

Department of the Army  
Pamphlet 25-1-1

Information Management

# Information Technology Support and Services

Headquarters  
Department of the Army  
Washington, DC  
25 October 2006

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

DA PAM 25-1-1  
Information Technology Support and Services

This rapid action revision dated 25 October 2006--

- o Adds new guidance for family member use and access of Army Knowledge Online (chap 3).
- o Updates procedures on Army Knowledge Online configuration management changes from previous edition (chap 3).
- o Adds minor change for the Army Web site registration process (chap 8).
- o Updates user processes for acquiring Information Technology support and services from the Army Small Computer Program (chap 9 and chap 11).
- o Provides minor updates and clarification throughout the pamphlet.

This administrative revision dated 20 March 2006--

- o Corrects typographical errors.
- o Changes Web site address for Web-based training (para 8-4b).
- o Corrects listings of cited paras in appendix A.

This major revision, dated 1 November 2005--

- o Consolidates Army Regulation 105-6 and Department of the Army Pamphlet 25-5 with this pamphlet.
- o Updates purpose, exceptions, and general information (chap 1).
- o Documents the procedures for information resource management, including budgeting, funding, billing, and internally controlling information resources--for example, systems, equipment, and services. The focus is director of information management operations funded primarily with Operations & Maintenance, Army (chap 2).
- o Provides an overview of Army Knowledge Management and its strategic plan. Adds guidance on the capabilities and use of Army Knowledge On-Line, including self-service functions, enterprise search and information retrieval, content management enterprise collaboration, enterprise collaborative environment, requirements and functional configuration management, joint capabilities, and the development of communities of practice/structured professional forums (chap 3).
- o Adds guidance on governance of the Army enterprise architecture, including its development, maintenance, and usage (chap 4).

- Implements the Army Net-Centric Data Management Program with information regarding terms and concepts, roles and functions, and the layers of data management (chap 5).
- Adds and updates guidance on managing information technology at the installation level. Guidance is provided on the roles of the Installation Management Agency, the Network Enterprise Technology Command, the regional unit/regional chief information officer, the director of information management, and the information management officer (chap 6).
- Addresses concerns regarding information technology support for telework, information access for persons using assistive technology, and information technology requirements for military construction projects. Implements new Public Laws and Army/Defense processes and practices concerning the use of technologies such as e-mail, the Internet, the Web, electronic business/electronic commerce, cellular telephones, satellite telecommunications, and others (chap 7).
- Provides guidance and procedures for Army public Web site management, including training and compliance requirement, director of information management Web site administration, and activities to ensure quality, reliable, and accessible information (chap 8).
- Adds and updates procedures for managing hardware and software assets, which includes procedural aspects of developing requirements, resourcing, acquisition, and contracting for information technology services and supplies (chap 9).
- Updates guidance on telecommunications systems, including additional and updated guidance on local area network/wide area network, network operations, base communications services, and messaging services (chap 10).
- Updates guidance on strategies for the delivery and support of information technology systems and services, including the redistribution of information technology assets, use of Government purchase cards for information technology assets, administering information technology contract performance, and electronic purchases (chap 11).
- Adds a sample telework application and agreement, a telework safety checklist, a supervisory-employee checklist, and telework termination form (app B).
- Provides additional and updated procedures and guidance regarding the billing and accounting for official phone services, unofficial phone service, long-haul services, and cable television (app C).



## Information Management

### Information Technology Support and Services

---

By Order of the Secretary of the Army:

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

Official:

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

---

**History.** This publication is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

**Summary.** This pamphlet provides procedures for acquiring and managing information technology support and services and applies to information technology developed for or purchased by the Department of Army. It establishes procedures for the administration of information resources and the supporting technology requirements. This pamphlet supports AR 25-1 in implementing Public Law 104-106 (the Clinger-Cohen Act, formerly Division E, Technology Management Reform Act) and Title 10, United

States Code. Chief information officer functions and those of corresponding information management/information technology official and management processes are delineated throughout this pamphlet. These management processes involve strategic planning, business process analysis and improvement, capital planning and investment control, and information technology performance measurements. Visual information, records management, and publishing procedures are covered in other publications and are not included in this update.

**Applicability.** This pamphlet applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve. It also applies to the information technology at all Army installations, activities, and communities.

**Proponent and exception authority.** The proponent of this pamphlet is the Chief Information Officer/G-6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may

request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through higher headquarters to the policy proponent. Refer to AR 25-30 for specific guidance.

**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, CIO/G-6, CIO Policy Decision (SAIS-GKP), 107 Army Pentagon, Washington, DC 20310-0107.

**Distribution.** This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

---

#### Contents (Listed by paragraph and page number)

##### Chapter 1

##### Information Technology Management, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Exceptions • 1-4, page 1

General • 1-5, page 1

---

\*This pamphlet supersedes DA Pamphlet 25-1-1, dated 20 March 2006.

## **Contents—Continued**

### **Chapter 2**

#### **Information Resources Management, page 1**

Command, control, communications, and computers/information technology in the Army's Strategic Plan • 2-1, page 1

Army Knowledge Management Strategic Plan • 2-2, page 2

Information technology capital planning and investment management • 2-3, page 2

Results and performance-based strategic management • 2-4, page 5

Planning, programming, budgeting, and execution for information technology requirements/capabilities • 2-5, page 12

Information technology waiver requirements process • 2-6, page 13

Information Technology Management Career Program-34 • 2-7, page 15

### **Chapter 3**

#### **Army Knowledge Management and Army Knowledge Online, page 16**

##### *Section I*

*Army Knowledge Management Overview, page 16*

Army Knowledge Management Strategy Plan • 3-1, page 16

The guiding principles of Army Knowledge Management • 3-2, page 16

##### *Section II*

*Army Knowledge Online Overview, page 17*

General • 3-3, page 17

Enterprise user accounts and access • 3-4, page 17

User assistance • 3-5, page 20

Self-service functions • 3-6, page 21

Enterprise search and retrieval of information • 3-7, page 21

Content management enterprise collaboration • 3-8, page 21

Enterprise collaborative environment • 3-9, page 22

Requirements and functional configuration management • 3-10, page 23

Joint capabilities • 3-11, page 23

### **Chapter 4**

#### **Army Enterprise Architecture, page 24**

Utilization • 4-1, page 24

Governance • 4-2, page 24

Architecture development plans • 4-3, page 25

Development • 4-4, page 25

Maintenance • 4-5, page 26

Army specific architecture development and validation requirements • 4-6, page 26

### **Chapter 5**

#### **Army Net-Centric Data Management Program, page 27**

General • 5-1, page 27

Terms and concepts • 5-2, page 28

Roles and functions • 5-3, page 30

Layers • 5-4, page 33

### **Chapter 6**

#### **Managing Information Technology at the Installation: Support and Organizational Constructs, page 36**

General • 6-1, page 36

Installation Management Agency • 6-2, page 36

Network Enterprise Technology Command regional units and regional chief information officers • 6-3, page 36

Director of information management • 6-4, page 37

Information management office/officer concept and functions • 6-5, page 40

## Contents—Continued

### Chapter 7

#### **Information Technology Management and User Principles and Procedures, page 44**

Information transmission economy and systems discipline • 7-1, page 44

Official and authorized uses of telecommunications and computing systems • 7-2, page 45

Information technology support for official spouse volunteers and statutory volunteers • 7-3, page 45

Support for health, morale, and welfare/morale, welfare, and recreation telecommunications • 7-4, page 46

Information access for the disabled • 7-5, page 46

Information technology support for telework/telecommuting • 7-6, page 48

Assuring information quality • 7-7, page 48

Training • 7-8, page 51

Directories • 7-9, page 52

Information technology requirements in military construction projects • 7-10, page 53

### Chapter 8

#### **Army Public Web Site Management, page 55**

Web site planning and sponsorship • 8-1, page 55

Content propriety and quality • 8-2, page 56

Usability criteria • 8-3, page 57

Training and compliance • 8-4, page 58

Consistent and nonredundant information • 8-5, page 58

Federal law, regulation, and policy compliance • 8-6, page 59

Director of information management Web site administration • 8-7, page 59

### Chapter 9

#### **Software and Hardware Asset Management, page 61**

Acquisition • 9-1, page 61

Information processing services • 9-2, page 64

Technical documentation • 9-3, page 65

Server consolidation • 9-4, page 66

Document management • 9-5, page 67

Electronic signatures • 9-6, page 67

Army information technology registry management and user principles and procedures • 9-7, page 68

### Chapter 10

#### **Telecommunications, page 72**

Network systems • 10-1, page 72

Network operations • 10-2, page 73

Local leased base communications services • 10-3, page 78

On-installation telephone services • 10-4, page 80

Off-installation telephone services • 10-5, page 81

Messaging services • 10-6, page 81

Long-haul services • 10-7, page 82

Video teleconferencing • 10-8, page 85

Satellite systems and services • 10-9, page 87

Land Mobile Radio Program • 10-10, page 89

Other Army radio systems • 10-11, page 89

Army radio frequency spectrum management • 10-12, page 90

### Chapter 11

#### **Delivery and Support of IT Systems and Services, page 91**

General • 11-1, page 91

Acquisition and delivery strategies • 11-2, page 92

Redistribution and disposal of information technology assets • 11-3, page 94

Use of Government purchase cards for purchase of information technology assets • 11-4, page 95

Administering information technology contracts performance • 11-5, page 96

## Contents—Continued

Electronic purchases • 11–6, *page 97*

### Appendixes

A. References, *page 98*

B. Sample Telework Application and Agreement, *page 103*

C. Funding, Billing, and Accounting for Information Resources, *page 108*

### Table List

Table 3–1: Account categories and types, *page 18*

Table 3–2: Collaborative Web sites, *page 23*

Table 9–1: Table of functional proponents, *page 69*

Table 9–2: Addition information required when submitting for webification exemption, *page 70*

Table 10–1: Joint to Army levels mapping, *page 77*

Table 10–2: Organizational levels to entities mapping, *page 78*

Table 10–3: Theater video operations center contacts, *page 86*

### Figure List

Figure 2–1: Building the enterprise solution, *page 5*

Figure 2–2: Hierarchy of FY2004 IT metrics, *page 10*

Figure 2–3: Relationship of IT/IV metrics and ISR, part III, *page 10*

Figure 2–4: Reporting process diagram, *page 11*

Figure 2–5: IT Metrics reporting timeline, *page 12*

Figure 2–6: AKM goal 1 waiver workflow, *page 14*

Figure 4–1: Army architecture validation process, *page 27*

Figure 7–1: Claim processing matrix, *page 50*

Figure 10–1: NETOPS mission areas and function, *page 73*

Figure 10–2: Information management services, *page 74*

Figure 10–3: Service-level management process, *page 76*

Figure C–1: List of telecommunications bill certification actions, *page 110*

Figure C–2: Optional measures to reduce telecommunications costs, *page 112*

### Glossary

## **Chapter 1 Information Technology Management**

### **1–1. Purpose**

This publication provides operational procedures and practical guidance to Army organizations furnishing and receiving information technology (IT) services, products, and support. The primary focus of this document is the implementation of policies mandated by Army Regulation (AR) 25–1. Its emphasis is on identifying and describing implementing procedures, explicit and implied, stemming from Defense policies and Federal authorities, to include the Clinger–Cohen Act (Title 40, United States Code, Subtitle III); Paperwork Reduction Act (as amended) (44 USC Chapter 35); and Office of Management and Budget (OMB) Circular A–130.

### **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 publication are explained in the glossary.

### **1–4. Exceptions**

The pamphlet does not address telecommunications service within the National Capital Region. The Defense Telecommunications Service—Washington per Department of Defense Directive (DODD) 4640.7 and Department of Defense Instruction (DODI) 5335.1 furnishes telecommunications services and equipment within the National Capital Region. AR 25–1 has the overarching Army policy for records management, printing and publishing, and visual information; however, procedures for those functions are not addressed in this pamphlet. For records management, see AR 25–400–2, AR 25–50, and AR 25–51; for printing and publishing, see AR 25–30 and Department of the Army Pamphlet (DA Pam) 25–40. For visual information, see DA Pam 25–91.

### **1–5. General**

The scope of this pamphlet includes all organizational levels. Special emphasis is given to IT support and services provided at the operational level. An essential principle is having a single organization at the installation, community, or corresponding entity charged with overseeing the delivery of IT services throughout the installation. This has been referred to as the “single director of information management (DOIM) concept.” There are several factors making this arrangement vital for good stewardship of the Army’s IT funds. Economies of scale, especially on larger installations, give leverage in IT acquisitions, and the development of required infrastructure can be approached best as a single utility to be provided to all installation customers. Otherwise, enterprise architecture is not practical or feasible. The concept also facilitates creation of a central clearinghouse for IT acquisitions at the operational level to ensure architectural compliance.

## **Chapter 2 Information Resources Management**

The efficient and effective use of information resources has a direct impact on the Army’s ability to perform its missions. Per 40 USC Subtitle III, the role of the Chief Information Officer/G–6 (CIO/G–6) is to manage command, control, communications, and computers/information technology (C4/IT) and execute information resources management (IRM) functions. Chapters 2 and 3 of AR 25–1 identify and describe the CIO mission and functions. Managing information resources for the improvement of Army’s performance of its mission is primary among those roles.

### **2–1. Command, control, communications, and computers/information technology in the Army’s Strategic Plan**

C4/IT planning is an integral part of the Army’s strategic plan (Total Army Plan (TAP)). TAP provides the strategic framework for sound programming decisions and includes Army strategic direction, required operational capabilities, and the programmatic guidance that feeds the C4/IT capital planning process. The CIO/G–6 manages resources supporting a specific set of C4/IT management decision packages (MDEPs) and manages a process to select, control, and evaluate the Army’s C4/IT investments to manage C4/IT and comply with 40 USC Subtitle III. This compliance involves building a strategy based on the CIO’s mission statement and TAP goals and objectives, which lay out approaches for achieving these goals with particular resource choices. All risk factors—for example, technical, managerial, legislative, and so on—are articulated in this process. Senior information management (IM)/IT officials at major Army commands (MACOMs) and installations must be engaged in the development of a similar process for investment planning at their respective levels.

## **2-2. Army Knowledge Management Strategic Plan**

*a.* The purpose of the Army Knowledge Management (AKM) Strategic Plan (SP) is to document the Army's strategy to implement the concepts of a network-centric, knowledge-based organization. The AKM SP is aligned to Army and Department of Defense (DOD) strategic planning documents and guidance and is approved by the Secretary of the Army and the Chief of Staff, Army (CSA). It is applicable to the total Army enterprise—the Active Army, Department of the Army (DA) civilians, the Army Reserve (AR), and the Army National Guard (ARNG)—during peace and war. It applies to all mission areas, whether in support of the institutional Army or the operational Army. The vision applies to soldiers, civilians, field units, commanders, Headquarters (HQ) DA staff elements, and MACOMs. The goals are to be achieved at all levels across the enterprise, with an emphasis on standardized, enterprise-level mission and business practices. As the Army functional proponent for the AKM strategy, the CIO/G-6 facilitates and oversees strategy and execution. The most current plan can be found on Army Knowledge Online (AKO) ([www.ako.army.mil](http://www.ako.army.mil)), on the AKM Web page, under the CIO/G-6 community page.

*b.* The purpose of the AKM implementation plan (IP) is to identify the Army implementation initiatives that support the AKM vision, goals, and objectives, as stated in the AKM SP. The Army CIO/G-6 develops the plan, overseeing the execution of the initiatives, monitoring, tracking, and reporting on the status of all initiatives, and facilitating the development of performance measures. Domain leads are key stakeholders in the planning and execution of the AKM SP and IP. The AKM IP's associated performance measures are reported through the Strategic Readiness System (SRS) and posted on AKO, AKM Web page, under the CIO/G-6 community page.

*c.* The Army CIO has organized itself to facilitate implementation and performance management of the AKM strategy. The goals establish a collaborative business model to accomplish Army missions. The CIO will track and measure AKM progress and accomplishments by evaluating the performance of the goals, objectives, and initiatives relative to the expected outcomes. The AKM IP milestones and deliverable schedule reflect the baseline, as well as the most current status of all actions in the plan. The published version of the AKM IP is the baseline against which all status reports are developed and posted to AKO.

## **2-3. Information technology capital planning and investment management**

The capital planning and investment management (CPIM) strategy is founded upon the concept of reviewing and evaluating all C4/IT related investments and establishing a recommended funding priority listing based upon the capabilities the proposed IT-related investments will provide for the Army. The recommended prioritization listing is used as a reference and support tool throughout the planning programming and budgeting execution (PPBE) and acquisition processes. The CPIM process fully incorporates the direction from 40 USC Subtitle III and relevant best business practices.

*a.* The goals of the CPIM processes include—

(1) Providing for the selection of information technology investments, the management of such investments, and the evaluation of the results of such investments.

(2) Integrating with budget, financial, and program management decision processes This includes minimum criteria to be applied to undertake a particular investment in information systems/information technology, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information systems investment projects.

(3) Providing for identifying information systems investments that would result in shared benefits or costs.

(4) Providing the means for senior management personnel to obtain timely information regarding the progress of an investment or an information system.

(5) Providing the linkage for each IT-related investment area to a defined TAP capability.

*b.* The IT portfolio is the central piece in the development of the CPIM process and is the formalization of an IT portfolio for the Army to document and review all IT-related investments.

(1) Structuring the portfolio with three areas enables like-type analysis/review of funding requirements and recognition of interdependencies and fielding timelines within these areas. From there, portfolio analysis as a whole can be accomplished with the resultant product being a recommended funding prioritization listing.

(2) Additionally, the portfolio structure allows for linking to the DOD information technology portfolio management process, Joint Warfighting Capability Assessment (JWCA) areas (battlespace awareness, command and control, force application, protection, focused logistics, and network centrality), the six business domains (accounting and finance, acquisition, human resources management, installations and environment, logistics, and strategic planning and budgeting), and the underlying enterprise information environment (EIE).

(3) The CPIM three subportfolio areas, each with corresponding investment areas, are—

*(a)* Enterprise enablers, which include architecture, information assurance, network operations (NETOPS), and AKM.

*(b)* Communications and infrastructure, which include battlefield communications and network management, satellite communications, and C4/IT infrastructure.

*(c)* Functional applications, which include soldier training, focused logistics, human resource management, and battlespace awareness.

c. The CPIM process is a tool for making prudent capital planning investment decisions.

(1) Executive-level officials monitor and approve Capital Planning Investment Management recommendations. The Army CIO reviews and approves the CPIM prioritization results and recommendations, which are foundational to developing the C4/IT investment strategy. As the functional proponent for Army's C4/IT investment strategy, the CIO also develops the necessary relationships with decision-makers in the budget process to reassure them that the CPIM process recommendations make the best use of scant IT resources and are in line with building the Army enterprise.

(2) The CPIM results and recommendations are then briefed to the CIO Executive Board (EB), whose membership comprises a representative group of key stakeholders. The CIO EB provides the necessary oversight by reviewing and endorsing capital planning investment recommendations.

