted of current IT systems to ensure they are still required and meeting user needs? (HQDA, MACOM)

(4) Are evaluations being conducted of existing systems for obsolescence? (HQDA, MACOM)

(5) Is an accurate inventory being maintained and validated annually for IT equipment? (DOIM, IMO)

(6) Are continuity of operations plans and procedures documented and distributed? (MACOM, DOIM)

(7) Has guidance been provided to ensure all software is checked for viruses before being loaded? (DOIM)

(8) Are existing capabilities and/or assets considered prior to upgrading, improving, or implementing local or campus area networks? (MACOM, DOIM)

(9) Are uneconomical IT service contracts identified and terminated? (ALL)

(10) Are spare capacity and functional expansion on IT systems being considered and/or used when new requirements are identified? (ALL)

(11) Have new radio frequency assignments proposals been submitted for new or proposed spectrum dependent equipment? (MACOM)

(12) Are there validated and approved frequency assignments for all existing spectrum- dependent equipment? (MACOM)

(13) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (MACOM, DOIM)

(14) Has guidance been provided to review and revalidate cellular telephones and pagers every two years? (MACOM, DOIM)

(15) 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)

(16) Is there a requirement for cellular phones and pagers to be recorded in the property book? (DOIM)

(17) Has local guidance been provided to certify monthly cellular telephone and pager bills? (DOIM)

(18) Have maintenance and support strategies been devised to minimize overall systems life cycle cost at an acceptable level of risk? (PEO, PM, MACOM)

(19) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (MACOM, DOIM, IMO)

(20) Are private sector service providers made aware that written assurance of compliance with software copyright laws may be required? (MACOM, DOIM, IMO)

(21) Does the Web site contain a clearly defined purpose statement that supports the mission of the organization? (All)

(22) Are users of each publicly accessible Web site provided with a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service? (All)

(23) 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)

(24) Is this Web site free of commercial sponsorship and advertising? (All)

(25) Is the Web site free of persistent cookies or other devices designed to collect personally identifiable information about Web visitors? (All)

(26) Is each Web site made accessible to handicapped users in accordance with section 508 of the Rehabilitation Act? (All)

(27) 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?
— 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?

(28) (28) Are operational security (OPSEC) 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.

(b) (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) (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) (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.

(29) Has the Web site reviewer performed a Key Word Search for any of these documents and subsequently removed sensitive personal or unit information from publicly accessible Web sites? (All)

— Deployment schedules.

— Exercise plans.
— Contingency plans.
— Training schedules.
— Inspection results, findings, deficiencies.
— Biographies.
— Family support activities.
— Phone directories.
— Lists of personnel.

e. Visual Information Management (Chapter 7)

(1) Does the mission guidance include responsibilities of the Visual Information (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? (FOA or MACOM)

(2) Is the VI manager the single staff manager for all VI functions on the installation? (FOA, MACOM, and Installation)

(3) Are all VI services and equipment, except those specifically exempted by the MACOM commander, consolidated for centralized VI management? (FOA, MACOM, and Installation)

(4) Do all VI activities under your purview have a Defense Visual Information Authorization Number (DVIAN)? (FOA, MACOM, and Installation)

(5) Does the VI manager approve all VI equipment as required by AR 25-1, Chapter 7? (FOA and Installation)

(6) Is VI policy being followed for multimedia/VI productions? For example, DD Form 1995 is used, funds identified up front, PAN registers maintained, DAVIS searches conducted, service support contracts awarded for less than 50 percent of the total production cost, Non-Local DAVIS entries, using JVIS contracting facility? (FOA, MACOM, 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 support document to include a standing operating procedure? (FOA and Installation)

f. Records Management (Chapter 8)

(1) Is a Records Management Program established in your organization? (All)

(2) Are all records management officials appointed in writing?