(3) The CPIM process is used for analyzing, tracking, and evaluating the risks and results of all major capital investments made for information systems/ information technology. The process covers the life of each system and includes explicit criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments.

d. The CIO investment strategy is developed through the collaborative efforts of the Army's multifunctional community of C4/IT stakeholders, to include joint representation, that collectively determine the "best value" investment solutions for the Army's most critical C4/IT requirements.

(1) The process incorporates strategic reviews, performance measures, capability gap assessments, risk assessments, and interdependency assessments each year for the multitude of investment areas. To accomplish this task, the CIO/G6 depends heavily upon subject matter experts within each investment area for the critical analysis and review of proposed IT-related investments, and for each of the investment areas, an investment area leader is identified.

(2) Investment area leaders are central to the information gathering and formulation of such information so that it can be presented for critical analysis and weighting during the prioritization process. In their role, they have many functions, including—

(a) Representing their investment area's needs and priorities, ensuring identification of capability and mission needs.

(b) Identifying opportunities, assessing capability gaps, and prioritizing investment area capabilities and services.

(c) Reviewing existing programs and systems within the investment area, assessing the ability to contribute to Future Force requirements, recommending which should be accelerated, sustained, transformed or eliminated.

(d) Coordinating with appropriate program evaluation group (PEG) representatives and program managers who have interests within their investment area.

(e) Rationalizing all existing and new capabilities and services within their Investment Area, insuring they fit within the integrated architecture.

(f) Reviewing budget submission for programs/systems within investment area to insure support of any transition/transformation plans.

(g) Serving as conduit among DOD JWCA area, business domains, and/or EIE representatives.

(3) To ensure accuracy and completeness of all information presented, it is critical that investment area leaders maintain close, cooperative relationships with key players in their respective communities. The following list is only a starting point; other representatives may be included as required. Key players include—

(a) PEG and CIO/G-6 representatives to each PEG.

(b) Program managers and subject matter experts (as appropriate).

(c) Battlefield operating systems and functional representatives.

(d) Army Budget Office, Office of the Deputy Chief of Staff, G-3 (ODCS, G-3), and ODCS, G-8 leadership (as appropriate).

(e) Each MACOM and regional CIO (RCIO) Representatives (as appropriate), including NETCOM/9<sup>th</sup> Army Signal Command, AR, and ARNG.

(f) Joint and DOD counterparts.

(4) The capital planning and investment strategy process core purpose is to advise the acquisition and execution communities when and where to stop, slow, maintain, accelerate, or start funding a C4/IT capability that supports our Nation's warrior missions, from an "enterprise" investment approach. In this vein, linkage to the PPBE cycle is essential to ensure that prioritization results are available during the funding deliberations. The CPIM process is a continuous one, even though it is shown in a linear format. Throughout the year, CPIM meetings keep the lines of communications open and information flowing between stakeholders and investment area leaders. The focus of efforts throughout the year may shift from data gathering, to analysis, to strategic matching of capabilities versus requirements, and to actual funding prioritization stage, which is shared with the key players in the PPBE process to aid in their efforts.

(5) The critical part of the CPIM process is the analytical stage when programs/systems are evaluated for prioritization within the investment strategy. This evaluation and selection stage of the process is critical to a sound investment strategy and is dependent upon cogent and timely data to support the prioritization discussions. The collection of good data and the knowledge to substantiate it are essential in the development of sound business case information—for

example, defined outcomes, benefits, capabilities, full life-cycle costs as well as key interdependencies and known risks.

(a) Each program/system will be evaluated within its investment area and then across the totality of IT requirements using the following criteria: strategic alignment; criticality of capability to mission accomplishment; performance and outcome achievement; risk; and functional IT interdependency.

(b) Key to the entire deliberative process is the human common sense check—that is, when the results generated using an automated decision tool are reviewed by the collective group, incorporating its wisdom and insights. This check stage is essential for reconciliation and the identification of where priorities can be adjusted to better meet the requirements of the Total Army.

e. The collaborative development of the recommended IT prioritization list begins the control step in the IT portfolio management process. Key to this step is the support of the leadership in the use of the IT recommended capabilities priorities list as the funding deliberations and decisions are undertaken.

(1) The IT prioritization list, developed through the CPIM process, becomes the framework for the Army C4/IT investment strategy, adding value to the Army C4/IT investments in two respects:

(a) Planners and programmers work collaboratively to determine optimal, affordable C4/IT investments that will deliver a “capabilities-based return on investment” in support of the Army TAP, the Army Strategic Planning Guidance, and the DOD/Joint Strategic Planning Guidance

(b) The investment strategy is based upon a crosscutting analysis of the value that C4/IT investments can leverage, or balance, across the mission areas of the TAP.

(2) Once the prioritization list and funding strategy are developed, they are briefed to the CIO/G–6 for refinement/revision/approval prior to briefing the CIO EB for information/concurrence. The views offered by the investment strategy allow the Army Leadership to see the IT interdependencies and linkages within the investment strategy, fostering a more informed decision process when making IT related funding decisions. The Army CIO EB’s review ensures the Army’s IT funds are strategically aligned with enterprise-wide mission needs to achieve both dominant warfighting capabilities and world-class business process success.

(3) The vetting of the investment strategy through the CIO EB is essential as its awareness and concurrence with the recommended investment priorities codifies the investment strategy and lends support to the recommendations prior to briefing the results to the PEGs and MACOMs.

(4) Briefing the PEGs and the MACOMs early in the program objective memorandum (POM) cycle is essential for full understanding by all concerned in the POM build of the CIO/G–6 recommended priorities.

f. Return on investment (ROI) is an area which the military has historically had difficulty with, as the Army is a not-for-profit organization, and therefore the fiscal soundness of some investments is balanced against the increased capability delivered as a result of the expenditure. In short, a sound investment for the Army provides the best services for our men and women in uniform and civilian service, in the most timely and affordable manner. For a project manager, return on investment can be determined by using measures such as, delivery on time, within cost estimates, with the final product meeting all performance requirements. For the CIO/G–6 investment strategy process, evaluating return on investment is not as simple, because the CPIM process develops a recommended funding prioritization list for use by the PEGs during the POM process. The IT investment strategy process looks to optimize planned expenditures, ensuring they are in line with architectural requirements and fully supportive of the Army’s strategy for building and supporting the Future Force. The investment management process supports the Army Leadership in the POM and transformation efforts within the IT arena. This review can lead to measures for potential, such as—

(1) How were the results of the IT prioritization efforts used by the PEGs during POM build?

(2) Were the priorities linked to the Future Force requirements?

(3) Did the prioritization process identify legacy or outdated IT systems for which funding could be reinvested?

(4) Did the prioritization process support the user such that migration of funds to pay for IT requirements was reduced?

(5) Was there an improvement in the “business capabilities” provided to the Army as result of the coordinated investment strategy?

(6) Did the investment strategy coordinate the Army’s technical capacity improvements across the institutional and tactical forces, streamlining connectivity with an increase in capability, while controlling cost expenditures? The development of the metrics to be used in evaluation of the process and in determining how the Army uses the results of the process during the POM process are incorporated into the CIO/G–6 portion of the SRS. Metric development and process evaluation are critical as feedback mechanisms, keeping the CPIM relevant. Critical evaluation of the conduct of the CPIM process, how the results unfold, and how the CPIM product is used during the POM development process is essential to the cyclical nature of CPIM. Throughout the cycle year, changes are made to the process based upon guidance received or information obtained. At the end of each cycle year, a meeting with the investment area leaders focuses on modifications to the process for the next year’s cycle to optimize our efforts and facilitate a more in-depth product more responsive to the needs of the POM developers.

g. The capital planning and investment strategy process is a long-term solution for the prioritization of the Army’s

IT-related investments. Only through a comprehensive enterprise portfolio management process can a coordinated, cohesive IT funding strategy become a reality. As with any “new process”, it takes time to get the system in place, increase the awareness within the respective communities and set the foundation for procedures that will be used. Only when this awareness and foundation stage is complete can the process actually begin to function. See figure 2–1 for important elements in building the enterprise solution.

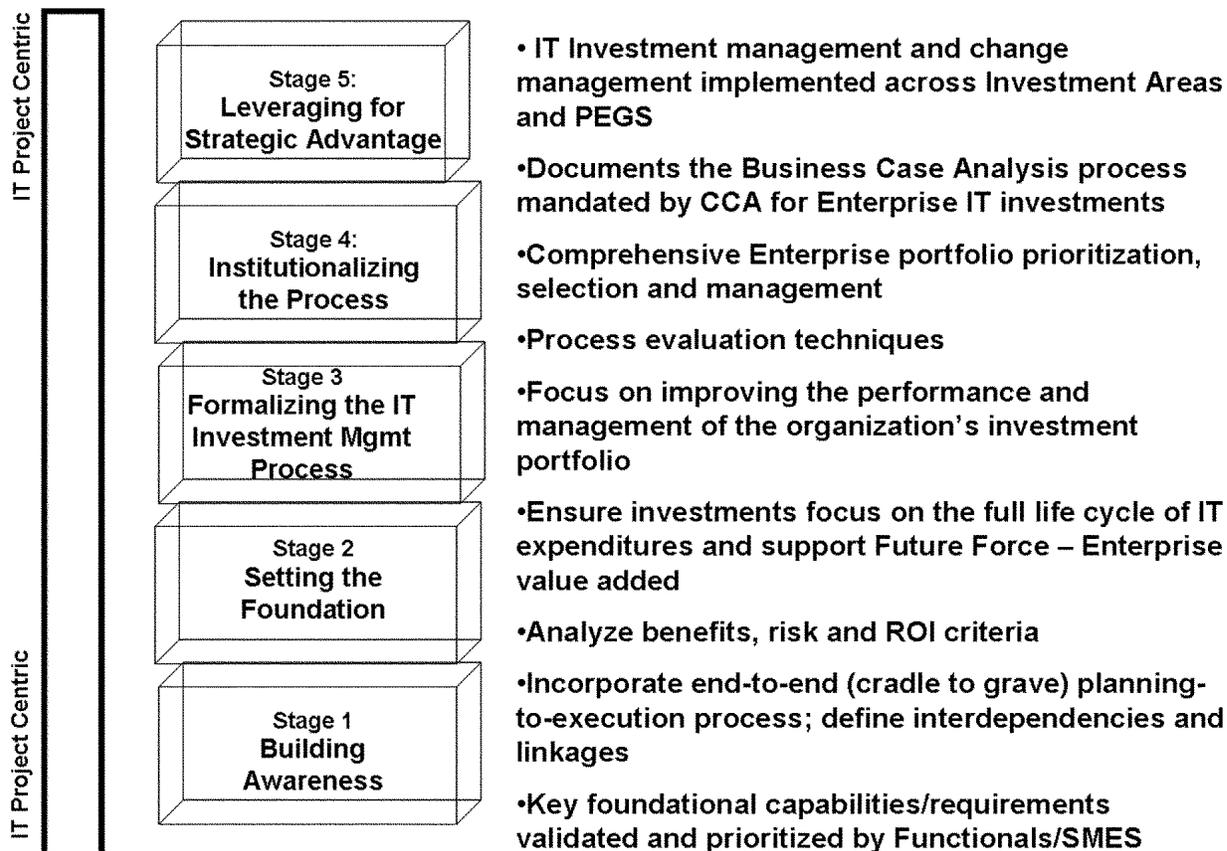


Figure 2–1. Building the enterprise solution

- (1) The key ingredients for full functionality of the CPIM process include:
  - (a) Good data/results that reflect actuality with reasonable fidelity for planning (life-cycle business case information, risks, performance measures, interdependencies).
  - (b) Accountable asset management, complete with postimplementation reviews.
  - (c) Leadership and decision processes that are synchronized and use a single, authoritative, list of investments.
  - (d) Buy-in to an acquisition strategy and process with proper incentives to promote investment choices that are in line with the Army enterprise.
- (2) The CPIM process makes the best use of resources available in meeting the diverse requirements of the Army, evolving to meet the challenges of the future. This effort requires commitment and collaboration across the Army to guarantee a sound, cohesive and responsive resourcing strategy, one with enough flexibility to respond to emerging requirements, integrating the solutions for the new requirements into an overall strategy, maximizing synergies gained from an Army-wide view. This effort ensures the Army meets the requirements and provides the best support possible to the Soldier during the transition to a modular, joint and expeditionary Army.

## 2–4. Results and performance-based strategic management

a. *General.* Performance measurements and results-based management play a pivotal role in transforming information management from a purely technical support function to one of managing information as a strategic asset. The Congress has enacted a statutory framework to achieve these results. The framework includes the Government

Performance and Results Act (GPRA); information resources management statutes, such as 40 USC Subtitle III; and financial management statutes. Each of these reforms aims at achieving more efficient and effective performance. The Army is required to develop performance measurements to measure how well information technology, in use or to be acquired, supports its programs. The resultant action includes the benchmarking of its functional and management processes against comparable organizations in the public or private sectors in terms of cost, speed, productivity, and quality of outputs and outcomes.

*b. Policy and guidance.* AR 25–1, paragraph 3–6, contains policy on IT performance measurements.

*c. Strategy-focused organization.* To improve its mission readiness, Army has adopted the strategic management approach using a balanced scorecard to document and communicate its vision, mission, and strategy; and integrating resources to strategic management.

*d. SRS.* The SRS is Army’s strategic management system. It documents and communicates Army’s vision, mission, and strategy for all in Army. SRS captures and measures related objectives. All Army elements should align their efforts to Army’s strategy. SRS cascades the strategic objectives through HQDA staff organizations and MACOMs to subordinate elements. Led by the DCS, G–3, the SRS offers much supporting documentation on AKO, both in the Knowledge Collaboration Center and at the SRS Web site. The SRS Web site can be found on the AKO homepage, under the operations community.

*e. Army IM/IT scorecard.* The Army CIO/G–6 uses a balanced scorecard to communicate and manage the Army IM/IT strategy.

(1) In fiscal year (FY) 05, the CIO/G–6 established a new vision, to deliver a joint net-centric information enterprise enabling warfighter decision superiority, and related mission, goals, and objectives which outline the strategy to achieve the vision. The CIO/G–6 goals and objectives become the Army’s IM and IT strategic objectives.

(2) CIO/G–6 has developed measures to support management/monitoring of this strategy and established performance reviews beginning in FY05.

(3) The CIO/G–6 scorecard aligns to the Army’s scorecard through related Army strategic objectives, for example, LandWarNet and Provide Relevant Information.

*f. Results and performance-based strategic management framework.* The integration of strategic objectives, performance measures, and related management processes constitutes a results and performance based strategic management framework. Goals and objectives at all organizational levels are established and linked. Measures are crafted for each objective to help identify strategy gaps and progress issues. Performance measurement is an iterative and continuous process. Management processes/controls provide the mechanisms to hold executives and staff at all levels accountable for results as indicated by the performance measures.

*g. Uses of performance measurements.* Performance measurement is a management tool and should be used by management as part of its regular periodic oversight. “Lead” measurements are predictive indicators. “Lag” measurements report whether we achieved what we set out to.

(1) Organizational leaders use performance measurements at various levels, and they have a different focus at various levels in the organization.

(a) At the enterprise level, they identify strategy gaps and progress issues. Enterprise measurements should be results based and outcome oriented.

(b) At the functional level, they report on requirements gaps and progress issues. Functional measurements can be based on the desired outcomes of the functional (domain) efforts as they feed the enterprise effort. These can be called intermediate outcomes and should help drive process-engineering efforts. For example, the capital planning and investment management process, the recruiting process, and the supply process should each develop process objectives and measures.

(c) At the program/project level, performance measurements report on cost, schedule, and performance. Program measurements can be output-oriented. These measurements indicate the program progress. Programs must also identify (intermediate) outcomes that the program aims to help achieve. These measurements indicate whether the program, even if successful, should continue.

(2) Measurements align through the alignment of objectives that they support. Enterprise strategic objectives, functional objectives, and programmatic tasks should all relate, aligned through a shared vision and mission and a cause-and-effect strategic relationship.

(a) An example may be used to illustrate performance. The program to provide installation information infrastructure should measure the execution against its program plan for a given year. This is a programmatic or output measurement. The functional use of that infrastructure is the intention of providing it. A related functional improvement measurement, such as improved functional productivity or effectiveness, would be an intermediate outcome. The ultimate reason for the infrastructure is the enterprise result. For Army, it is force readiness and successful joint employment. They are outcome measurements.

(b) Managers at each level should coordinate and align within higher and lower level objectives, using related measurements.

(c) Each level should identify outcome-oriented measurements if possible. Often one level will need to rely on a

higher level to collect the data for the higher level measurement. If a function has not improved effectiveness or efficiency based on a given improvement, the investment should be allocated elsewhere.

(3) Well-designed performance measurements enable an analysis to determine strategy gaps and operations/implementation issues. Critical to the analysis is an open look at all aspects and factors. Alternative courses of corrective action can be vetted with stakeholders and the selected course of action initiated.

(4) Measurements are designed to inform us about achieving our strategy and objectives. Strategy and objectives must be aligned throughout the enterprise. Initiatives (short-term improvement efforts) and resources must be aligned to strategy and objectives.

(5) Measurements for an objective can inform about the benefits of a related initiative. Measurements should be electronically linked to data sources when possible.

*h. Evaluation criteria for IT performance measurements.* To be valid and useful, performance measurements should meet a number of criteria. Information managers, as well as functional managers, should evaluate existing or proposed performance measurements. In addition, these managers should review the performance measurements and refine them over time to assure that they address the range of goals, types of measures, and changing management and program requirements. Outcome measurements of the vision or stakeholder satisfaction with products and services are multi-dimensional and hard to identify and quantify. However complex, only outcome measures are considered worth pursuing at the enterprise and functional levels. Key evaluation criteria include—

(1) Are we measuring the right thing? Do the measurements—

(a) Address improvement in performance of mission?

(b) Address improvement in reaching goals and objectives?

(c) Assess the "value-added" contribution made by—

1. The organization's overall investment in information management.

2. Individual programs or applications.

3. Capturing the requirements of internal and external customers.

4. Addressing the internal performance of the IM function.

5. Reflecting improvements in organizational learning and innovation.

6. Addressing costs, benefits, savings, risk, or ROI.

(2) Do we have the right measures? Are the measurements—

(a) Targeted to a clear outcome (results rather than inputs or outputs)?

(b) Linked to a specific and critical process in the organization?

(c) Understood at all levels that have to evaluate and use the measurements?

(d) Effective in prompting action?

(e) Credible and possible to communicate effectively to internal and external stakeholders?

(f) Accurate, reliable, valid, and verifiable?

(g) Built on data that are available at reasonable cost, appropriate, and timely for the purpose?

(3) Are the measurements used in the right ways? Are the performance measurements used—

(a) In strategic planning (for example, to identify baselines, gaps, goals, and strategic priorities)?

(b) To guide prioritization of program initiatives?

(c) In resource allocation decisions?

(d) In day-to-day management of tasks, dollars, and personnel?

(e) To communicate results to stakeholders?

*i. Examples of performance measurements used by various organizational levels.* IT performance measurements are primarily used for specific programs and projects. However, they are also an effective tool in assessing the degree of effectiveness and efficiency in the delivery of IT support and services at any level. To comply with the spirit and intent of both GPRA and 40 USC Subtitle III, the goals and measurements used at lower organizational levels should be linked with Army's mission/strategic goals. Hierarchically linked performance measurements demonstrate how organizational achievements contribute to the strategic goals of the enterprise. If an IT investment does not measurably improve the Army's mission performance (no matter how well the program met its cost and schedule baselines or output and performance indicator measures) that investment should not be made. Listed below are some basic guidelines to consider for developing IT performance measurements. See also paragraph 2-4h for guidance on IT metrics used at the installation level.

(1) *Enterprise level.* At the enterprise level, the focus is on mission results, and information is needed to choose policy directions and make mission decisions. These managers report and justify the use of IM/IT expenditures. At this level, performance measurements will be used to determine—

(a) If investments in C4I/IT programs are yielding acceptable ROI, including quantifiable improvements in mission effectiveness.

(b) If the resources invested are yielding the expected results.

(c) If investment priorities are synchronized with overall Army mission priorities.

(d) If approved architectures are being implemented in a timely and cost-effective manner.

(e) If there is a proactive oversight system to ensure that benefit, cost, and schedule goals are met.

(2) *Functional level.* At the functional level, the focus is on unit results where information is needed to manage and improve operations. Performance measurement at the functional level begins with analysis of the organization's higher headquarters' mission, functional strategic plan(s), IT strategic plan, and other related guidance. From these sources, functional managers and commanders at the functional level determine their organization's mission and objectives and how IM/IT activities and initiatives support them. At the functional level, the mission-related outcome measures are defined, and the interests of the IM/IT user community are directly represented. The functional level, in concert with the users, assesses the results and benefits of an investment. The link between IT investments and organizational performance is most evident at this level.

(3) *Program/project level.* At the program/project level, activity and task information is critical to make tactical decisions and execute management decisions. Managers are leading programs, projects, or acquisitions that are sponsored by functional-level managers. These managers are involved in accomplishment of actual IM/IT efforts. The project manager works with the sponsoring user to track the results of the project in quantifiable functional terms. The traditional program management measures (cost, schedule, and performance) are not enough. The evaluation of the project must also include assessment of the results of the project on the larger functional environment and how those results support Army strategic plans.

*j. Army Information Technology Metrics Program.*

(1) *Overview.* The Army IT Metrics Program annually collects data on IT operations and infrastructure at all Army installations, as well as at AR and ARNG elements. The IT Metrics Program provides a common framework that allows installation commanders and IT managers to assess the current status of the IT infrastructure and evaluate the degree to which each component supports mission accomplishment.

(a) By identifying mission capability shortfalls, commanders and IT managers at all levels can make informed decisions regarding allocation of limited IT investment resources. The collection of each installation's IT metric data is linked to other Army and the Assistant Chief of Installation Management (ACSIM)/Installation Management Agency (IMA) management initiatives, the most important link being to Army Baseline Services and the fact that the IT metrics programs feeds infrastructure capabilities and performance into the installation status report, part III (ISR, part III). The ISR, part III is the report card on the performance of all services provided on an installation.

(b) The IT metrics data collected correlate the performance data (reflected in the ISR, part III service ratings) to costs (contained in the service based costing (SBC) model) to provide cost estimation data. This cost estimation data are fed onto the standard service costing (SSC) model, a methodology used to develop predictive cost equations to estimate what a service "should" cost based upon performance standards. This information, in turn, is fed by HQDA into the Army's Installation Management—Headquarters Information costing model for use by MDEP personnel in defense of POM funding. To summarize, the data input into the IT metrics system is intended to drive base operations funding requirements.

(c) The IT metrics reporting methodology also allows resource managers and commanders to identify, at a glance, which IT capabilities have the greatest relative shortfall from full mission capability. Furthermore, the relative ratings of the component attributes enhance the IT manager's ability to determine the elements of his/her infrastructure that contributes most to the shortfall. Appropriate decisions can then be made regarding reallocation of resources, or shifting of management focus.

(d) Individual Army installations collect the metrics data from tenant activities and organizations and report, via the IT metrics interactive Web site, to their respective RCIO-level metric representatives. The RCIO-level metric representatives "validate" or confirm the data inputs from their installations and forward the information to HQDA. After final submission to HQDA, centralized software analyzes the consolidated results and produces two key reports for each installation:

1. IT Metrics Capability Rating Report, which breaks down the data input for each individual metric capability and attribute.

2. The Input for Installation Status Report (ISR) III Rating Report, which contains each installation's "color" (Green/Amber/Red) ratings, used by the DOIM, to prepare input for the IT portion of the ISR, part III. Input is provided for the following services:

a. Service 15, Communication Systems and Support

b. Service 16, Visual Information

c. Service 17, Document Management

d. Service 18, Information Assurance

e. Service 19, Automation

(e) Validation of installation reports by the RCIO-level metric representatives is based on several factors: previous years' reports and trends for the installation, regionwide historical trends, personal knowledge of the installation and the technology supporting each metric, and Army plans affecting the installation. Ideally, RCIO-level metric representatives will consult with other members of the RCIO staff. The validation process needs to be a team effort, pulling on the experience and knowledge of the DOIM as well as the RCIO, the NETCOM/9<sup>th</sup> Army Signal Command, and other

Army organizations. Technology requirements are driven by the operational requirements of the tenants of a given installation. From that perspective, the local DOIM must play the key role as the interface between the technical and operational communities. A given operational requirement may be met in a variety of ways. Both the technical and operational views are needed to gain an accurate, comprehensive estimate of requirements.

(2) *Structure.* The structure of the Army IT Metrics Program is based upon seven capabilities, all high-level, macroservice areas that must be supported by IT managers and professionals at Army installations. Some of these are direct, “hands-on,” daily management functional areas (such as telecommunications, automation, and networks). Others, however, are operated by other installation staff elements (for example, administrative services). In these cases, IT managers must be prepared to support the IT-unique portions of this effort. The Army IT Metrics Program is built on a three-tier structure, as depicted in figure 2–2. Each IT capability is made up of major components, labeled attributes; each attribute is further divided into individual metrics.

(3) *Data gathering.* It is at the metric level that installation IT managers and professionals will collect, compile, and report the data necessary to build the overall evaluation. Limited explanatory comments may also be submitted for each metric. For each metric, four basic data elements are collected:

(a) Full mission requirement, which is the required quantity of a given metric for an installation to perform its power projection, sustainment, or training mission at 100 percent as determined by the IT manager and its commander.

(b) Current capability, which is the measurement of the “actual quantity” of that same metric that is currently on hand, installed, and operational.

(c) Primary funding source (MDEP) charged against.

(d) Source of the data (normally the office symbol of the section within the DOIM that provided or consolidated the data).

(4) *Percentage rating.* The ratio of “current capability” to “full mission requirement” results in a percentage rating for that metric. Weight factors assigned to each metric allow their weighted scores to be rolled up into a percentage rating for the attribute which they compose; similar weight factors allow attributes to roll up into a percentage rating for the IT capability. Weights and standards for individual metrics and attributes are set by CIO/G–6. For both attributes and capabilities, a rating of “100” represents full mission capability; a rating of less than 100 represents some relative degree of degradation from full mission capability.

(5) *ISR, part III input.* Compilation of IT metrics data at each installation facilitates the IT manager’s ability to provide input to the IT portion of the ISR, part III. The ISR, part III attempts to capture the local commanders evaluation of the installation’s ability to provide “services.” A broad range of installation services (personnel, law enforcement, logistics, housing, IT support, and so on) is covered and that evaluation is reported in a Green/Amber/Red summary format. The data collected as part of the IT/VI Metrics Program provide the detailed foundation underneath those summary ratings for IT infrastructure (see fig 2–2).

<u>7 Capabilities</u>	<u>28 Attributes</u>	<u>159 Metrics</u>	
#1 – Info Transfer	1.1 Telephone Svc	14 Metrics	
	1.2 Trunked Sys	17 Metrics	
	1.3 Non-Trunked Sys	9 Metrics	
	1.4 Infrastructure	1.4.1 Fiber Availability	
		1.4.2 Twisted Pair Avail	
1.4.3 Cable Condition			
1.4.4 Wireless Infrastructure			
1.5 Manpower Rqmts	4 Metrics		
#2 – Video Teleconf	3 Attributes	10 Metrics	
#3 – Networks	4 Attributes	24 Metrics	
#4 – Document Mgt	6 Attributes	17 Metrics	
#5 – Info Assurance (IA)	2 Attributes	18 Metrics	
#6 – Automation	4 Attributes	24 Metrics	
#7 – Visual Information (VI)	4 Attributes	18 Metrics	

Figure 2-2. Hierarchy of FY2004 IT metrics

(6) *Reporting Process.* AR 25-1, paragraph 3-6i, requires DOIMs to submit, through their RCIO representatives, their installations' IT metrics data on an annual basis through the IT metrics interactive Web site. Figures 2-3 and 2-4 are examples of the IT Metrics reporting process. Figure 2-5 depicts a timeline for report submission.

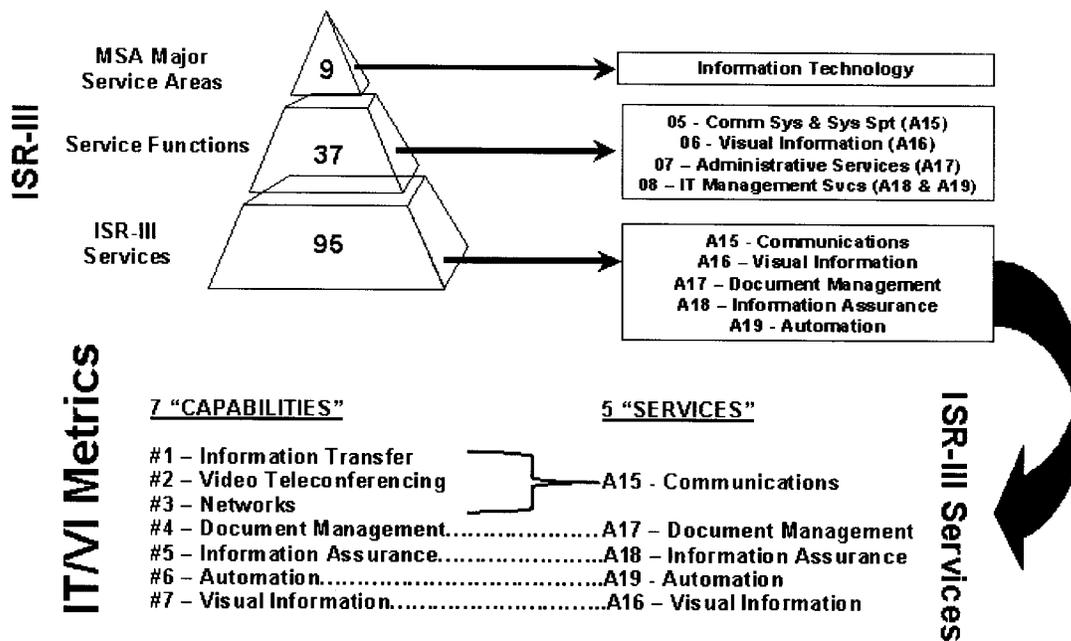


Figure 2-3. Relationship of IT/IV metrics and ISR, part III

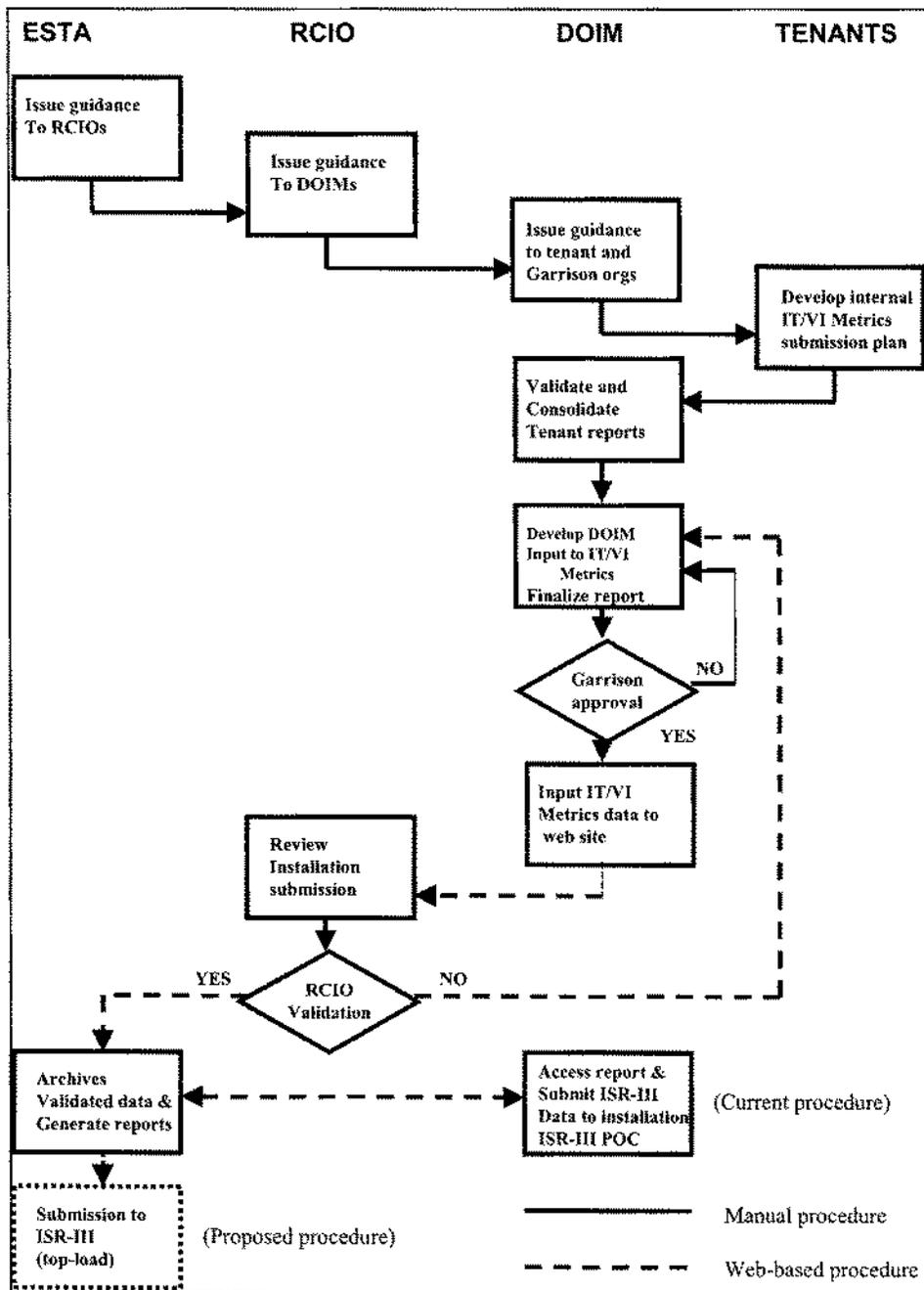
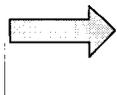


Figure 2-4. Reporting process diagram

<u>FY QTR</u>	<u>EVENT/ACTION</u>	<u>RESPONSIBLE ORG.</u>
4 <sup>th</sup> Qtr	Issue Army-wide guidance for upcoming report cycle	CIO/G6 & ESTA
4 <sup>th</sup> Qtr	Verify assignment of installation IT/VI Metric Managers	RCIO
4 <sup>th</sup> Qtr	Establish an Installation IT/VI Metrics Working Group	DOIM
4 <sup>t</sup> Qtr	Issue guidance to tenant organizations	DOIM
1 <sup>st</sup> Qtr	Current report cycle opens. IT/VI Web Sites available for installation input	ESTA
1 <sup>st</sup> Qtr	Raw data submitted by installation tenants	DOIM
1 <sup>st</sup> Qtr	Installations complete submissions	DOIM
2 <sup>nd</sup> Qtr	Validation of installation reports and forward to ESTA	RCIO
2 <sup>nd</sup> Qtr	Current report cycle closes. Posting of final reports to web site	ESTA
2 <sup>nd</sup> Qtr	Top-load IT/VI Metrics data to “feed” installation ISR-III reporting	ESTA
3 <sup>rd</sup> Qtr	Conduct annual IT/VI Metrics Workshop	ESTA
3 <sup>rd</sup> Qtr	Finalize changes and guidance for upcoming cycle	CIO/G6 & ESTA



**NOTE:** Underlying the whole process is the need for **CONTINUOUS ATTENTION** by the RCIO IT/VI Metrics Manager to their Installation IT/VI Metric Managers, and in turn, to the subordinate POCs.

Figure 2-5. IT Metrics reporting timeline

(7) *Access.* In order to gain access to the IT metrics interactive Web site, a user must first be entered into the CIO/G-6 point of contact (POC) database. Each RCIO controls access to the IT interactive Web sites thru the POC database for their particular region. The RCIO has the ability to add/delete/modify POC records of all users below their level. The RCIO can assign “read” access to the installation DOIM.

(a) Because the DOIM and the installation’s IT metrics manager work hand in hand, the installation’s IT metrics manager should be appointed in writing by the installation’s DOIM.

(b) The IT metrics managers not only for gather installation’s input and input all data into the IT Metrics Web-based system, but also grant access and maintain (adding/deleting/updating) the installation’s multiple-user accounts (point of contact accounts). Persons desiring access to the IT metrics interactive Web sites must first contact the installation’s IT metrics manager, by contacting the installation IT metrics help desk for assistance. The IT metrics help desk can be contacted by e-mail at IT\_Metrics@hqda.army.mil.

k. *PPBE.* The PPBE for IT requirements is part of the larger PPBE process in place throughout executive branch. The OMB provides the overarching guidelines for the PPBE. The planning and programming phases reflect specific guidance from the Office of the Under Secretary of Defense Comptroller. The budgeting phase reflects specific guidance from the Office of the Secretary of Defense (OSD)/Networks and Information Integration (NII) Resource Directorate as directed by the Comptroller to manage the IT portion of the DOD budget submission.

## **2-5. Planning, programming, budgeting, and execution for information technology requirements/capabilities**

a. *Planning.* Planning is an ongoing process throughout the DOD—short term (budget planning), midterm (program planning for the POM years), and extended planning for the out years both within the acquisition community (the extended planning annex) in general and for each service and agency and subordinate element as it plans for its future (for example, Joint Vision 2020, the Army Transformation Plan, and the Army leadership’s focus areas). In each instance the requirement for IT capabilities is an important part of the planning process to both support the planning process and support mission accomplishment. Every echelon within the Army plans for its future and provides those plans to its higher headquarters.