(3) Are records managers included in the planning process for new or replacement automated systems? (All)

(4) Are records management reviews of command subordinate headquarters conducted at least once every three 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 will be available to read electronic records throughout their retention period? (All)

(7) Does the DOIM ensure carry-over funds for postage meters and Advance Deposit Trust Account (ADTA) do not exceed 30 days at the end of the fiscal year? (MACOM and Installation)

(8) Do all information collections from the public, affecting ten or more individuals, have OMB approval? (All)

g. Publishing and Printing Management (Chapter 9)

(1) Are policy publications issued as regulations? (HQDA, FOA and MACOM)

(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? (All)

(4) Are Army-wide forms for electronic generation approved by the functional proponent and U.S. Army Publishing Agency? (HQDA, FOA and MACOM)

(5) Is field printing coordinated through the Defense Printing Service and Printing Officer? (All)

Glossary

Section I
Abbreviations

AAE
Army Acquisition Executive

AAFES
Army and Air Force Exchange Service

AASA
Administrative Assistant to the Secretary of the Army

ACERT
Army Computer Response Team

ACP
Allied Communications Publication

ADMG
Army Data Management Group

ADMSP
Army Data Management and Standards Program

ADP
automatic data processing

AEA
Army Enterprise Architecture

AEAF
Army Enterprise Architecture Framework

AEAFD
Army Enterprise Architecture Framework Document

AEAGD
Army Enterprise Architecture Guidance Document

AEAMP
AEA Master Plan

AFIS
American Forces Information Service

AFRTS
American Forces Radio and Television Service

AKM
Army knowledge management

AKO
Army Knowledge Online

AMC
(U.S.) Army Materiel Command

APPP
Army Printing and Publishing Program

AR
Army regulation

AODR
Army Operational Data Repository

ARNG
Army National Guard

ARSTAF
Army staff

ASA
Assistant Secretary of the Army

ASA(ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASARC
Army Systems Acquisition Review Council

ATM
asynchronous transfer mode

AUTODIN
automatic digital network

AVIC
Army Visual Information Center

BASOPS
base operations

BOD
Beneficial Occupancy Date

BPR
business process reengineering

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 (C4) and information technology

CAP
Computer/Electronic Accommodations Program (CAP)

CATV
cable television

CCTV
closed circuit television

CCWO
Commercial Communication Work Order

CDAd
Component data administrator

CD-ROM
Compact disk-read only memory

CFDAd
Component functional data administrator

CFR
Code of Federal Regulation

CINC
Commander in Chief of Unified or Specified Command

CIO
Chief Information Officer

CJCS
Chairman of the Joint Chiefs of Staff

CJCSI
Chairman of the Joint Chief of Staff Instruction

COE
Common operating environment

COMCAM
Combat camera

COMSAT
Commercial satellite

COMSEC
Communications security

CONUS
Continental United States

COOP
Continuity of Operations Plan

COTS
Commercial off-the-shelf

CPA
Chief of Public Affairs

CSA
Chief of Staff, U.S. Army

DA
Department of the Army

DAB
Defense Acquisition Board

DARMP
Defense Automation Resources Management Program

DAS
Director of the Army Staff

DAVIPDP
Department of the Army Visual Information Production and Distribution Program