*b. Requirements Identification.* Typically, POM instructions include asking each MACOM commander to provide a narrative assessment of the MACOM's ability to accomplish its mission, identify significant shortfalls, identify internal resource adjustments, as well as adjustments with other MACOMs because of mission realignments etc. Urgent IT requirements/capabilities may be identified in this vehicle program. The second vehicle is through the MDEP development process. For proper validation and to ensure appropriate resourcing, each MDEP manager must provide the relevant PEG the resource requirements for an MDEP for the current POM or mini-POM.

(1) The Director of the Army Budget takes the lead on budgeting matters and establishes budgeting policy and processes that directly support the Army's reporting of the IT resources to the OSD, OMB, and the Congress. While the budget process for IT is not a separate process in the Army's implementation of the DOD PPBE, the reporting of IT budget resources to OSD, OMB, and the Congress is submitted in separate budget exhibit documents, exhibits 53 and 300. These exhibits are reported twice a year. The budget estimate submission (BES) in September is provided to the OMB and includes exhibit 53, which is a tabular listing of Army's IT resources by IT initiative, and the exhibit 300 reports for major IT investments. OMB reviews these submissions and provides comments and feedback in December as part of the OMB pass-back guidance on the budget estimates. As part of the OMB pass-back guidance, exhibit 300 reports that do not have security certifications and accreditations for systems in the form of a valid authority to operate (ATO) will require the submission of a plan of action and milestone report. The plan of actions and milestones will describe the actions planned to correct the security issue and achieve the valid ATO. The President's budget submission incorporates OMB guidance from the BES and includes facts-of-life changes since the BES, including program budget decisions and program decision memoranda. The submission of the President's budget in February is forwarded to Congress as part of the President's budget request. Exhibit 53 is forwarded to the Congress along with an edited version of the exhibit 300 report, called the Selected Capital Investment Report. Interim timelines for reporting the IT budget are set by OSD/NII and discussed in the annual program/budget call memorandum issued by the OSD Comptroller. OMB Circular A-11 and 40 USC Subtitle III define the IT resources that must be reported.

(2) OMB Circular A-11, Section 300, outlines the reporting of major IT investments. The Capital Asset Plan and Business Case report, also known as the Capital Investment Report (CIR), is designed to demonstrate to Army management and to OMB that the agency has employed the disciplines of good project management, represents a strong business case for the investment, and has met other administration priorities to define the proposed cost, schedule, and performance goals for the investment. The information on the CIR helps management to—

(a) Ensure that spending on capital assets directly supports the Army's mission and will provide a return on investment equal to or better than alternate uses of funding.

(b) Identify poorly performing investments (investments that are behind schedule, over budget, or lacking in capability).

(c) Identify capital assets that no longer fulfill ongoing or anticipated mission requirements or do not deliver intended benefits to the agency or its customers.

(d) Ensure that strong business cases are provided for IT investments.

(3) These business cases should include security, privacy, enterprise architecture, and provide the effectiveness and efficiency gains planned by the business lines and functional operations. The following IT resources are generally exempt from IT reporting:

(a) Information resources acquired by a Federal contractor that are incidental to the performance of Federal contract.

(b) Programs, projects, and activities that are embedded in noncommand, control, and communication weapon systems or embedded in service force structure and therefore are not readily identifiable in the budget. Final definition resides with OSD/NII to determine the reporting of command, control, and communications activities.

(c) Highly sensitive and special access programs whose resources are specifically exempted from budget reporting by the ASD/NII and other OSD authorities. In general, these resources are reviewed through the separate or intelligence budget process.

## **2-6. Information technology waiver requirements process**

*a. Background.* The waiver process is the resource implementation of Army Knowledge Management (AKM) Goal 1, "Adopt governance and cultural changes to become a knowledge-based organization." The AKM Goal 1 waiver process provides the visibility required to ensure that non-IT programmed dollars spent on IT initiatives are appropriately documented and meet Army guidelines for IT investments.

*b. Applicability.* This guidance applies to all IT expenditures over \$25,000 used for Operation & Maintenance, Army (OMA), and \$100,000 for research, development and acquisition. AKM Goal 1 waivers are not a mechanism to obtain additional funds beyond that which already exists in the requestor's budget.

*c. Procedures.* The Army CIO/G-6 publishes annual AKM Goal 1 Resource Execution Guidance and Year-End Review Guidance to reiterate the waiver requirement, communicate changes in the process, and provide updated lists of CIO-managed MDEPs, IT Army program elements, and IT elements of resource. These lists are all used to report IT expenditures and in evaluating whether a waiver is required.

*d. Waivers.* All waiver requirements are processed through the workflow process automation application located on

AKO. The waiver form and accompanying workflow instructions may be accessed at <https://akodisc4ko1.us.army.mil/intranet/workflow/home.jhtml>. A link to the End-User Guide is also provided on the application's main page. Figure 2-6 shows the workflow steps.

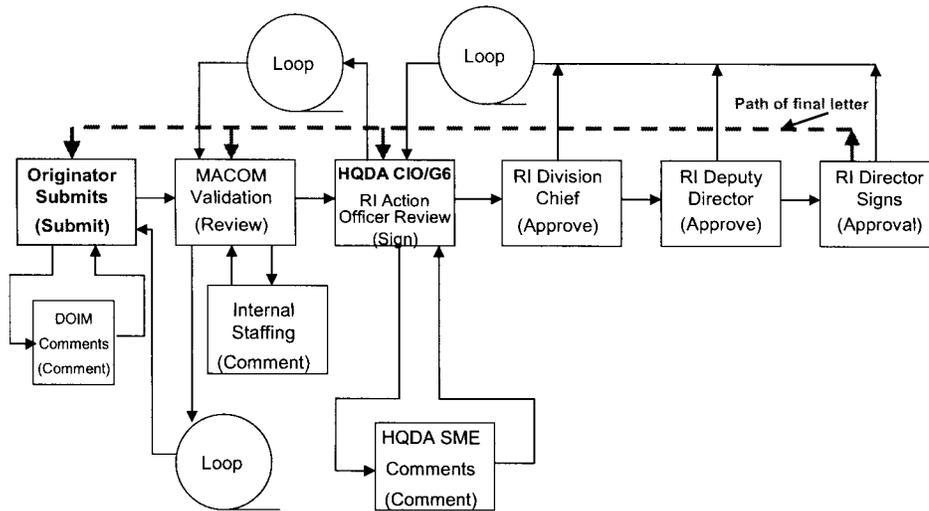


Figure 2-6. AKM goal 1 waiver workflow

*e. Installation functions* At the installation level, mission commanders need to coordinate IT requirements with the DOIMs for standards, accreditation, networkiness, Information Installation Infrastructure Architecture (I3A), and similar Army standards even though funding with mission dollars. The tenant agency may include the agency information management officer (IMO) in the internal organization review as a commenter. This does not require adapting the current Goal 1 waiver process steps because the IMO review cannot be substituted for the DOIM review.

*f. DOIM functions.* DOIMs will not validate mission requirements but will review requirements to ensure compliance with standards; they should determine whether the requirements are on the nonreimbursable or reimbursable services list and offer applicable reimbursable services to the mission commander. NETCOM/enterprise System Technology Activity provides a technical control review and validates all enterprise-level fielding requirements. AKM Goal 1 waivers for garrison requirements are originated by the local DOIM and staffed through the RCIO for comment before submission to Headquarters (HQ) IMA for MACOM validation.

*g. MACOM functions.* MACOM senior IM officials review and approve all MACOM C4/IT mission requirements, ensure compliancy with overall funding guidance and AKM goals and standards prior to forwarding to Army CIO/G-6.

*h. HQDA CIO/G-6 functions.* The Director, Resource Integration ensures all requirements are reviewed for enterprise solutions, goals and policies, prior to approval.

*i. End-of-year procedures and reporting requirements.* The AKM Goal 1 year-end process is intended to alleviate time constraint issues involved in obligating resources during year-end and applies to all MACOMs, HQDA functional proponents, and direct reporting units that plan to migrate non-IT programmed dollars at year end to procure IT goods and services. End-of-year waiver requests are processed through the “process automation application.” The waiver originator should select “end-of-year waiver” in the new process window in order to access the correct form. All end-of-year waiver requests follow the same review and approval steps as waivers that have funds already identified. Followup verification reporting is required for all approved end-of-year waivers.

*j. Common communications and computing infrastructure semiannual reporting requirements.* MACOMs and HQDA functional proponents are required to report CCCI expenditures using the CCCI reporting tool within the “process automation application” (see para 2-5d). CCCI includes all equipment and services that Army organizations provide to the majority of their workforce for common use. This does not include common IT services provided by the installation DOIM. Examples of CCCI are: personal computers, office automation software other than commercial products covered under the Enterprise License Agreement, networking equipment, copiers, scanners, and printers. These semi-annual reports must be completed within 30 days following the end of the reporting period (October through March and April through September).

## 2-7. Information Technology Management Career Program-34

Harnessing the intellectual capital of our workforce through effective knowledge management represents an important cultural shift, one that is vital to the Army's transformation effort. Consequently, Information Technology Management (ITM) Career Program-34 (CP-34) will support a wide variety of knowledge management education, training, and professional development opportunities to support AKM. Effective project management is probably the single most important factor to ensure successful implementation of key IT requirements. Senior Government leaders have recognized the vital need for skilled project managers, and have embedded project management into the requirements of the President's management agenda. ITM Career Program-34 will support a variety of initiatives designed to provide project management training across the Army. The length and mode of these programs vary, but all focus on training targeted audiences in the field.

*a. Overview.* The CP-34 develops, coordinates, and promotes multiple training, education, and career development programs to broaden and enhance the skills and knowledge of the ITM workforce. The competitive professional development programs are designed to transform technical professionals into ITM leaders who are adept in leadership, business and technology skills based on the following principles and practices:

- (1) Cross-functional approach to ITM career development by mandate of 40 USC Subtitle III.
- (2) AKM initiatives, as mandated by the Secretary of the Army and the CSA.
- (3) Options for flexible and marketable skills for Army civilians in an environment of downsizing, outsourcing and an aging workforce.
- (4) A dynamic career management system and innovative programs to support DA critical information missions, help create a more able and competitive ITM workforce, and promote professionalism and leadership within the CP-34 community.
- (5) Selection of ITM professionals at GS-11 and above. GS-09s (noninterns whose positions have been documented at the full performance level) may apply on a waiver basis with their management's written approval. CP-34 includes the following job series within IT job categories:

(a) Core Series 2210, Information Technology Specialist; 301 (I), Information Management Specialist; 391, Telecommunications Specialist.

(b) Specialty Series 1001, General Arts & Administration Specialist; 1020, Illustrator; 1060, Photographer; 1071, Audio-Visual Production; 1084, Visual Information Specialist, Publishing/Printing; 1082, Publishing Writer/Editor; 1083, Publishing-Technical Writer/Editor; 1654, Printing Specialist Other; 343, Records Management Specialist; 1410, Librarian

*b. CP-34 professional development.* The Career Program-34 Competitive Professional Development Program supports professional training, education, and career development in—

- (1) Information technology management.
- (2) CIO/G-6 core competencies.
- (3) Knowledge management.
- (4) Information assurance.
- (5) ITM program and project management emerging technologies (biometrics, e-business, e-Government, and so on).
- (6) Business leadership.
- (7) Public policy/public administration.

*c. Sponsored programs.*

(1) Information Resources Management College (IRMC), Fort McNair, Washington, DC. IRMC, as part of the National Defense University ([www.ndu.edu/irmc](http://www.ndu.edu/irmc)), offers state-of-the-art training varying in length from 5 days to 14 weeks. The annual catalog provides a listing of course titles and dates. A CIO Certificate Program and the Advanced Management Program are offered. The CIO Certificate Program and the Advanced Management Program provide a breadth of courses centered on Federal CIO competencies and practices and awards a CIO certificate and academic credit towards a master's degree. Individual courses may also be taken lieu of complete certificate and program studies. Tuition is free to DOD employees, and ITM professionals may request funding for authorized travel/per diem.

(2) The Information Resources Management College also offers Certification in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4011. This program is open to civilian ITM professionals, GS 13-15, and requires a bachelor's degree. Applicants who are no more than one grade lower than minimum requirement or who do not meet the degree requirement may request a waiver. Award of the certificate requires completion of four 1-week intensive courses (5 days in residence or 10 to 12 weeks in an online format). Individuals currently in the CIO Certificate Program may elect to complete that program with a concentration in Information Assurance by including the above four courses as part of the eight-course requirement.

(3) The National INFOSEC Education and Training Program provides education at universities that have been designated as centers of excellence in information assurance. All selected universities were reviewed and approved by the National Security Agency. Information is available at [www.nsa.gov/isso/programs/nietp/univout.htm](http://www.nsa.gov/isso/programs/nietp/univout.htm).

(4) The U.S. Army Signal Center, School of Information Technology, Fort Gordon offers a limited number of IA/IT

courses. Tuition is free. Funds may be requested for travel/per diem. Additional information is available at [www.gordon.army.mil/sit/sit/Courses.htm](http://www.gordon.army.mil/sit/sit/Courses.htm).

(5) The Clinger–Cohen course provides comprehensive knowledge about 40 USC Subtitle III and other ITM legislation and policies. This course allows activities to ensure their employees are up to date in meeting the latest Government ITM requirements. Courses are given at field locations.

(6) The Office of Personnel Management Management Development Centers offer leadership, management, and technology seminars to mid- and senior-level employees to improve their knowledge and skills. The seminars provide the latest knowledge to ensure participants are current in their functional areas and also may cross-train in other functional areas in preparation for advancement. The seminars are located at Shepherdstown, WV, and Denver, CO. Additional Information is available at [www.leadership.opm.gov/fei.html](http://www.leadership.opm.gov/fei.html).

(7) College and university training colleges and universities provide a source of education to ensure the currency of technological, management and leadership knowledge and skills for the ITM Workforce. The CP–34 Competitive Professional Development Program emphasizes distribution of limited university program funds to the maximum number of qualified nominees. Accordingly, part-time academic programs are encouraged, although full-time applications will be considered for acceptance. Nominees will submit an acceptance letter from the school and an academic plan containing leadership, business, and technical courses during a 12-month period. The academic plan will identify the school, course titles, and the level of the courses (undergraduate or graduate), course dates, tuition costs, textbook costs, and other fees (itemized). Although all authorized educational expenses are funded for selected nominees, *neither salary nor benefits are reimbursed*. Providing for salary and benefits for approved full-time students is the function of the student’s activity. All selections will be made and approved by the functional chief representative. Because this program emphasizes part-time academic study, successful nominees may re-apply the following year.

*d. Applications.* All applications for competitive professional development training programs are due to Career Program-34 quarterly.

(1) Individuals may receive reimbursement for books, tuition, and lab fees for courses. Travel and TDY funds are available for developmental assignments, training with industry, and select courses/programs (Information Resources Management College). Travel and travel duty funds are not available for university training. Rental cars are not authorized for any training or career developmental opportunities. Training programs are open to all eligible employees. Employees are selected based on the following criteria:

- (a) Career goals.
  - (b) Ability to successfully participate in a rigorous training program.
  - (c) Potential for professional development.
  - (d) Job performance.
  - (e) Supervisor’s recommendations/endorsements.
  - (f) Army’s requirements for core competencies.
  - (g) Post-training utilization plan.
- (2) A supervisory endorsement citing the applicant’s performance (include current performance appraisal), leadership potential, and organizational benefit must be included with each application package.
- (3) Applications must be submitted through command channels to: HQDA, CIO/G–6, ATTN: SAIS–EIH, Human Capital Management., 107 Army Pentagon, Washington, DC, 20310–0107 or by e-mail to [ITMCareers@hqda.army.mil](mailto:ITMCareers@hqda.army.mil).

## **Chapter 3 Army Knowledge Management and Army Knowledge Online**

### **Section I Army Knowledge Management Overview**

#### **3–1. Army Knowledge Management Strategy Plan**

The AKM SP states that the Army’s strategy is to improve organizational performance by implementing a net-centric, knowledge-based organization. The goal of AKM is standardized, enterprise-level mission and business practices. The Army CIO/G–6 is the functional proponent for the AKM SP and facilitates and oversees its execution (see AR 25–1, para 1–8).

#### **3–2. The guiding principles of Army Knowledge Management**

These principles support the Army’s net-centric, knowledge-based vision. The AKO portal is the principal tool to find, select, organize, improve, share, and benchmark enterprise information for mission results and affords the warfighter multiple collaborative capabilities. It involves sharing all of an enterprise’s information assets, including databases, documents, policies and procedures, as well as previously unarticulated expertise and experience resident in individual

workers. Efficiencies and combat decision dominance are just a few of AKM's value-added principles. Other examples of these principles include—

- a.* Standardization of business rules, processes, and information across the enterprise to eliminate unnecessary duplication, incompatibility, and redundancy of data, systems, and business processes.
- b.* Capturing and validating information once, reusing it across the enterprise, and placing greater significance on collaborative strategies for satisfying the common needs of soldiers and civilians.
- c.* Enabling and accelerating sound decisionmaking through architecture-based analysis and evaluation and ensuring security and protection of sensitive information.
- d.* Integrating performance management in every decision process and providing incentives for continuous improvement and evolutionary transformation.

## **Section II**

### **Army Knowledge Online Overview**

#### **3-3. General**

- a.* AKO supports the Army business units and the warfighter. AKO is an essential system to the warfighter by providing access to a broad depth of information found anywhere in the world, enabling warfighters to share knowledge and collaborate utilizing multiple capabilities and to access and update readiness information.
- b.* The range of services provided through AKO includes enterprise user authentication, user assistance, enterprise search and retrieval, self service functions, access to functional/domain specific applications and services through single sign-on and enterprise collaboration services.
- c.* AKO will continue to evolve and add capabilities and refresh services to leverage technological advances. Information on specific enterprise capabilities and services and their employment is maintained on AKO through user assistance functions (see para 3-5).

#### **3-4. Enterprise user accounts and access**

- a.* AKO is the gateway to all Army information, systems, and services and is the single mechanism for generating user identification and accounts. The account management guidelines below specify who has access to the AKO portal and describe the process for account approval and management. Once approved, each individual account will be entered into the AKO Directory Service as an authorized account. All intranet applications and subordinate portals in the Army will use the AKO directory service to authenticate personnel as valid Army users, unless excepted by the CIO/G-6.
- b.* The owners of intranet application and subordinate portal manage access, roles, and authorizations for users within their respective application and content areas. For example, AKO identifies and authenticates the individual at the other end of the intranet is john.doe@us.army.mil; the application or subordinate portal linked to AKO then validates whether or not the individual has access and authorizations to a particular application.
- c.* Authentication is performed using secure lightweight directory access protocol services, the Integrated Total Army Personnel Database (ITAPDB), or the Defense Enrollment Eligibility Reporting System (DEERS). As additional security measures beyond the password process are implemented for Army systems (for example, public key infrastructure, common access card, biometrics), the AKO Enterprise Directory will make the necessary engineering changes to incorporate these features. Procedural and directory service interfaces between the AKO Enterprise Directory and other Army applications eliminate the additional development costs for those applications.
- d.* In accordance with Army policy, e-mail encryption and digital signature certificates issued on the CAC/PKI are based on AKO e-mail addresses (that is, FirstName.LastName@us.army.mil).
- e.* AKO maintains four general account categories of members as defined in table 3-1.
  - (1) Full accounts are based on employment status and are initially validated using active Army or DOD databases. Within the full account category, certain full account holders are authorized to sponsor accounts. Account sponsors—
    - (a)* Ensure sponsored individuals have a legitimate need for an account.
    - (b)* Monitor usage and behavior of those individuals they sponsor.
    - (c)* Revalidate sponsored accounts on an annual basis to ensure a continued legitimate need for the account.
    - (d)* Immediately terminate any sponsored account when the legitimate need no longer exists, such as when an Army contractor support service contract expires.
    - (e)* Ensure all accounts for non-U.S. citizens are approved through proper channels as outlined in AR 25-2, paragraph 4-15.
  - (2) Sponsored accounts are AKO accounts for users being sponsored by a full account holder. Sponsored accounts are to be established only for persons with a legitimate need for AKO to perform Army business or for morale and welfare purposes of our soldiers. Sponsors must ensure all non-U.S. citizens desiring AKO accounts are approved through appropriate channels as outlined in AR 25-2 because it is the function of the sponsor and the organization's security officer to ensure that those needing and AKO account have a legitimate need for the account to perform official Army business. "E-mail only" accounts are another form of a sponsored account; however, these accounts do

not require approval beyond the sponsor, including the accounts of non-U.S. citizens. Sponsored accounts require annual renewal.

(3) Family member accounts (FMAs) can be automatically verified through DEERS. The primary account holder will not receive a notification that a family member over the age of 18 has requested an account. For those under the age of 18, an approval must be granted before the activation of the FMA. An FMA will be deactivated once eligibility is lost under DEERS. A sponsored account may be re-established if legitimate needs exist for an AKO account for someone losing DEERS benefits as well as for extended family members such as parents and siblings.

(4) Dual accounts combine different account types. For example, in a situation where a person is both retired Army and a contractor, a user might have an account that combines a full account and a sponsored account.

**Table 3-1**  
**Account categories and types**

Account category	Account type
Full account	Active Army <sup>1</sup> ARNG <sup>1</sup> AR <sup>1</sup> DA civilian <sup>1</sup> Nonappropriated fund (NAF) civilian <sup>1</sup> Army, ARNG, AR retired Medical retired U.S. Military Academy cadets Reserve Officer Training Corps (ROTC) cadets on contract or scholarship
Sponsored account	Army contractor DOD civilian Other active U.S. military service member Federal civilian agency employee Foreign officer (attached to Army) Local nationals Medical discharge with benefits Army volunteers/academia ROTC cadets not on contract or scholarship
AKO e-mail only account	A sponsored account allowing only access to AKO e-mail. Normally used to provide a way to validate a user for access to an Army system. This may include future Army recruits (formerly Delayed Entry Program) and foreign nationals.
Family member account	A family member of a full account holder who has DEERS benefits.
NOTE: Dual account	In some cases, AKO accounts may combine different account types, such as an account for a person who is both retired military and a contractor.

Notes:

<sup>1</sup> Full account holders authorized to sponsor accounts.

*f.* The following steps are required to establish an AKO account:

(1) To register for an account, the applicant must determine their eligibility for a full, sponsored, or FMA based on the established criteria (See table 3-1).

(2) All AKO accounts will be registered in a `firstname.lastname@us.army.mil` format.

(3) After the account type is determined, the applicant clicks on the “Register for AKO” link under the “NewUser” section of the AKO Home page and follows the instructions.

(a) For full accounts, the applicant’s Social Security number, date of birth, and all other information are required during the registration process for authentication. The information provided by the applicant is compared against the information contained in the ITAPDB and used to verify that the applicant is authorized to have an AKO full account. These data are maintained in the ITAPDB and are used for verification purposes only.

(b) For sponsored accounts, including “e-mail only” accounts, only those full account holders noted in table 3-1 are authorized to sponsor accounts. The applicant must provide the sponsor’s AKO Web mail address. Submission of a Social Security number is mandatory for ROTC cadets and Delayed Entry Program recruits. Additionally, the applicable sponsored account type sought must be specified, and the sponsor must ensure those being sponsored for an account have a legitimate need to interface with the Army and that they are aware of AKO rules. An e-mail message is sent automatically to the identified sponsor requesting authorization to grant the account.

1. To approve the request, the sponsor logs into his or her AKO account, clicks on “My Account,” and goes into the sponsor management console under “My Account” settings. Once the sponsor approves the account, the application is

sent to his/her first-line or higher supervisor (minimum O-3 or GS-11 supervisor) for final approval. "E-mail" only accounts do not require this secondary approval.

2. Once approved by the supervisor, the account is activated immediately.

(c) For FMAs, an applicant must provide a Social Security number, date of birth, and the Social Security number of the primary family full account holder as requested during the registration process for authentication.

1. The information provided by the applicant is compared against the information contained in the DEERS and used to verify that the applicant is authorized to have an AKO FMA.

2. Once the request for an FMA is validated, the account will be activated immediately. FMAs do not require annual renewals.

g. Changes to user account names may be required because of marriage, divorce, or other legal requirements. Full accounts and FMAs are validated against an Army or DOD personnel database; therefore, this requires the account holder to first contact and change that applicable master personnel database using established processes. Once this is done, the account holder should contact the AKO help desk for assistance in making the name change. Sponsored account holders must notify their sponsor of the proposed change prior to contacting the AKO help desk for assistance. A surviving spouse of active duty Soldiers and retired Soldiers can be authorized a full AKO account as long as they are eligible in DEERS.

h. The following user functions and guidelines apply:

(1) Each AKO account holder must be aware of Army security and IA policy. All account holders are required to review and acknowledge online an understanding of IA requirements. All account holders are accountable for their actions in the AKO. An account holder who disregards AKO rules and guidelines receives an initial warning from AKO. If serious enough, immediate inactivation of the account will occur. A second offense may result in either inactivation of the AKO function in which the rules violation occurred or complete deactivation of the AKO account. Reactivation of the account requires a memorandum to the Office of Information Technology Services from a first-line or higher supervisor (minimum O-3 or GS-11) stating the user has been counseled and requesting the account be reactivated. Actions of FMA or sponsored accounts are supervised by the full account holder. When a FMA or sponsored account holder is notified of a rules violation as noted in the paragraph above, the sponsor of that account holder also receives a notification. The sponsor determines whether or not that account should be immediately terminated after the initial warning. If the decision is to terminate the account, the sponsor should immediately contact the AKO help desk to initiate the action. If the decision is not to inactivate, the account sponsor instructs the individual on acceptable behavior and actions within AKO for continued use of the account.

(a) If the account holder is under investigation and/or subject to adverse action, a commander or activity director, in the grade of lieutenant colonel or payband equivalent who possesses the relevant knowledge, skills, and abilities as comparable employees performing at the GS-14 level or above, may request the restriction, suspension, or termination of AKO user privileges. When a user's account is restricted, the user will no longer have full access to all AKO services. When a user's account is suspended, the user's access to AKO will be temporarily disabled. The user will not be able to login to AKO, access any sites behind AKO, or access any sites that use AKO authentication. The user will lose access to AKO e-mail. Requests should be considered after legal review and the command has reason to believe that—

1. Continued use of AKO may hinder organizational operations (AR 25-2, para 4-11b).

2. The user has engaged in conduct in violation of DOD/Army law, regulation, or procedure.

3. The user has violated the AKO Terms of Service/Terms of Use guidance or associated procedures, policies, or regulations.

4. The user is the subject of adverse personnel action or investigation.

(b) Requests for termination should only be considered in extreme cases. Upon account termination, all user access and privileges associated with AKO cease. Data or content that the affected user has stored on AKO will not be retrieved nor provided to the user later, unless requested and approved through legal channels.

(c) Reactivation of the account requires a memorandum to the AKO Account Suspension Officer from a commander or activity director, in the grade of lieutenant colonel, or above, or payband equivalent who possesses the relevant knowledge, skills, and abilities as comparable employees performing at the GS-14 level or above, stating the user has been counseled and requesting the account be reactivated.

(2) All account holders have a user name identifier listing the type of account such as active Army, Army civilian, contractor, family member, and so on. Account holders with multiple identifiers have each account designation noted. In addition, descriptive information, including nationality, is displayed for foreign officers and representatives as required by AR 25-2, chapter 4. Additional guidelines and examples for user identifiers are as follows:

(a) All full accounts and FMA have a friendly name (includes rank, account type, FMA, etc) noted after the e-mail or in place of the e-mail address. A full account would be displayed as jane.doe@us.army.mil (LTC/Army); FMA as James.jones@us.army.mil (FMA).

(b) Current contractors have CTR (for contractor) and abbreviation of company name added to their friendly name, for example, John.doe@us.army.mil (CTR-Smith Consulting). New contractors with no existing AKO accounts would have CTR added to their e-mail address, for example, john.doe.ctr@us.army.mil. A company name will be displayed in

the friendly address. Contractors with existing AKO accounts will have their contractor information added to their friendly name, for example, John.doe@us.army.mil (CTR–Smith Consulting/LTC Army Ret.).

(c) Existing and new foreign nationals and local nationals would receive new e-mail addresses including their account type and country code, for example, jane.doe.UK.com@us.army.mil or fred.jones.ln.jp.com@us.army.mil. The type of foreign official will be displayed in the friendly name as outlined in AR 25–2, paragraph 4–15.

(3) The establishment of multiple accounts and the use of alias/anonymous user names for accounts are prohibited.

(4) The use of group accounts is generally unavailable. Exceptions may be granted by AKO on a case-by-case basis for functions that require continuity of operations such as help desks and command general information access that permits continuity of operation, functions, or capabilities. Requests for an exception should be forwarded to the Office of Information Technology Services.

(5) Foreign officers and representatives are allowed access to any capabilities of the AKO that can be audited within the portal, excluding chat rooms and instant messaging. The policy stated in AR 25–2, chapter 4, must be followed in reference to accounts where foreign nationals have access within AKO.

i. The following apply to deleted or inactive AKO accounts:

(1) Orphaned accounts are still active in the directory but for some reason the requirements for an individual to access the account are no longer met. This includes an individual who leaves the Army, ARNG, or AR by reason other than retirement or medical retirement with benefits. This applies to account holders who are missing in action or deceased. A contractor who has an expired contract with the Army should have any account inactivated immediately for security reasons. It is the role of the sponsor or a commander or activity director in the grade of lieutenant colonel or payband equivalent that possess the relevant knowledge, skills, and abilities as comparable to employees performing at the GS–14 level or above to terminate such accounts.

(2) Sponsored accounts that are not used for a period of 90 days will be deactivated. This is done for security reasons and to ensure account holders periodically review updates and announcements within AKO. An e-mail notification is sent to the account holder and sponsor that the account will be deactivated in 5 business days if not used. Account holders are able to reactivate the account by resetting their passwords. Full and FMA accounts do not have a time limit for utilization because those accounts are validated against an active directory for currency and are automatically inactivated once users no longer meet the requirements to hold an AKO account.

(3) When a full account holder no longer has an account, all sponsored accounts are immediately inactivated. It is the role of the full account holder to ensure sponsored accounts that need to remain active for support of Army business are reactivated under another full account holder when deemed appropriate.

(4) Accounts for active duty members remain active for 180 days after honorable or general discharge for out-processing requirements. All other types of discharges will have their accounts immediately inactivated, and it is the role of each unit to ensure this occurs.

(5) AKO account information of a deceased Soldier is not considered “personal effects.” AKO records are properly classified as “government” records. Requests for AKO information must be processed under the Freedom of Information Act (FOIA) procedures. The Casualty Affairs Officers (CAOs) may advise family members seeking AKO information of the possibility of filing a FOIA request, and subject to advice and guidance from the Human Resources Command, the Command Judge Advocate may assist family members in getting their requests to the appropriate officials. The CIO/G–6 FOIA officer will perform the following:

(a) Request from the AKO Program Officer printout screen shots of the residuary account records, information, and/or indicia of use (that is, records of user groups, chat rooms, and address book use of the decedent).

(b) Provide material to legal counsel for FOIA exemption screening noting the potential privacy interests of living third parties.

### **3–5. User assistance**

a. AKO user assistance is accessible from the homepage via the “Help” link. The help function consists of training materials, frequently asked questions, user guide, and provide feedback.

(1) *Training materials.* This section contains slide presentations, startup guides, study guides and various learning tools. It can be utilized in development of organizational, community, team, and individual sites. These materials are designed to enhance the user’s proficiency in development and administration of AKO sites within the portal.

(2) *Frequently asked questions.* This is a collection of previously asked questions by users with technical responses. It can be accessed by category or specific question.

(3) *Ask a question.* This is the location to submit questions to the help desk for resolution.

(4) *My question.* This feature allows user to track status of their question.

(5) *User guide.* This is an online reference that provides definitions and functions of the AKO portal.

(6) *Provide feedback.* This feature enables the user to submit general feedback or recommendations to improve the AKO Portal.

b. In addition to the AKO homepage, users may telephone or e-mail the help desk 24 hours, 7 days a week at Defense Switched Network (DSN) 654–4357, (703) 704–4357, and (877) 256–8737, or e-mail help@us.army.mil; for

AKO-Secure (SIPRNet), call DSN 654-3713, (703) 704-3713, and (866) 853-3753, or e-mail akos.help@us.army.smil.mil.

### **3-6. Self-service functions**

a. Self-service capabilities are provided and maintained by the functional proponents and are the single authoritative source for user information worldwide. Individual information for an applicable user is provided in each of the self-service functions. An AKO user will not necessarily have information in each self-service center, depending on their category and type of account.

b. Examples of the self-service functions include—

- (1) My Benefits.
- (2) My Finances.
- (3) My Training.
- (4) My Medical.
- (5) My Family.
- (6) My Education.
- (7) My Legal.
- (8) My Travel and others.

### **3-7. Enterprise search and retrieval of information**

a. AKO information sources include content resident within the AKO and links to information on Army, military services, and related mission Web sites. Search functions match a user's specified information requirements with content in relevant information sites on AKO. AKO uses search and retrieval tools to retrieve relevant results based on the user's needs definition and proper selection of the search source.

b. Taxonomies/ontologies are the foundation that enable the search tool to provide a user precise, relevant, and timely results. When developing taxonomies/ontologies, it is the role of the functional proponent to ensure consistency with the enterprise ontology currently under development. When a user searches the Internet or AKO, the search tool looks for the words and generally has an interface to a unique taxonomy of the functional community. The taxonomy of the functional community terms, phrases, and acronyms strengthens the precision and relevance of the search results. Similarly, ontologies map and maintain the multiple concepts and relationships with changing views. The search tool can find and retrieve the correct word or phrase "meaning" no matter the change.

### **3-8. Content management enterprise collaboration**

a. *AKO content management.* AKO has a broad range of content that includes resident and linked content objects. The primary AKO content repository is the Knowledge Center (KC), which allows the user, community or team to create KCs or personal team areas available from any Internet connection. This knowledge repository allows the user, based on the type of user account (para 3-4c), to upload and download files, share files, subscribe to working teams content, control versions, and delete files. While AKO has content in other locations, to include community pages, threaded discussions, and so on, the site administrator maintains the rules for reference posting, versioning, and archiving of content. The primary content site, the KC, has AKO-defined roles and rules for maintenance and archiving. AKO content management continues to mature as its content processes and technology grow to meet user requirements.

b. *Roles within the KC.* Content roles allow the user access to content based on applied rules such as account type, access level, and specific site restrictions. Users with access to a KC or folders are identified as one of three types:

(1) Administrator, which controls all permissions over the content; views all content; adds new files and folders; deletes content; adds and removes users; and changes user access levels. Administrators create the KCs and personal team sites and control the following permissions: the ability to delete knowledge centers and folders; set file expiration dates for content communities and personal teams; rename content areas, communities, teams; customize folder access within a community; and establish or change a community, folder, or team area's security access.

(2) Author, which specifies user with access to a KC and permission to download and upload files.

(3) Read only, which specifies user with read-only access may view and download files but cannot make content changes.

c. *Basic content management capabilities.* A user with an active account can perform selected content management functions based on account type and site access restrictions. Basic content management functions include—

(1) Download file—retrieve content from remote source.

(2) Add file—adding a file to specific site. Some locations require special permissions.

(3) Move or copy an object or a file—move or copy an object or file to a specific site. Some folders require special permission.

(4) Search and subscribe to specific sites—search for knowledge centers or AKO subject content areas and request access (subscribe) to them. Once the administrator grants access, the user can perform a keyword search by name or browse the site list.

*d. Advanced content management capabilities.* Users with extensive information needs can use the KC's advanced content management capabilities:

(1) Versioning, which provides the users the ability to create multiple versions of a file. Users can collaborate on this file while keeping the edits and changes intact. The KC toolbar has a "new version" button with a descriptive wizard to upload new versions. Maintaining versions allows the users to review prior editions and auto-forward them.

(2) Linking files in multiple folders, which allows the user to place the file in one folder and then link to other folders. Collaboration often requires a user to locate the same file in multiple folders. With the correct permissions, the link allows a user to download the file regardless of the folder being searched.

(3) Archive— provides authorized users a direct link to ARIMS for archiving documents contained in the KC.

### **3–9. Enterprise collaborative environment**

*a. Current services and capabilities.* AKO currently offers a range of enterprise synchronous and asynchronous services and capabilities through AKO:

(1) Text collaboration through e-mail, IM, chat and threaded discussion.

(2) Calendar.

(3) Notifications with the ability to both push and pull targeted information to targeted user groups.

(4) User feedback through polls, surveys and system statistics.

(5) Member lists.

(6) Sharing and storage of content and documents through knowledge centers and their related files.

(7) Self-service links.

(8) Content links to internal and external sources of content, including access to functional/domain specific applications and services through SSO.

*b. Site creation.* AKO will continue to expand and enhance services and capabilities through the AKO Requirements and functional capabilities management process (see para 3–9). Up-to-date information on specific capabilities and services and their employment will be maintained on AKO as changes occur.

*c. Organizational sites.* Organizational sites provide commanders with a virtual means to communicate key messages, push out targeted notifications, organize critical content and gather critical feedback and input. In the AKO enterprise collaborative environment, organizational sites are based on the official Army hierarchy and can be cascaded from the MACOM or HQDA level down to individual units and divisions. Commanders also have the flexibility to grant varying levels of access, establishing, for examples areas targeted to all AKO users and limiting areas to internal organizational groups.

*d. Team sites.* Team sites provide leaders and action officers with the ability to pull geographically dispersed individuals into teams and work groups to collaborate on specific projects and tasks. The AKO Enterprise Collaborative Environment allows team leaders to tailor their site to enable the exchange of information, collective problem solving, establishment and monitoring of milestones, and development of documents and other task/project related products.

*e. Individual work sites.* Individual work sites increase personal productivity by empowering all Army personnel with the ability to create a personalized site on AKO that centralizes the services and content required to accomplish everyday tasks and missions.