DAVIS
Defense Automated Visual Information System

DBMS
Data base management system

DCID
Director of Central Intelligence Directive

DCSIM
Deputy Chief of Staff for Information Management

DCSINT
Deputy Chief of Staff for Intelligence

DCSOPS
Deputy Chief of Staff for Operations and Plans

DCSPER
Deputy Chief of Staff for Personnel

DDD
Direct Distance Dialing

DISA
Defense Information Systems Agency

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

DISN
Defense Information Systems Network

DITMS
Defense Information Technology Management System

DMATS
Defense Metropolitan Area Telephone System

DMS
Defense Message System

DOD
Department of Defense

DODD
Department of Defense Directive

DOIM
Director of Information Management

DPW
Department of Public Works

DSN
Defense Switched Networks

DTLOMS
Doctrine, Training, Leader Development, Organizations, Materiel, Soldiers

DTMF
Dual Tone Multiple Frequency

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

DVTC
Desktop Video Teleconferencing

E-Mail
Electronic Mail

EA
Enterprise architecture

EB/EC
electronic business/electronic commerce

EIPP
Educational Institution Partnership Program

FAO
Finance and Accounting Officer

FAR
Federal Acquisition Regulation

FDAD
Functional Data Administrator

FOA
Field operating agency

FOIA
Freedom of Information Act

FORSCOM
U.S. Army Forces Command

FOUO
For Official Use Only

FTS2000
Federal Telecommunications System 2000

FX
Foreign Exchange

FY
Fiscal year

GBS
Global Broadcast Service

GILS
Government Information Locator Service

GOCO
Government owned, contractor operated

GOTS
Government Off-the-Shelf

GPO
Government Printing Office

GPRA
Government Performance and Results Act of 1993

GPS
Global Positioning System

GSA
General Services Administration

HLA
High level architecture

HMW
Health, morale, and welfare

HQ
Headquarters

HQDA
Headquarters, Department of the Army

HUMINT
Human intelligence

IA
Information assurance

IAVA
Information assurance vulnerability assessment

IER
Information exchange requirement

IM
Information management

IMO
information management officer

IMSC
Installation Information Management Support Council

INMARSAT
International Maritime Satellite

INSCOM
U.S. Army Intelligence and Security Command

IP
internet protocol

IPR
in-process review

ISA
Interservice Support Agreement

ISP
internet service provider

ISR
intelligence, surveillance, and reconnaissance

ISSM
information systems security managers

ISSP
Information systems security program

IT
information technology

ITA
IT Architecture

ITM
Information Technology Management

IT OIPT
Information Technology Overarching Integrated Product Team

IVD
Interactive video disk

JCP
Joint Committee on Printing

JCS
Joint Chiefs of Staff

JPO
Joint Program Office

JS
Joint Staff

JTA
(DOD) Joint Technical Architecture

JTA-A
Joint Technical Architecture - Army

JVIS
Joint Visual Information Services

JVISDA
Joint Visual Information Services Distribution Activity

LAN
local area network

LDAP
Lightweight Directory Access Protocol

M&S
Modeling and Simulation

MACOM
major Army command

MARKS
Modern Army Recordkeeping System

MARS
Military Affiliated Radio System

M/CATV
Master/Community Antenna Television

MCEB
Military Communications-Electronics Board

MDEP
Management Decision Evaluation Package

MEDCOM
Medical Command

MICO
Management Information Control Officer

SATCOM
Satellite Communications

MILSTAR
Military Strategic and Tactical Relay System

MNS
Mission Needs Statement

MOP
memorandum of policy

MP
Master Plan (as applies to information management)

MSC
major subordinate command

MTOE
Modified Table of Organization and Equipment

MWR
Morale, Welfare, and Recreation

NAC
National Audiovisual Center

NAF
Nonappropriated Fund

NAFI
Nonappropriated Fund Instrumentalities

NARA
National Archives and Records Administration

NATO
North Atlantic Treaty Organization

NCR
National Capital Region

NFIP
National Foreign Intelligence Program

NIPRNET
Unclassified but sensitive Internet protocol router network

NSA
National Security Agency

NSS
National Security System

OA
operational architecture

OASD
Office of the Assistant Secretary of Defense

OASD(PA)
Office Assistant Secretary of Defense (Public Affairs)

O&M
operations and maintenance

OCONUS
outside of the continental United States

ODISC4
Office of the Director of Information Systems for Command, Control, Communications, and Computers

OE
operational elements

OMA
operations and maintenance, Army

OMB
Office of Management and Budget

OPA
other procurement, Army

OPSEC
Operational Security

ORD
operational requirement document

OSA
Office of the Secretary of the Army

OSD
Office of the Secretary of Defense

PA
public affairs

pam
pamphlet

PAN
production approval or authorization number

PC
end-user microcomputer (personal computer)