*f. Community sites.* Community sites provide communities with collaborative services that enable information sharing, dissemination of proven practices, virtual mentoring and peer assists, and collective learning and problem solving. Community sites differ from organizational sites in that they are not bound by official organizational structures but are often organized around a functional area, issue, topic, or profession that often cut across organizational lines. The AKO collaborative environment supports the mission of a variety of community types, including the two major types of communities recognized and sponsored by the DOD and the Army:

(1) Communities of practice (see AR 25–1 for definition).

(2) Communities of interest (COIs) (see Memorandum, Chief Information Officer, 9 May 2003, DOD Net-Centric Data Strategy, and AR 25–1 for definition).

(3) Structured professional forums, a community of practice subtype employed by the Battle Command Knowledge System to support practice areas and functions within the leader development and training domain (see glossary for definition).

*g. Knowledge networks.* Knowledge networks provide an official Army organization with the ability to aggregate and organize into a cohesive whole all of the services and capabilities required to manage communications, collaboration and knowledge services related to its particular function or domain. A knowledge network can comprise a wide variety of AKO sites and services with the integration through single sign on of additional function specific applications and services (see table 3–2).

**Table 3–2  
Collaborative Web sites**

Type	Subtype	Mission	Sponsorship
AKO homepage		Army Sr. leadership communication to AKO users	CSA's Office
Organizational sites	MACOM/functional	Functional/MACOM leadership communication	MACOM/functional leadership
	Subordinate	Unit leadership communication	Unit leadership
Virtual Team Sites	Official (chartered)	Enable team or group work efforts among geographically or organizationally disbursed team members	Chartering organization/official
	Informal	Enable team work efforts among geographically or organizationally disbursed team members	Team lead
Individual worksites		Increase personal productivity	Individual
Online community sites	Communities of practice	Collective development of a shared vocabulary within a mission area	Practice proponent
	COIs	Collective development of a shared vocabulary with a mission area	Mission area proponent
Knowledge networks		Integrate all services and activities required to communicate, collaborate and provide knowledge services related to a function or domain	Official Army organization

### 3–10. Requirements and functional configuration management

*a.* The AKO requirements management process is the authoritative means for all AKO users to provide constructive AKO feedback directly to the AKO division. The process is initiated by users via the AKO “feedback” button on the left menu frame of the home page. By utilizing the feedback button, AKO users drive the development and implementation of new functionality on AKO. All functional requirements are captured in a centralized system and evaluated based on a business case. AKO users should submit new functional change requests solely via the feedback button, as it expedites the review and evaluation process.

*b.* AKO requirements and change requests (CRs) are entered into the AKO functional change management process through direction taken from Army leadership, strategic plans, and missions. Change requests are submitted by AKO Functional Capabilities Control Board (CCB) members. General users wishing to submit an AKO CR may contact the AKO CCB member for their organization. All CRs must be vetted through the submitting community and submitted by the community’s CCB member to ensure that it is correctly input into the process. The functional change management lead in the Army CIO/G–6 is the recipient of all AKO CRs that enter into the AKO functional change management process. The AKO CCB convenes biannually and virtually, as needed, to review changes made to AKO and prioritize major enhancements that have been suggested. The AKO functional CCB page (found at <https://www.us.army.mil/suite/page/135320>) offers further information including a list of AKO CCB members, a diagram of the AKO functional change for each level of the management process, and the AKO CR document.

*c.* The functional configuration management process is integrated into the requirements management process to ensure a tight relationship between user needs and functionality development. The AKO Capabilities Control Board, the governing body for AKO, conducts a final review, validation, and recommendation for all functional changes to AKO. AKO Capabilities Control Board membership encompasses every AKO community.

### 3–11. Joint capabilities

*a. General.* The biggest challenge that the DOD faces is to improve the speed and quality of decision-making by connecting information producers and consumers more effectively through information technology and net-centricity. Global Information Grid (GIG) Enterprise Services (ES) is a suite of information, Web, and computing capabilities that will improve user access to mission-critical data. GIG ES will provide access anytime and anywhere to reliable decision-quality information through the use of cutting-edge, Web-based, networked services.

*b. GIG.* The GIG ES, consisting of hardware, software, policy, processes, and procedures, provides a way for the department to coordinate staff and allocate resources more efficiently by—

- (1) Rapidly discovering, obtaining, and tailoring information.
- (2) Helping teams share relevant information in real time in multiple media.
- (3) Protecting the integrity of information down to the last tactical mile and preventing its unauthorized disclosure.

(4) Publicizing information needs and notifying the necessary personnel when the required information becomes available. GIG ES enables DOD information and decision superiority from the command center to the warfighter.

(5) The Net-Centric Enterprise Services (NCES) Program is a joint IM/IT effort administered by ASD/NII and managed by the Defense Information Systems Agency (DISA). This program provides nine core enterprise services (CES) in the form of Web services and in a service-oriented architecture. NCES program details and information about the CES may be found on the GIG ES portal (<https://gesportal.dod.mil/>) using a common access card or DOD Public Key Infrastructure certificate for access.

*c. Enterprise services management/network operations.* This set of services provides end-to-end GIG performance monitoring, configuration management and problem detection/resolution, as well as enterprise IT resource accounting and addressing, for example, for users, systems, and devices. Additionally, this service area, similar to 911 and 411, encompasses general help desk and emergency support to users. Beyond these common core services, mission areas, domains, and communities of interest will leverage CES to develop services to meet unique mission critical needs (for example, Joint Battle Management Command and Control and Business Management Modernization Program). These services provide—

(1) Messaging—the ability to exchange information among users or applications on the enterprise infrastructure, such as e-mail, DOD-unique message formats, message-oriented middleware, instant messaging and alerts.

(2) Discovery—the process for discovering information content or services that exploit metadata descriptions of IT resources stored in directories, registries, and catalogs (to include search engines).

(3) Mediation—to help broker, translate, aggregate, fuse, or integrate data.

(4) Collaboration—the ability for users to work together and jointly use selected capabilities on the network. Examples of this include chat, on-line meetings, and work group software.

(5) Applications—the infrastructure that hosts and organizes distributed on-line processing capabilities.

(6) Storage—the physical and virtual places to host data on the network with varying degrees of persistence, such as archiving, continuity of operations and content staging.

(7) Information assurance/security—the capabilities that address vulnerabilities in networks, infrastructure services or systems. Further, these provide characterizations of the “risk strength” of components as well as “risk posture” of the hosting run-time environment in support of future dynamically composed operational threads.

(8) User assistant services—automated “helper” capabilities that reduce the effort required to perform manpower intensive tasks.

## **Chapter 4 Army Enterprise Architecture**

### **4-1. Utilization**

*a.* The Army enterprise architecture (AEA) is a description of the Army’s “to-be” enterprise, which acts as a framework/decision tool to support and improve Army transformation, business process management, system interoperability, and IT portfolio management. It is a federated architecture, incorporating operational views (OVs) (requirements), systems views (SVs) (architectures), and technical views (TVs) (technical standards) for Army tactical units, functional areas, and installations (see AR 25-1, paras 4-3, 4-4, and 4-5).

*b.* AEA products are used to assist Army leaders in the analyses of processes supporting various decisions. The timely and appropriate use of valid AEA products provides an effective enabling tool for an array of analyses in support of Army decisions.

(1) They are used to identify overlap and gaps in capability, interoperability, and supportability of IT and national security systems. They provide an analytical base for strategic sequencing of acquisitions, optimization of equipment fielding solutions, and the range of capital planning and investment decisions.

(2) Their effective use in these analyses helps avoid the costs of maintaining redundant capabilities and also greatly reduces risks to timely and affordable achievement of strategic objectives, including net-centricity, interoperability, and transition from current to future force. The ineffective use of AEA poses an increased risk of adverse strategic consequences.

### **4-2. Governance**

*a.* Effective governance is vital to ensure that AEA products and services are effectively used to inform Army analyses and decisions, as and when intended.

*b.* Processes to govern AEA planning, development, and maintenance must be in place, with accountability for roles established before the start of each AEA initiative.

*c.* Army architecture development is one of several functions assigned to Army mission area and domain leaders. Domain leaders identify stakeholders and establish COIs for efforts within their domain. Once established, a COI joins the domain leader in scoping and planning the effort.

- d. Army mission area and domain leaders are designated by the Secretary of the Army and the CSA.
- e. The CIO/G-6 serves as a supporting command to all mission area and domain leaders providing a common set of tools and templates that enable the integration and federation of architectures at the domain, mission area, and Army Enterprise level. The CIO/G-6 will coordinate and facilitate the Army architecture validation process described in paragraph 4-6 and act as the Army pre-certification authority for all Army architectures requiring OSD certification and approval.

### 4-3. Architecture development plans

Architecture development plans (ADPs) are developed by the Architecture, Operations, Networks, and Space (AONS) Directorate of the CIO/G-6, in collaboration with various stakeholders. ADPs articulate the purpose and scope of AEA efforts and delineate actions to develop, use, and maintain the products to be developed.

a. *Purpose.* The purpose is defined in terms of the primary customer's intended use(s) of AEA products or services. Each individual ADP identifies—

- (1) The primary user of deliverable products or services.
- (2) The executive decisionmaker or executive-level body to be informed by deliverables.
- (3) Specific analyses to perform or questions to inform (for example, identification of gap or overlap feasibility, affordability, and selection of alternative course of action).
- (4) Key decision processes and forums to be informed.
- (5) Documents that provide the basis for requirements.
- (6) Any relevant strategic objectives or joint mandates.

b. *Scope.*

(1) Each ADP defines what is in and what is outside the scope of the architecture effort and the constraints that must be dealt with. Scope determinations are made on the basis of a practical assessment of resources and competence availability, and the value that can realistically be expected to accrue to the enterprise from the chosen scope of architecture work.

(2) ADPs identify—

- (a) The extent of the time horizon goal.
- (b) The architectural assets to be reused, leveraged, or considered for use.
- (c) Products the effort will produce and the producers of those products.
- (d) Estimated resource requirements.
- (e) Detailed descriptions of scope for modeling and simulation requirements.

c. *Schedule.*

(1) ADPs provide detailed guidance for developing integrated architecture. Each ADP serves as a roadmap with an implementation plan to achieve the ADP's purpose. They contain data sufficient to facilitate initiation of project plans and enable project level control of costs, schedules, and performance.

(2) Schedule data address timelines for review and validation of product sets to be developed. They are sufficient to ensure that critical development sequences are fully synchronized.

### 4-4. Development

a. *Collaboration.* Architecture development requires collaboration. It is important to identify the appropriate stakeholders early and to provide a forum in which they can collaborate early, to build and gain stakeholder consensus on an ADP, roles and governance processes.

b. *Development process.* The architecture development process varies, depending on the type of analysis or decision to be informed. Although each AEA effort has a set of questions to answer and products that represent the solution set to those questions, the development process used may differ. For example, the unit architecture development methodology is used to facilitate the necessary links between the architecture development process and the Army's force development process. It provides the Army's architecture community with detailed guidance required for the production of consistent and comparable Architectures to support Army Transformation for deployable forces, from initial requirements analysis through to the fielding of the operational unit. A different methodology and guidance, defined by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01B, would be used to develop AEA products in support of the analyses and decisions in the concept development process. A requirement to support investment decisions would entail a slightly different process as well.

c. *AEA integration and federation.*

(1) Once the architecture has been developed, it needs to be integrated into supported and supporting architectures. For example, the architecture that is developed for a mechanized maneuver organization would need to be integrated with supporting fires architectures within the Army warfighting mission area and federated with the Army logistics domain architecture to ensure interoperability and alignment to Army Transformation. Integration across the OVs, SVs, and TVs of architecture (product-level integration for each architecture effort). This level of integration addresses

required analysis on how the architecture itself is integrated (how the products interrelate and are built so that the OVs, SVs, and TVs are fully traceable).

(2) Federation is the process of aligning architectures from multiple domains, mission areas, and even other component services and other non-DOD, Government organizations. Federation ensures interoperability and enterprise alignment, while maintaining the ability to develop, use and manage architectures at appropriate (small enough) scale to be useful and manageable.

*d. Project schedule and control.* Lack of synchronization could lead to misapplication of resources, duplication of effort, development of architecture products in a sequence that is inconsistent with warfighter needs, and deployment of noninteroperable, nonintegrated IT war fighting capabilities. AEA efforts must be managed and controlled as projects.

#### **4-5. Maintenance**

*a. Continuous improvement.* The Army must be a dynamic, learning organization with the flexibility to evolve rapidly in response to operational, political or technological changes within the warfighter, business, or EIE mission areas. Mission area and domain leaders ensure that their respective architectures reflect the continuous process improvement that should result from proactive business process management and the use of outcomes-based performance metrics within their respective mission areas/domains.

*b. Configuration management (CM).* CM ensures that changes to architectural products are managed in a cohesive, systematic, and architected way. Two types of CM must be practiced throughout the Army relative to architecture development efforts: CM of the architecture tools and templates used by Army architects at all levels, and CM of the developed architectures themselves. Architecture developers (mission area and domain leaders) implement configuration management with respect to the architectures under their supervision. Strong internal configuration management is essential to ensure the availability of valid AEA products for reuse. A set of security policies and procedures to govern the control and release of architecture information must complement the CM process. Architecture configuration management at all echelons must conform to configuration management in place at the next higher level (for example, program-level architectures must conform to domain architectures, domain architectures must conform to mission area architectures and mission area architectures must conform to army enterprise and DOD-level architectures as appropriate). AONS, in coordination with the Army executive architects, supervises the CM of Army-wide architecture tools and templates as described in paragraph 4-6.

*c. Validation.* Paragraph 4-6 describes the process by which Army architectures are validated and federated to ensure alignment with enterprise-level operational, technical and system requirements and architectures. Each army domain must submit an annual update to its domain architecture to be validated by the Army's executive architects (DCS, G-3/5/7; Assistant Secretary of the Army (Acquisition, Logistics, & Technology) (ASA (ALT))); and CIO/G-6). The Army's executive architects will act to adjudicate conflicts and identify gaps/overlaps across Army domain architectures.

#### **4-6. Army specific architecture development and validation requirements**

*a.* Army architectures are developed using Army-wide tools and templates produced and published by AONS in coordination with the Army executive architects. The CIO/G-6 publishes simplified versions of the DOD Architecture Framework (DODAF) tailored specifically for use by Army architects. For more information, refer to [www.defenselink.mil/nii/ea](http://www.defenselink.mil/nii/ea).

*b.* Army domain architectures must, at a minimum, include DODAF AV-1, AV-2, OV-4, OV-5, SV-2, SV-8 and TV-1 documents. These documents must be developed using appropriate Army templates so that domain-level architectures can be federated at the mission-area level.

*c.* Army program- and system-level architectures will include, at a minimum, DODAF AV-1, SV-4 and SV-6 documents. These documents must be developed using appropriate Army templates so that program-level architectures can be federated at the domain- and mission-area levels. Programs must also provide DODAF AV-2, SV-2, SV-8, and TV-1 configuration change requests or waiver requests for any elements of their program that do not conform to the respective designs for the domain-level architecture of which they are a federated component.

*d.* Army domain-level architectures must be developed and validated before the program- or system-level architectures for elements within a domain can be completed or submitted for validation against Army or DOD domain, mission area, and enterprise level architectures.

*e.* Figure 4-1 shows the Army architecture validation process. AONS is a supporting organization in this process tasked to facilitate and assist mission area and domain leaders by providing a set of common architectural tools and templates and processing Army architecture validation packages through the Army architecture validation process.

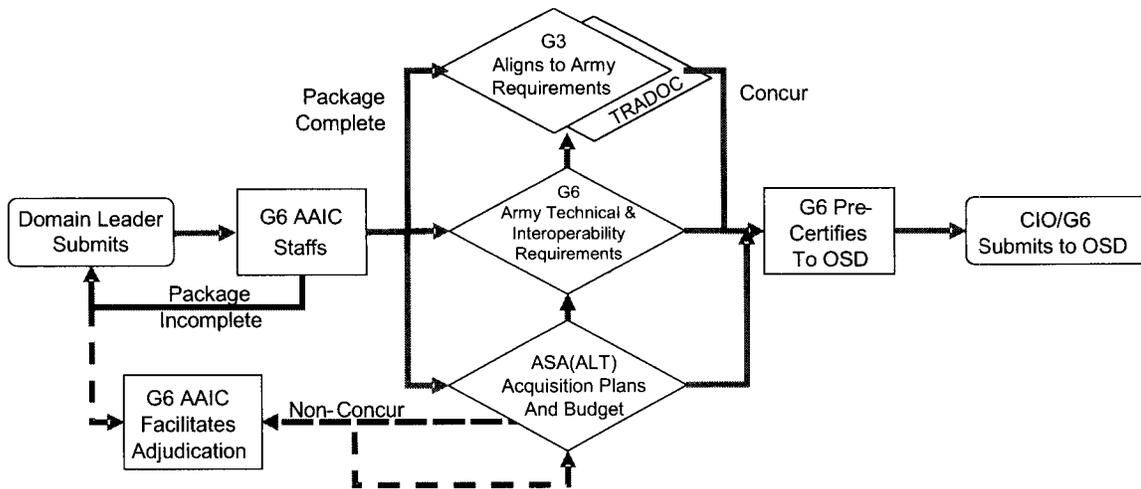


Figure 4-1. Army architecture validation process

f. In the Army architecture validation process—

(1) AONS assist program, domain, and mission area architects to prepare architecture validation packages by providing common tools, templates and submittal package prescreening.

(2) The DCS, G-3/5/7, in coordination with the United States Army Training and Doctrine Command (TRADOC) and other stakeholders, validates architectures with respect to required operational capabilities, identifying cross-mission functionality gaps and overlaps and ensuring alignment of business and enterprise information systems and architectures to the warfighting mission area architecture.

(3) The CIO/G-6 validates that submitted architectures are in compliance with the Army and DOD technology strategies and standards for interoperability, security, and technology and ensures alignment to Army planning and constraints with respect to network and communications infrastructure development.

(4) The ASA (ALT) validates the accuracy of architectures with respect to 5-year defense plan PPBE funding plans, acquisition plans, and other programmatic issues.

## Chapter 5 Army Net-Centric Data Management Program

### 5-1. General

a. *Purpose and scope.* The purpose of the Army Net-Centric Data Management Program (ANCDMP) is to provide guidance and oversight for the Army's implementation of the DOD Net-Centric Data Strategy and associated data management activities. Managing and leveraging information across the Army and, as appropriate, within DOD, is the overall mission of the ANCDMP. This chapter gives guidance and procedures about ANCDMP policy and direction contained in paragraphs 4-7 through 4-12 of AR 25-1. The procedures contained in this chapter apply to all Army organizations and programs that manage data and address the engineering of the ANCDMP, the identification and planning of ANCDMP projects, and the accomplishment of ANCDMP projects to ensure that Army data assets (in all forms) meet the DOD net-centric data goals and function in a net-centric environment.

b. *Net-centric data goals.* Further explanation of the goals is found in the DOD Net-Centric Data Strategy, chapter 2.2.