PCMCIA
Personal Computer Memory Card International Association

PDA
Personal Digital Assistant

PEG
Program Evaluation Group

PEO
Program Executive Officers

PIN
Personal identification number

PKI
Public Key Infrastructure

PMO
Program Management Office

POM
program objective memorandum

PPBES
Planning, Programming, Budgeting, and Execution System

PPSS
Post-production software support

RCERT
Regional Computer Response Team

RCS
requirements control symbol

RFS
Request for Service

RDT&E
research, development, test, and evaluation

SA
system architecture

SATCOM
Satellite Communications

SB
supply bulletin

SCI
sensitive compartmented information

SCIF
sensitive compartmented information facility

SF
standard form

SIGINT
signal intelligence

SIPRNET
Secret Internet protocol router network

SLA
Service Level Agreement

SOM
System Operational Manager

SOP
standard operating procedures

SSL
Secure Sockets Layer

STARC
State Area Command

STE
Secure Telephone Equipment

STU-III
Secure Telephone Unit, Type III

T&E
test and evaluation

T-ASA
Television-Audio Support Activity

TA
technical architecture

TCP/IP
transmission control protocol/Internet protocol

TDA
Tables of Distribution and Allowances

TDD
Telephone Devices for the Deaf

TECHDOC
Technical documentation

TEMPO
Telephone Management Project Office

TJAG
Judge Advocate General

TOE
Tables of Organization and Equipment

TPF
Total Package Fielding

TRADOC
U.S. Army Training and Doctrine Command

TSAMS-E
Training Support Automated Management System-Enhanced

URL
Uniform Resource Locator

USACESO
US Army Communications-Electronics Services Office

USASC
United States Army Signal Command

USAR
United States Army Reserve

USARC
United States Army Reserve Command

USAVIC
United States Army Visual Information Center

USC
United States Code

USPFO
United States Property and Fiscal Office

VI
visual information

VIDOC
Visual Information Documentation Program

VIRIN
visual information record identification number

VISP
Visual Information Systems Program

VTC
video teleconferencing

WAN
wide area network

WWW
World Wide Web

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
Within the context of the Army Enterprise Architecture (AEA), a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes in support of accomplishing tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element (PSE).

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 processes
Enabling activities that support mission and mission-related processes and functions, e.g., manage legal process, performance assessment, combat health support, family support, etc.

AEA Framework Document (AEAFD)
The AEAFD provides developers, users, and managers throughout the Army with a common theoretical approach for developing and presenting architectures within the Army. It is the theoretical basis for the Army Enterprise Architecture Guidance Document's (AEAGD) procedures.

AEA Guidance Document (AEAGD)
The AEAGD provides detailed procedures that implement Army policy regarding AEA models and products.

AEA Master Plan (AEAMP)
The AEAMP provides the Army's management strategy, to include priorities, schedules, taskings and resource allocations, for managing the decentralized and incremental AEA development efforts

Army Data Management Program
Establishes information about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data.

Army Operational Data Repository
A meta-data repository used for architectures of functional Army systems.

Application
The system or problem to which a computer is applied. Reference is often made to an application as being of the computational type, wherein arithmetic computations predominate, or of the data processing type, wherein data handling operations predominate.

Architecture
The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.

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 Enterprise Strategy
The single unified vision for strengthening the Army's combat, combat support, and combat service support forces.

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 non-current records in accordance with National Archives and Records Administration approved schedules.

Army Visual Information Steering Committee (AVISC)
Colonel or civilian equivalent level from each MACOM/FOA.

Artificial Intelligence (AI)
Capability of a device to perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.

Authentication
A security service that verifies an individual's eligibility to receive specific categories of information.

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.

Automated information system (AIS)
A combination of computer hardware and software, telecommunications information technology, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. Excluded are computer resources, both hardware and software, which are physically, part of, dedicated to or essential in real-time to the mission performance of weapon systems. An AIS can include computer software only, computer hardware only, or a combination of the above.

Bandwidth
The maximum rate at which an amount of data can be sent through a given transmission channel.

Baseline Architecture
A description of the current set of IT resources and capabilities.

Benchmark
A procedure, problem or test that can be used to compare systems, components, processes, etc, to each other or to a standard.

Benchmarking
A method of measuring processes against those of recognized leaders to establish priorities and targets leading to process improvement.

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 Reengineering (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. Reengineering 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 which includes, both audio and video programming and which is provided to multiple subscribers.

CAP acquisition program
A directed, funded effort designed to provide a new, improved, or continuing weapons system or automated information system (AIS) capability to meet a valid operational need. These programs are in categories, which facilitate decentralized decisionmaking, execution, and compliance with statutory requirements.

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.

Capability configuration
A combination of architectures or architecture views that describes a warfighting or business process capability. An integrated set of an operational architecture view, a systems architecture view, and a technical architecture profile that focuses on capabilities, not separate systems or subsystems. A capability configuration describes the operational needs, systems solutions, and technical standards to provide a warfighting or warfighting support capability.

Classes of Telephone Service

a. Class A (Official). Telephone service authorized for the transaction of official business of the Government on DOD/military installations and which requires access to commercial telephone company central office and toll trunks for the proper conduct of official business.

b. Class B (Unofficial). 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.

c. Class C (Official-Restricted). 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.

d. Class D (Official-Special). 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, which 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, which 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 and electronic warfare (IEW) systems.

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 enable the connection of computer systems for the purpose of transmitting data and other forms (e.g., voice and video) among the systems.

Communications security

Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. 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.

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
a. One of the subordinate organizations that constitute a joint force. Normally, a joint force is organized with a combination of Service and functional components.
b. An assembly or any combination of parts, subassemblies, and assemblies mounted together in manufacture, assembly, maintenance, or rebuild.
c. In logistics, a part or combination of parts having a specific function, which can be installed or replaced only as an entity.

Concept
A document or theory that translates a vision or visions into a more detailed, but still abstract, description of some future activity or end-state, principally concerned with a 3- to 15-year time frame.

Configuration
That can be expressed in functional terms (i.e., expected performance) and in physical terms (i.e., appearance and composition).

Connection Fee
The charge, if any, imposed on a subscriber by the CATV franchisee for initial hookup, reconnection, or relocation of equipment necessary to transmit the CATV signal from the distribution cable to a subscriber's receiver.

Construct
A structure built according to specific principles or using a particular set of elements. For example, house constructs include wood frames, concrete blocks, steel trusses, and geodesic domes. Computer constructs include serial, parallel, analog, and digital structures.

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, which meets the stated requirement in the least costly way. Cost effectiveness does not imply a cost saving over the existing or baseline situation; rather, it indicates a cost saving over any other 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. (JCS Pub 1)

Database
A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications.

Data Dictionary
A centralized repository of information about data such as meaning relationships and other data, origin, usage, and format.

Data element
A basic unit of information built on standard structures having a unique meaning and distinct units or values. Within the context of information systems, it is a combination of characters or bytes referring to one separate item of information, such as a name, address, or age.

Data model
A graphical and textual representation of analysis that identifies the data needed by an organization to achieve its mission, functions, goals, objectives, and strategies and to manage and rate the organization. It identifies the entities, domain (attributes), and relationships (or associations) with other data and provides the conceptual view of the data and the relationships among data.

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. AFIS/DVI is the data base manager and provides policy guidance concerning the operation of DAVIS functions. The DAVIS is accessible through Web site http://dodimagery.afis.osd.mil.

Department of Army Visual Information Production and Distribution Program (DAVIPDP)
Provides for the annual identification, funding and acquisition of VI production and distribution requirements. All Army organizations identify their requirements for non-local multimedia/VI productions and forward their requests to their supporting MACOM/FOA VI manager for validation. MACOM/FOA VI managers forward valid requirements to ODISC4 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 he or she claims to be.

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.

Document Imagery
The science and technology of producing:
a. Micro-images on microforms;
b. Binary-coded record representation of a document requiring computer processing to recreate an eye-readable document image on a viewing or printing device.

Domain
This is 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 Business/Electronic Commerce
A means of performing enterprise activities that involves the use of electronic technologies, including such techniques

as facsimile, electronic mail, World Wide Web software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

Electronic Business/Electronic Commerce Initiative
The use of electronic business/electronic commerce techniques to accomplish Army business transactions in support of defined mission objectives.

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 these types of records 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 personal identification number (PIN) or password, smart card, digitized signature, and biometrics. Crypto-graphic 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 information technology. An enterprise architecture describes the "target" situation that the agency wishes to create and maintain by managing its IT portfolio.

Environment
The conditions (e.g., physical, political, economic, and religious) within which, an architectural configuration must operate.

Executive Control and Essential Command Supervision (ECECS).
Those managerial staff functions and positions located above the direct program managerial and operational level of individual MWR programs that support planning, organizing, directing, coordinating, and controlling the overall operations of MWR programs. Executive Control and Essential Command Supervision (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 (APF) and Non-appropriated Fund (NAF) MWR assets.

Extranet
Similar to an Intranet, an extranet includes outside vendors and uses Web technology to facilitate inter-business 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.

Film or Video Clip
A limited form of visual information (VI) product. An assemblage of motion picture footage or videotape (usually documentary) in continuity, usually without editorial or optical effects, and normally without audio except that recorded during the documentation using single system sound or video recording. Simple titles may be used for identification purposes.

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 AEAFD, 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). (AR 5-22)

Government Performance and Results Act (Public Law 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. (JCS Pub 1) Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights.

Information Assurance Vulnerability Assessment (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 (IER)
Substantive content, format, throughput requirements, and classification level.

Information Management
Activities required to coordinate, plan, organize, analyze, integrate, evaluate, and control information resources effectively.

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, and 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 information technology.

Information System
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Information Systems Security (ISS)
The overarching term which encompasses signal security and computer security. The term provides for integrating SIGSEC and COMPUSEC efforts into a unified approach to protecting sensitive (classified and unclassified) information in electronic form during transmission or while contained in information processing systems.