(1) Institutionalize data management. Data approaches are incorporated in department processes and practices. The benefits of enterprise and community data are recognized throughout the Department.

(2) Enable data to be trusted. Users and applications determine and assess the authority of the source because the pedigree, security, and access control level of each data asset is known and available.

(3) Make data accessible. Users and applications post data to a shared space. Posting data implies that descriptive information about the asset (metadata) is provided to a catalog that is visible to the enterprise and the data are stored so

that users and applications in the enterprise can access it. Data assets are made available to any user or application except when limited by policy, regulation, security, and law (for example, the Health Insurance Portability and Accountability Act of 1996), operational and/or technical constraints, or practicality (for example, bandwidth constraints).

(4) Enable data to be understandable. Users and applications comprehend the data, both structurally and semantically, and readily determine how the data may be used for their needs.

(5) Make data visible. Users and applications discover the existence of data assets through catalogs, registries, and other search services. All data assets (intelligence, nonintelligence, raw, and processed) are advertised or made visible by providing metadata that describes the asset.

(6) Support data interoperability. Many-to-many exchanges of data occur among systems through services and/or interfaces that are sometimes predefined or unanticipated. Metadata are available to allow mediation or translation of data between interfaces, as needed.

(7) Be responsive to user data needs. Perspectives of users, whether data consumers or data producers, are incorporated into data approaches via continual feedback to ensure satisfaction.

## 5-2. Terms and concepts

*a. Overview.* This section presents a description of the net-centric environment within which the ANCDMP exists. Standards, data assets, and metadata are basic concepts that constitute the elements of the net-centric data solution. Data performance planning (DPP), data interoperability, COI, and data management are mechanisms and processes for moving toward the solution. Related terms and concepts are defined in the glossary.

### *b. Net-centric environment.*

(1) Data that enable effective and timely decisions are the core of the net-centric environment. Here, data imply all data assets such as system files, databases, documents, official electronic records, images, audio files, Web sites, and data access services. One of the CIO/G-6 goals is to populate the network with all data and shift the paradigm from “process, exploit, and disseminate” to “post before processing.” Under this concept, all data are advertised and available for users and applications when and where needed. Users receive alerts when data they have subscribed to are updated or changed. Users and applications have instant access to data posted to the network without processing, exploitation, and dissemination delays.

(2) Users and applications tag data assets with metadata, or data about data, to aid the location of data assets. Users and applications may tag data-asset data to aid the exchange of data assets. Users and applications post data assets to shared space for use by the enterprise.

### *c. Standards.*

(1) AR 25-1, paragraph 4-8, identifies four Army data standards vital to implementing the data goals: authoritative data sources (ADS), enterprise identifiers (EID), information exchange standard specifications (IESS) and eXtensible markup language (XML). An ADS is a data asset designated as authoritative. EID is an implementation independent identifier for a real or abstract asset. IESS is a standardized specification of a data asset that is exchanged. XML is a tagging language that describes and annotates data being exchanged.

(2) More standards are required to enable the net-centric environment: technology standards, data wrapping standards, discovery and availability standards, and architecture development standards.

*(a)* Technology standards include structured query language (SQL) and International Organization for Standardization (ISO) 11179 and implement the standardized expression needed for certain content. In the SQL command, CREATE TABLE Customer, CREATE TABLE is the SQL data definition syntax and Customer is the content. Standards addressing uniform expression are SQL and ISO Standard 11179. SQL forms the language usually used to express data content’s definition, access, and protection in each collection of data asset instances. ISO Standard 11179 for data element metadata controls the engineering of the metadata around unitary facts. XML is a text-based method and set of syntax rules for encoding (tagging) metadata, allowing COIs to develop mission specific markup language. Tagging of data in the net-centric environment uses XML syntax rules.

*(b)* Data wrapping standards, usually typified by XML and spread by the World Wide Web Consortium, wrap collections of data in tags to be transported between processes and environments in a technologically independent way. Simple object access protocol (SOAP) is a common XML-based protocol providing the envelope syntax for sending and receiving XML messages.

*(c)* Standards for discovery and availability impact net-centricity. These standards include universal description, discovery and integration (UDDI), and Web services description language (WSDL). UDDI provides a conceptual phone book for Web Services. Organizations may register information about their Web services and types of services with UDDI. WSDL describes the operational information—where the service is located, what the service does, and how to talk to, or invoke the service. These standards are important to the concepts of visibility and accessibility of data as addressed in the DOD Net-Centric Data Strategy. Reference for the DOD approach to visibility and accessibility is found in the DOD Discovery Metadata Standard.

*(d)* Architecture development standards are needed because the semantic meaning and rules for information exchange need to be determined. It is important to remember that XML does not create semantics; it uses already created

semantics. Semantics need to be captured and documented in the integrated architecture development process and products. In the context of data interoperability it is vital to focus on data-related architecture products and model those elements that help develop the COI and cross-COI Ontology. Data-centered ontologies include entities, relationships, properties, values, and axioms/rules.

*d. Data asset.*

(1) A data asset is data in all forms: raw, processed, intelligence, nonintelligence, processes, applications and data sources. All data assets must be supported by a data asset product.

(2) A data asset may be an IESS data asset when it represents a consensus based data exchange standard determined by its user community. An IESS is a standard because it is subject to configuration management by its user community.

(3) A data asset may be designated as an ADS when its value set is declared to be definitive. An ADS value set is subject to configuration management.

(4) A data asset may have its data uniquely defined through EID so that EID-based assets can be discovered, analyzed, and combined.

(5) A data asset may be in either XML format or some other format.

(6) Data assets in information systems must be periodically reviewed to ensure that data assets (exposed and unexposed) are available to the widest possible community. A data asset is considered exposed when it is tagged/registered with a proper metadata registry; registered in an enterprise searchable catalog; understandable; and accessible to the widest possible community.

*e. DPP.*

(1) The DPP process aids in the creation and management of products needed to define the data and metadata of data assets. Thus, DPP identifies, plans, and manages projects associated with data assets throughout the entire lifecycle of the data asset. DPP projects produce products for future and improved data integration and reuse. DPP enhances project scoping, responsiveness to business change, and management of systems development sequencing and prioritization.

(2) A data asset project is an organized set of activities used to solve problems related to the seven goals of the DOD Net-Centric Data Strategy. Data asset projects produce one or more data asset products identified within the DPP process.

(3) Data asset products are the data-specific inputs needed or outputs produced in data asset life cycle activities. Data asset products commonly organize and define interrelationships of data in support of each organization's missions, functions, goals, objectives, and strategies. These products give the basis for the incremental, ordered design and development of one distributed virtual database founded on successively more detailed levels of data specifications to build out the data asset product set. DPPs identify the set of data asset products in each data asset project. Data asset products may be explicitly identified as DODAF views or may exist implicitly within DODAF views. DODAF cites a set of architecture views (AV, SV, TV, and OV) that, when used as an integrated set, describe characteristics pertinent to the purpose, design, and implementation of the architecture. Explicit data asset products are AV-2, OV-3, OV-6a, OV-7, SV-6, and SV-11. Remaining DODAF views may be implicit data asset products required to derive the information for the explicit products. All data asset products must be integrated and interrelated within and across COIs.

*f. Metadata.*

(1) The term metadata refers not only to the set of definitions of the data in a data asset (for example, products, parts, and prices), but also to its formats, processing, transformations, and routing from source to target information system. Everything except the data's content constitutes metadata. All products in the DODAF, including the data asset products, are metadata and must be core architecture data model (CADM) conformant. All metadata management tools must be capable of creating CADM conformant products. The term Data Performance Planning System from AR 25-1, paragraph 4-7, means any CADM conformant metadata environment.

(2) Metadata allow for content management. Metadata foster knowledge of the content, the environment within which content resides, the interrelationship among content environments, and the ability for content to evolve. High-quality metadata management promotes flexibility, interoperability, evolution, and discovery.

(3) In the context of net-centric conforming data asset DPP, metadata include information supporting the definition of missions, events, information systems, functions, and organizations associated with COIs.

*g. Data interoperability.*

(1) The data aspects of interoperability may be summarized by the term basic interoperability, which is the exchange of information that preserves the meaning and relationships of the data exchanged. In order for information to be fully understandable and interoperable, it is required at a minimum that—

(a) Its semantics and syntax are well specified.

(b) Its data elements are identifiable at the enterprise level.

(c) Its authoritative data sources are well defined and managed.

(d) Its exchange mechanisms are able to support current and future demands.

(2) Interoperability consists of two parts: shared value streams and shared understanding. Both are created from within the COI and are expressed via the IESS.

(3) The role of EIDs within data interoperability is to support technology independent mechanisms to understand both metadata and values (both single value and value sets).

(4) The role of ADS is to minimize the versions of the “truth.” Additionally, an ADS enables the coordinated migration of “truth” from an originating value state through a chain of value states until the data source is either archived or deleted.

(5) Finally, the role of XML is to take the value streams from an originating system and to transport them to an IESS or vice versa. Embedded within the XML stream are the EID tags that enable users to both understand the authority of the value sets and the supporting metadata. It is the primary function of a data model to provide a common specification of the meaning and relationships of information by which interoperability may be achieved. The IESS is a logical data model that represents the shared data of legacy system physical data models from members of a COI. The COI’s end product is not only the IESS; it is also the mapping between the IESS’s logical data model and the legacy system physical data models. To have consistent semantics across all the IESS logical data models, there needs to be two additional data model layers: enterprise data elements and shared data structure templates (conceptual data models).

(a) The enterprise data elements are fact-based, semantic templates for all the columns in the tables of the logical data model. These enable COI logical data models to be interrelated. The enterprise data elements will come mainly from the DOD Data Dictionary System by discovering those data elements that are truly unique. For example, at the enterprise data element level there is a need for one supply condition code, not 27.

(b) The shared data structure templates (conceptual data models) facilitate the “manufacturing” of data models’ well-engineered collections of commonly employed enterprise data elements (for example, materiel requisition or disposition, facility location characteristics, and person biographic information). Shared data structure templates mainly will be “mined” from the Defense data architecture. Enterprise data elements are based on the ISO standard 11179, Part 3; and the conceptual, logical, and physical data models are based on ISO/American National Standards Institute (ANSI) standard SQL.

#### *h. COIs.*

(1) A COI is a collaborative user group that must exchange information in pursuit of shared goals, interests, missions, or business processes, and that must have a common vocabulary (names, meaning, and schema/format) and set of business rules for the information exchange.

(2) The COI structure consists of three layers. The first layer is an Army data harmonization and integration (ADHI) COI that defines the central concepts that are used in total or in part by any other COI. Examples of such basic concepts are facilities, organizations, persons, and materiel. The second and third layers consist of institutional and expedient COIs, respectively. Enterprise data elements and shared data structure templates constitute the primary data asset for the ADHI COI. Whatever data schema an institutional COI develops would have to be conformant (in the ISO 11179 sense) to the ADHI schema as a starting point. Only then would each institutional COI extend its data specification to cover its functional area. Expedient COIs, which typically are cross-functional, will need to coordinate capability gap analysis results with institutional COIs for long-term correction and management.

(3) Institutional COIs supervise the long-term development and configuration management of their respective functional area vocabularies, business rules, and authoritative data sources. Expedient COIs are formed to address high-priority, capability deficiencies that must be addressed in a timely fashion to support command priorities and operations. Expedient COIs will typically be cross-functional and will need to coordinate capability gap analysis results with institutional COIs for long-term correction and management.

(4) COIs form in a variety of ways and may be composed of members from one or more functions and organizations as needed to develop the shared mission vocabulary. Every COI has a lead and a set of stakeholders supervising its operations. COIs contain data asset producers and consumers. COIs may cross mission areas and domains. Expedient COIs may be created when necessary. Their data asset products are incorporated into the parent’s COI product set. New COIs are formed as needed and old COIs terminated when no longer useful.

*i. Data Management.* Data management addresses the independent management of data shared by multiple applications. Data management supports data exchange and includes data dictionary, directory services, and database management systems (DBMS). DBMS support the definition, storage, and retrieval of data elements from monolithic and distributed DBMS. Information systems that employ commercial off-the-shelf (COTS) DBMS must conform to the requirements of SQL:2003, Core.

### **5–3. Roles and functions**

DOD Net-Centric Data Strategy calls for establishing COIs to address the organization and maintenance of data using metadata and GIG enterprise services consistent with DOD and Army enterprise architecture guidance and pertinent legislation. Further details concerning the framework for the development and integration of COI and cross-COI data and other standards will be addressed in follow-on guidance generated by the Army CDAd in cooperation with the mission area and domain leads and their respective COIs. The following items provide initial guidance on the way

ahead for Army Net-Centric Data Management. The primary set of functions is specified in AR 25-1, paragraphs 4-7 through 4-12. Additional functions are specified below.

*a. COI formation.*

(1) COIs are established to address net-centric data problems. The organizational construct is based on mission areas and associated domains to ensure that COI efforts support Joint and Army requirements in a net-centric environment. Initial institutional COIs fall under mission area leads associated with the GIG mission areas. Mission area and COI leads coordinate with the CIO/G-6 to ensure that cross-mission area and cross-COI information exchange requirements and standards are coordinated, addressed, and documented. Mission area leads will ensure a systems engineering approach is utilized to minimize overlaps and redundancies of COIs within a mission area.

(2) Army organizations wanting to form a COI must determine the appropriate mission area and coordinate with the respective Army mission area and domain lead. Army organizations asked to participate in Joint COIs will notify the appropriate Army mission area and domain lead. The Army will establish COIs only if no Joint COI addressing the area of interest or specific problem (for which the COI needs to form) exists.

(3) For the purpose of gathering Army input and establishing common Army positions to Joint COIs, Army-only COIs may form for a period to be determined by the Army mission area lead. Army only COIs may also form if the Army mission area lead determines that the purpose of the COI is an Army unique issue.

(4) COIs established by the Army, unless formed to answer an Army unique issue, will be open to Joint, interagency and multinational organizations and coordinate as appropriate with Joint mission area and domain leads. COI leads will be appointed by the mission area lead, within the respective mission area.

(5) The COI assists Army mission area and domain leads in the oversight and coordination of the development, implementations and maintenance of COI and cross-COI developed information exchange standards specifications and associated standards and processes.

*b. Additional functions of the Army component data administrator (CDAd).* The CIO/G-6, the Army CDAd, is the Army lead for implementing DODD 8320.2, to include—

(1) Coordination, integration and maintenance of IESS.

(2) Coordination of ADS across Joint and Army COIs.

(3) Coordination of enterprise identifiers across Joint and Army COIs.

(4) Development and coordination of technical implementation guidance.

(5) Coordination, management and integration of COI data-related architecture products with operational, system and technical architecture products.

(6) Coordination, integration, and maintenance of other related data standards that may be identified as critical to the success of data interoperability.

*c. Additional functions of mission area leads and domain leads.*

(1) Army mission area and domain leads will collaborate with Joint COIs associated with their mission area and cross-mission area requirements when formation of a COI is required. The Army mission area or domain leads will engage the appropriate DOD/Joint body to request formation of that particular COI. If the request is not supported by the DOD/Joint body, the mission area lead may opt to form an Army-only COI. If an Army COI is required, the lead will oversee and coordinate, within their mission area, the development of a common information exchange standards specification, to include specific ontologies and the development of a common mission area vocabulary (names, meaning, schema/format) and the business rules for the exchange of information.

(2) Mission area leads will appoint, as necessary, COI leads in their respective mission areas. Mission area and domain leads will work with the designated COI lead to establish appropriate governance strategies as well as data stewardship priorities, resources, proponentcy, and migration strategies for legacy systems in the COI.

(3) Mission area leads coordinate, harmonize, and achieve, to the greatest extent practical, non-redundant, shared data asset metadata in and across domain COIs.

(4) Mission area leads will notify the Army CDAd of the formation of COIs associated with their mission area and provide the Army COI lead point of contact.

(5) Army mission area leaders—

(a) Define domains and domain owners.

(b) Manage subordinate domains.

(c) Supervise mission area architecture and capability planning.

(d) Identify ADS within the mission area.

(e) Monitor cross mission area and enterprise coordination.

(f) Coordinate resource requirements for the establishment and maintenance of COI activities and products.

(g) Coordinate with Joint, interagency, and multinational counterparts.

(6) Army domain leads—

(a) Manage domain portfolios and information capabilities.

(b) Ensure COI capabilities and infrastructure are resourced.

(c) Monitor domain architecture and capability planning.

- (d) Identify ADS within the domain.
  - (e) Facilitate cross-domain information sharing
  - (f) Coordinate with Joint, interagency, and multinational counterparts.
- d. Additional functions of COI leads.*

(1) The COI leads will oversee the data management activities, identify appropriate governance strategies, and appoint a COI data administrator to carry out and implement data management actions for the COI.

(2) COI leads will provide courses of action for the transition of legacy systems and data repositories that need to be incorporated into the GIG.

(3) COI leads will coordinate with the Army CDAd to ensure that their activities, efforts, and products are integrated at the Army and Joint level.

(4) COI leads will ensure that their common vocabulary is harmonized with their COI ontology development and the mission area ontology efforts to enable visibility and accessibility and accessibility of their data assets.

- (5) COI leads—
  - (a) Develop the COI common vocabulary (semantic and logical agreements for data).
  - (b) Capture COI operational/business rules for the exchange of data.
  - (c) Register COI data schemas and models in coordination with Domain leads.
  - (d) Identify ADS within the COI.
  - (e) Promote data sharing across the enterprise.
  - (f) Supervise the COI net-centric migration plan.

*e. Additional functions of COI data administrators and COI data standards producers.* COI data administrator functions are found in AR 25–1, paragraph 4–8d. The duties focus on the coordination and integration of COI and cross-COI data standards in their domain area. COI data standards producer functions are found in AR 25–1, paragraphs 4–9 through 4–12. The duties focus on the coordination and integration of data standards within their COI.