Information Technology (IT)
a. With respect to an executive agency, IT means 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 (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
b. The term " information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
c. Notwithstanding subparagraphs (A) and (B), the term"information technology"does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Infostructure
The infostructure is defined as the shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities 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.

Intranet
A computer network that functions like the Internet, using Web browser software to access and process the information that employees need, but the information and Web pages are located on computers within the organization/enterprise. A firewall is usually used to block access from outside the Intranet. Intranets are private Web sites.

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 are satellite on it for support.

Installation Information Infrastructure Architecture (I3A)
The I3A is a standard communications infrastructure architecture for the U.S. Army installations embracing the JTA-A for all technology implementations. The installation infrastructure objective architecture designs are "roadmaps" for installation managers to plan, manage, budget and migrate towards.

Integrated product team (IPT)
A work group composed of representatives from all appropriate functional disciplines working with a team leader to build successful and balanced programs, identify and resolve issues, and make sound and timely recommendations to facilitate decision-making.

Integration
The process of making or completing by adding or fitting together into an agreed upon 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.

Interconnection
The linking of interoperable systems.

Interface
A boundary or point common to two or more similar or dissimilar telecommunications systems, subsystems, or other entities against which or 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 between them and/or their users.

Intranet
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 (ftp), and other Internet services.

IT Architecture
An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals 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 information technology acquisitions of the Army. The process will include the selection, management, and evaluation of IT investments.

IT Investment Portfolio
A collection of IT investments that represent the best balance of costs, benefits, and risks and is designed to improve the overall organizational performance, maximizes 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 IT/C4I, 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.

Joint Visual Information Services (JVIS)
Visual information services operated and maintained by a DOD Military Department to support more than one DOD organization.

Lessons learned
Descriptions of operational problems encountered or opportunities missed that are directly related to the use or absence of particular technologies, methods, or standards.

Life cycle
The total phases through which an item passes from the time it is initially developed until the time it is either consumed in use or disposed of as being excess to all known materiel requirements.

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 three budget and execution years of the MDEP, and the PDIP is the five 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.

Meta-data
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.

Micrographics
The science and technology of document and information microfilming and associated microfilm systems.

Mission
A group of tasks, with their purpose, assigned to military organizations, units, or individuals for execution.

Mission-Related
Processes and functions that are closely related to the mission (e.g., the mission of Direct and Resource the Force has the mission-related functions of planning, programming, policy development, and allocating of resources.

Mixed Media
A combination of one or more visual information media and one or more non-VI media, such as a filmstrip and an accompanying printed material.

Modeling and simulation (M&S)
Representations of proposed systems (constructive and virtual prototypes) embedded in realistic, synthetic environments to support the various phases of the acquisition process, from requirements determination and initial concept exploration to the manufacturing and testing of new systems and related training.

Morale, Welfare, and Recreation (MWR) Programs
Those military MWR programs (exclusive of private organizations as defined in DOD Instruction 1000.15) located on DOD installations or on property controlled (by lease or other means) by the Department of Defense 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
Multimedia is 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 -

a. Involves intelligence activities;
b. Involves cryptologic activities related to national security;
c. Involves command and control of military forces;
d. Involves equipment that is an integral part of a weapon or weapons system; or
e. Is critical to the direct fulfillment of military or intelligence missions.(Definition is from P.L. 104-106, The Clinger-Cohen Act of 1996 (formerly Div E, Information Technology Management Reform Act, Defense Authorization Act of 1996)

Negotiation
The communication by any means of a position or an offer on behalf of the U.S., the 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 approving authority will authorize the requesting command to initiate and conduct the negotiation.)

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.

Node
A location at which information is produced, consumed, or transformed. It can be further typed by its use in the development of architecture (e.g., operational element node, PSE Prime Mission Element [PME] node, or organizational node). In the context of operational architectures (OAs), it is an organization, organizational element, activity, or a person depending on the objectives of the specific architecture and the level at which the architecture is being developed. Either notional or physical assignments can be used depending on the needs and objectives of the specific architecture effort.

Nonappropriated Funds (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 (NAFI)
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.

Non-Public Data/Information
Data/Information which is either personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a Freedom of Information Act exemption, or is 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 (OA)
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 element
The forces, organizations, or administrative structure that participate in accomplishing tasks and missions.

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.

Operational requirements document (ORD)
A formal acquisition document used to define a proposed system as a whole and specify the objective and minimum (threshold) performance levels that the system must provide.

Organizational level
The horizontal/vertical viewpoint of an organization having subordinate components, e.g., MACOM, corps, division, brigade.

Outcome-based criteria
An assessment of the results of a program activity as compared to its intended purpose.

Output measure
Tabulation, calculation, or recording of activity of effort

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 to which clients are satisfied) and outcomes (the results of a program activity compared to its specific contributions to program objectives.

Periodical
A non-directive 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 system (PPBES)
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Printing
The processes of composition, platemaking, presswork, and binding, including micro-publishing, 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 nonfederal 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. It does not include making grants or cooperative agreements.

Program costs
Total life cycle costs less operations and support costs.

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.

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 of the Department of the Army or because of the informational value of the data in them.

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 respect to information creation, information maintenance and use, and information disposition in order to achieve

adequate and proper documentation of the policies and transactions of DA and effective and economical management of DA operations.

Records Management Program
A program that includes elements concerned with the life cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information and Privacy Acts.

Reproduction
Making copies from an earlier generation of materials, including all copies beyond the original or master copy.

Requirements determination
The process of deciding what is essential to support a strategy, campaign, or operation.

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 (CJCSI 6250.01).

Self-service copying
End user operated copying and reproduction using automatic copy processing or copier/reproduction devices (excluding those items capable of producing multicolor copies) having a throughput speed of 69 copies per minute or less.

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.

SIGINT
A category of intelligence information comprising all COMINT and electronics intelligence (ELINT).

Smart card
A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuit chips (ICC) 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 (e.g., compiler, library routines, manuals, circuit diagrams); usually contrasted with hardware.

Spam
Widely posted junk mail.

Spamming
Posting or emailing unsolicited messages to a large number of mailing lists.

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 goal
Long-range changes target that guide an organization's efforts in moving toward a desired future state.

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 non-appropriated fund activity that procures services made available pursuant to the terms of the franchise agreement.

Support agreement
It is an agreement to provide recurring base operations 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. (JCS Pub 1) 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.

Synchronization
See data synchronization.

Systems architect
Responsible for integration and oversight of all Army information systems. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) is the Army's Systems Architect.

Systems Architecture (SA)
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 sixteen-year strategic planning horizon that includes the six-year span of the program (POM) years plus an additional 10 years. TAP presents comprehensive and cohesive strategic, mid-term 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 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 TA 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.

Technical architecture profile
The parts of the JTA-ARMY that are relevant to a specific operational architecture view and a specific systems architecture view in support of a capability configuration.

Technical documentation (TECDOC)
Documentation of an actual event made for purposes of evaluation. Typically, technical documentation contributes to the study of human or mechanical factors, procedures, and processes in the fields of medicine, science, logistics, research, development, test and evaluation, intelligence, investigations, and armament delivery (see VIDOC).

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.

Telecommunications center (TCC)
Facility, normally serving more than one organization or terminal, responsible for transmission, receipt, acceptance, processing, and distribution of incoming and outgoing messages.

Telecommuting
Telecommuting is defined as 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 doctrine, training, leader development, organizations, materiel, soldiers (DTLOMS) 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, file, a Web page, an application, and so forth). 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)
Is that aspect of information technology that pertains to the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery, with or without sound, for the purpose of conveying information.

VI Activity
An organizational element or a function within an organization in which one or more individuals are classified as visual information (VI), 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 non-technical 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 visual information (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 which loans, issues, and maintains a inventory of motion media, imagery and/or equipment.

VI management office
Staff Office at major command, 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 visual information (VI) still and motion films, tapes, discs, or graphic arts. Includes the original, intermediate and master copies, and any other recorded imagery that is retained.

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, and related administrative records.

VI Records Center
A facility, sometimes specially designed and constructed, for the low-cost and efficient storage and referencing of semi-current 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:

a. Result in obtaining a visual information product.

b. Support the preparation of a completed VI production such as photographing, processing, duplicating, sound and video recording, instrumentation recording, film to video transferring, editing, scripting, designing, and preparing graphic arts.

c. Support existing VI products such as distribution and records center operations.

d. 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 non-production 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
Defined in AR 71-9 as 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, online chat forums, searching, content, newsfeeds and others.

Web site
A location on the Internet; specifically it refers to the Point of Presence (POP) 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.