*f. Additional functions of the COI.* Each COI creates and maintains the COI’s shared vocabulary, shared data spaces, metadata catalogs, and the registration of all pertinent metadata. During the accomplishment of the COI’s program and scope of work, COIs—

- (1) Create a shared understanding of the terms, a vocabulary used to describe and define the data assets.
- (2) Assist Army mission area and domain leads in the oversight and coordination of the development, implementation and maintenance of COI and cross-COI developed information exchange standards specifications and associated standards and processes.
- (3) Execute data performance planning through data asset projects that identify, create, and maintain data asset products. When OVs, SVs, and TVs required to sufficiently model the mission-related architecture, desired capabilities, and related ontology do not exist, then COIs must develop or coordinate for the development of necessary products.
- (4) Capture the data asset specifications used by the COI. COIs work with architecture efforts in their problem space to ensure that data asset products stay aligned and integrated with all other appropriate DODAF products.
- (5) Focus on that part of its subject area with the highest return on investment. High-priority information usually includes information required by a new or future capability and information that must cross organization or system boundaries. Operational and system architecture descriptions may be used to identify this information. Architecture products from associated architecture domain lead(s) help guide COI efforts to set information priorities.
- (6) Ensure data assets are visible and accessible.
- (7) Ensure data asset products meet the requirements of the NCES, including tagging data assets with discovery metadata and posting data assets to appropriate shared spaces.
- (8) Register their data asset products through the Army CDAd for posting to the DOD Metadata Registry.
- (9) Create and maintain a metadata catalog of data assets. All data owners ensure that their data assets are described using the COI’s subject-area vocabulary. This description includes the operational data owner in charge of the asset. The cataloging of data assets in the net-centric environment ensures that intended and unintended data consumers are able to discover the data asset by facilitating the organization of the data assets. The NCES discovery service, in accordance with the DDMS, makes descriptive metadata in each COI catalog available.
- (10) Determine use of a COI shared data space.
- (11) Ensure that data assets that are to be interoperable are supported by EIDs, IESSs, and, as appropriate, XML to support asset identification and access, shared data exchanges, and exchanged data formatting.
- (12) Identify data assets that are the ADS in the COI subject area, including the operational data owners supervising their management. COIs may have to resolve potentially contradictory sources and coordinate with DOD-wide governance bodies to reconcile/adjudicate authoritative source(s).
- (13) Document the COI data visibility and access plan showing how and when they make their data accessible across the GIG. COI stakeholders and associated systems coordinate to develop and execute the plan.
- (14) Determine data owners and controllers to determine data creation and update cycles that govern the business rules related to data interchange.
- (15) Develop data asset projects’ plans, schedules, and funding. All COI participants and data owners update their

planning, programming, and budgeting system processes and policies, as well as acquisition processes and policies, to reflect their participation in the COI effort.

*g. Additional functions of COI stakeholders.*

(1) Along with the user community, material developers, program managers, system owners and data producers make up the stakeholders of a COI. The system development, acquisition, and migration approach defined by the COI will need to be planned for and executed by the stakeholders of the COI. Stakeholders—

- (a) Assist in the development and execution of the COI net-centric migration plan
- (b) Tag data with discovery metadata.
- (c) Make data available to shared space.
- (d) Create searchable catalogs of data assets.
- (e) Register metadata in appropriate registries, directories.
- (f) Plan and budget for services or capabilities to be exposed to the enterprise.

(2) The above stakeholder efforts are associated with working within the COI construct. In the absence of COI activity, stakeholders and material developers can take the following actions to prepare for net-centric operations:

- (a) Identify and prioritize shareable data assets within their individual systems.
- (b) Identify candidate ADS (those currently used by the system or considered for use by the system).
- (c) Identify candidate services that the system may provide to the enterprise.
- (d) Plan for migration of their system/application to operate in a net-centric environment using Web services and associated protocols (for example, XML, SOAP, UDDI, and WSDL).

*h. Additional functions of Army components.* During the information management process, Army MACOMs and functional organizations—

- (1) Execute their information management functions in accordance with AR 25–1.
- (2) Ensure materiel developers comply with Army and DOD data needs by developing and maintaining data artifacts (such as standards, policies, procedures, data models, and business rules), and use them as appropriate to ensure maximum interoperability within and among COI-based IT systems.
- (3) Work with mission area and domain leads and respective COIs to manage the COI data asset projects and products.
- (4) Provide and use only ADS used by the organization's business processes so that uncontrolled duplicate data sources are eliminated.
- (5) Designate operational data owners who are people who exercise authority over the contents of the ADS. Their decisions include what data must be collected, how data are represented and stored, how data are validated, the required degree of accuracy, precision, and other quality factors, when data are released, who is allowed to access and update data, and so on. (This is an operational role, requiring authority to match functions. It is not directly concerned with IT, though it will require supporting IT expertise.)
- (6) Make data available to consumers in the GIG, which entails removing any arbitrary system implementation barriers to data access. Restrictions on data access will remain, but these are all based on deliberate policy choices (for example, security classification) and not on the accidental result of incompatible infrastructure.
- (7) Make data discoverable and understandable, which requires provision of appropriate descriptive metadata. Discovery metadata allow potential consumers to locate data sources through a search service. Data owners supply discovery metadata. Additional metadata may be required for consumers to understand whether the intended meaning of the data is acceptable for their purpose, especially when establishing a machine-to-machine data exchange. These structural/semantic metadata are registered with the DOD Metadata Registry.
- (8) Develop and use a common vocabulary (ontology) via one or more COI that includes all steps in the IM process depending on an ontology that defines the meaning of data. COI IESSs are developed to document COI common vocabulary and represent the logical-conceptual parts of the COI ontology for data interoperability and information exchange.
- (9) Ensure that data management resource requirements are identified and addressed in the POM process such that Army Components must work within the POM process to articulate the financial resources and the manpower authorization requirements necessary to implement the ANCDM policy in their function area.

#### **5–4. Layers**

The ANCDMP consists of three distinct layers: the ANCDMP layer, the DPP layer, and the project execution layer. These layers cascade one into the other.

*a. ANCDMP layer.*

(1) *Strategy.*

(a) The strategy of the ANCDMP is top-down guidance and facilitation coupled with bottom-up data asset development. Data asset products reside in COIs and are integrated in a federated metadata environment. The data asset products across Army COIs are harmonized. These data asset products are registered, as appropriate, to the DOD Metadata Registry and harmonized across DOD as appropriate.

(b) The ANCDMP goal is to achieve net-centricity by developing an integrated set of data asset products resulting in an enterprise level understanding of terms and concepts and associated business rules for the exchange of information.

(2) *Governance.* The oversight of the ANCDMP is through policy, guidance, and COI data goal assessments. Supporting the guidance are workshops, white papers, seminars, and software tool sets. These assist Army staff as they develop, publish, integrate, and maintain all data asset products in and across COIs.

(3) *Assessments.*

(a) The DOD and Army Net-Centric Data Goals are the characteristics through which data performance planning, data asset projects, products, and assets are assessed.

(b) Metrics are established for each goal to assess the degree to which they have been achieved. One or more objectives are established in each goal. One or more strategies are established in each objective. Objectives and strategies characterize broad actions to pursue each goal.

(4) *Program components.* ANCDMP includes process, technology standards, metrics, project management, Army data standards, DPP, and training and awareness.

(a) The process includes the overall strategies and activities required to be performed to accomplish the program's objectives. Examples of ANCDMP process projects include the data policies and procedures, the management of data asset product specifications, the management of those products into the DOD Metadata Registry, and the ANCDMP methodology through which all ANCDM products are created, interrelated, employed, and evolved.

(b) The standards include: SQL, ISO 11179, SOAP, XML, UDDI, and WSDL. The Army adopts relevant standards and use profiles if they are recognized by the appropriate standards bodies and are found to be appropriate for Army use.

(c) The metrics include different classes of metrics that can be measured across the IT life cycle to determine resource requirements associated with data related architecture products and views (that is, schedule and cost).

(d) The project management includes the organization, planning, ongoing management, and evaluation of various ANCDM projects.

(e) The Army data standards include ADS for definitively identifying source data assets, IESS for creating shared data specifications, XML for data transport, and EID to uniquely identify instances of data assets.

(f) The DPP is a structured approach through which the full set of ANCDM projects are identified, defined, and collected so that resulting data assets and their products are judged compliant with the DOD net-centric data goals.

(g) The training and awareness includes seminars, documents, white papers, workshops, and Web sites through which all projects of the ANCDMP can be understood and completed.

b. *DPP layer.*

(1) *Strategy.*

(a) The ANCDMP applies Army direction for managing COI activities and the development of data asset products. DPP is the term coined by the Army CDAd to describe this process. It is the COI program management plan for the development, scheduling, resource management, and evolution/migration strategy of the COI systems to the common COI net-centric interoperability solution(s). Programs of record in a COI coordinate as appropriate to ensure that their individual development and fielding plans are harmonized with the COI DPP for the purpose of coordinated fielding of capabilities.

(b) DPP defines the COI mission, scope, schedule, resource requirements and metrics for success; the COI participants; required data asset products; and the coordinated plan for harmonizing the fielding of capabilities. It also provides guidance on the implementation and use of ADS, EIDs, and XML in the COI. Where COIs identify requirements to exchange data across COI boundaries, the DPP addresses those common COI solutions.

(c) DPP results in the development of the data asset project action plans that set out the plans to achieve the DOD net-centric data goals for data.

(d) DPP projects are identified to implement strategies that achieve objectives and attain capabilities. Supporting action plans achieve DPP projects. Measures identified for the supported goal are incorporated into the action plan for the specific project (such as the development of a COI common logical data model).

(e) DPP projects do not effect the creation and/or evolution of data assets. DPP projects identify, plan, and manage data asset project accomplishment. Actual data asset projects develop and/or use the data asset products to create or evolve a specific data asset. To eliminate the stovepiping of data interoperability solutions, data related architecture products must be integrated with the supporting, nondata-related products within the OV, SV, and TV DODAF architecture views. This process should focus on ensuring proper integration with, and mapping to, higher level architectures and ontologies as appropriate.

(f) A focus of a data asset project within DPP is to create and manage an environment within the Army that enables the development of flexible, interoperable, and evolvable data assets.

(2) *Projects.* DPP projects begin with a problem statement that is taken through a thorough functional and technical analysis process, resulting in a viable solution for implementation at the proper Army level, ranging from specific, pair-wise, and database-to-database exchanges up to enterprise-level data sharing in a "virtual, distributed single database"

environment. DPP projects result in the identification of specific data asset projects. At a minimum, every DPP project has three steps:

(a) Developing the problem statement. The problem statement is an external statement of requirement or deficiency to identify the need, or the identification of the deficiency to be addressed, the new need to be addressed, or the need for improved performance to be addressed. Performing the required analysis includes employing COI/enterprise missions, functions, and organization to frame or focus the analysis. If possible, refine this analysis to the point of specifying the problem space to the appropriate level of detail. Develop an initial DPP project problem statement. Identify the specific objectives that must be achieved to support mission performance. This is a statement of desired results, with specific and measurable outcomes that contribute to achievement. Use existing and legacy data models to produce a documented normalized data model representation of the current data-for-exchange environment. Review the information with user representatives to verify the “as is” or current environment documentation. The product of this review is a verified specification of the current environment.

(b) Configuring relevant data asset projects to include their work breakdown structures as task statements that support the accomplishment of the data asset project. The data asset project includes the various data performance goals and objectives to be achieved. Alternative approaches are created and evaluated through proof of principle projects that validate the suggested alternative (risk reduction) or validate the specifications (for issuance to the developer).

(c) Managing the data asset project to include monitoring and evaluating the proper use of a created data asset, cycling back lessons-learned reports, issue resolution reports, or refinement of performance metrics employed in the development effort. In the data asset project, the nature of the technical solution, evaluations via the functional user, and technical environments are accomplished.

(3) *Project classes.* ANCDM projects are accomplished in support of some aspect of the ANCDMP overall program. Each project has a firm goal, specific objectives, a work plan, metrics, deliverables, and a schedule that must be accomplished. Each project is scoped, its work plan developed, resource loaded and staffed, and managed during its accomplishment. All deliverables must fit within the overall set of all deliverables from all the other ANCDM projects. The following are examples of DPP project classes:

(a) Architecture projects are targeted at the engineering, design, deployment, and long-term evolution and maintenance of the components within the ANCDMP. Included are the ANCDMP’s overall process, specific standards such as SQL, XML, 11179 Data Element metadata, metrics, project management, the Army data standards such as EID, ADS, IESS, XML (as appropriate for data transport), and the metadata repository environment that creates, holds, and interrelates all data asset products within and across all COI.

(b) Concept of operations projects address: process, standards, metrics, project management; technical components such as ADS, EID, IESS, XML; and the federated metadata repository environment.

(c) DPP infrastructure projects are generally in these areas: metadata management, CADM conformance, the evolution of the environment’s functionality, and extensions to the DPP functionality.

(d) Training and awareness projects create various presentations, workshops, courses, and support services such as hotline and online tutorials.

(e) Methodology projects allow different groups of persons, whether contractor or Army, to produce the same set of deliverables from the same or similar requirements. The methodology is to be at least one or more levels more detailed than the actual management of the work. Methodologies have well engineered deliverables and metrics for work efforts. Methodologies are associated with training, workshops and, consulting. Methodologies may address any aspect of the ANCDMP effort. Ultimately, methodologies are procedural guidance that allows quality products to be developed.

(f) Technical support projects are engineered to make experts available to those performing an ANCDMP project.

*c. The project execution layer.*

(1) This accomplishes the ANCDMP projects that have been identified and planned in the previous layers.

(a) From the ANCDMP layer, the projects include those related to policy, guidance, the DPP process, explicit and implicit data asset product engineering and specification, and also workshops, and other types of training and facilitation.

(b) From the DPP layer, the projects relate to the detailed planning required for the proper accomplishment of the various data asset projects.

(c) Finally, from the project execution layer, the complete set of all projects identified and planned is executed, monitored, and the various lessons learned are cycled back.

(2) In the area of data assets, examples of specific projects include: analysis and development of the IESS; identification of ADS, implementations of EID, development of XML schemas, configuration management, and test of COI interoperability solutions.

## Chapter 6

# Managing Information Technology at the Installation: Support and Organizational Constructs

### 6-1. General

- a. NETCOM is in charge of Army-wide oversight of enterprise level assets.
- b. The DOIM monitors installation-specific IT assets. The DOIM is assigned to the Army's IMA region and is under the technical control of NETCOM through the RCIO. NETCOM provides technical guidance to the DOIM for information management services. In this way, standard basic service levels are offered enterprise-wide, independent of a user's organization or location.
- c. NETCOM provides Army-wide common C4/IT services and applications. These services and applications are offered according to baseline service levels funded by the ACSIM. The service provider defines baseline services based upon affordability within available resources. Changes in baseline resources may require changes in baseline services. Changes in service levels must be consistent and equitable. NETCOM (through the DOIM) negotiates Service Level Agreement (SLA) extensions to baseline services with customers for service needs above the established Army baseline for each service. SLA extensions are based on measures such as availability, reliability, and response time that are checked to assess NETCOM operations and customer satisfaction. In this way, standard service levels are provided enterprisewide. Common service and application categories include, but are not limited to—
  - (1) Telecommunications.
  - (2) Visual information.
  - (3) Document management.
  - (4) Automation.
  - (5) Information assurance.

### 6-2. Installation Management Agency

- a. The IMA provides equitable management of Army installations to aid mission readiness and execution; enable the welfare of soldiers, civilians, and family members; improve infrastructure; and protect the environment. The garrison DOIMs, who are on the IMA table of distribution and allowances (TDA), support the following objectives and business processes:
  - (1) Sustain and improve the infrastructure.
  - (2) Support mission commanders.
  - (3) Apply process and quality improvement initiatives/programs.
  - (4) Protect the force.
  - (5) Provide environmental stewardship.
  - (6) Leverage IT and knowledge.
- b. HQ IMA exercises command and control and resource oversight of the DOIM through the extension of its headquarters staff at the region to the garrison commander. Staff supervision and technical control of the DOIMs is given through the NETCOM RCIOs.

### 6-3. Network Enterprise Technology Command regional units and regional chief information officers

- a. In accordance with the IMA, NETCOM regional units were established to provide C4/IT support to IMA Regional Directors (RDs). Each RCIO performs regional functions for C4/IT capabilities and assets for a designated region.
- b. NETCOM regional units and RCIOs enforce C4/IT policies, standards, architectures, programs, plans, and budgets for all IT in their assigned areas.
- c. The RCIO exercises staff supervision for C4/IT units under the supervision of the RD. The RCIO exercises TECHCON for C4/IT units not yet assigned to the RD. The RCIO aids signal operations, automation management, network management, and information security. The RCIO advises the RD on all C4/IT issues and coordinates programs, issues, actions, and so on, with other regional staffs. The RCIO reviews and suggests actions on C4/IT requests, needs, budgets, and SLAs. The RCIO develops the RD's communications plans, C4/IT budgets, automation plans and standards (see AR 25-1, para 3-2). As a tenant, the RD/NETCOM staff receives baseline services from the garrison DOIM and the garrison. The RCIO duties are divided into two major functions:
  - (1) C4/IT enterprise leadership.
    - a. The RCIO uses guidance given by the CIO/G-6, NETCOM (including commands or brigades), and the RD to develop a vision and strategic objectives that aid the needs of customers.
    - b. The RCIO is involved with the processes that develop links between vision and projects, while considering resource constraints. The regional C4/IT strategic plan is based on the Army CIO/G-6/NETCOM C4/IT strategic plan.
    - c. The RCIO is a member of the NETCOM RCIOs council that meets at least semiannually to discuss items of mutual concern.

(d) The RCIO arranges an annual meeting of a council of DOIMs whose membership is composed of all activity DOIMs and other C4/IT entities not yet under an IMA, but within the region.

(2) Management and oversight of C4/IT services. RCIOs have an operational focus for the delivery of services needed by regional customers and applies proven management principles, as well as C4/IT know-how, in the delivery of C4/IT services. RCIOs identify, foresee, find, and react when a business line or organizational direction change will affect the delivery of C4/IT. An RCIO is a key leader in any outsourcing of C4/IT services and approves all C4/IT outsourcing plans. A key concern for an RCIO is the delivery of the most commonly outsourced required services, including daily C4/IT operations, network/Local Area Network (LAN) operations, client /server operations, administrative services and help desk operations. An RCIO ensures that Army-approved enterprise solutions are applied within the region. An RCIO also ensures that established metrics are used to assess outsourced services and determine reasonable performance incentives and penalties.

#### **6-4. Director of information management**

a. An installation DOIM provides common C4/IT support and services to the installation or assigned geographical area through a fully integrated IT activity. An installation information manager is the DOIM, who must be fluent in local business processes and technology to help tenant organizations achieve mission goals. A DOIM gives IT services and aid to tactical units while in garrison and may aid Emergency Operations Centers in the continental United States (CONUS) and outside the Continental United States (OCONUS). Installations/activities need an array of IT services based on size, location, and a varied customer base. Activities and associated C4/IT assets are placed under the operational control of the installation commander or designated DOIM. DOIMs must apply reliable tactics to deliver high-quality C4/IT services to customers. A DOIM has several vital roles in the installation's capital planning and investment management processes. Most important, a DOIM validates new initiatives and ensures they comply with C4/IT guidance and Army enterprise architecture. A DOIM establishes and aids application of the most suitable knowledge management technology services and products for the agency.

b. In CONUS locations a DOIM is established under the garrison TDA and structured based on the IMA Standard Garrison Organization. In OCONUS locations, a DOIM is established under the signal battalion/support battalion authorization documents and structured based on command modifications to the standard garrison organization. A DOIM structures are based on key mission duties; the size/workload of the DOIM has major impact on the structure and staffing levels of the DOIM organization. A DOIM organization may be enlarged to meet customer's mission/business needs over the baseline. In CONUS locations a DOIM may work directly for the installation commander, the garrison/area support group/base support battalion commander, or the executive assistant (base operations) as determined by command structure. In OCONUS locations a DOIM works for the signal unit commander.

c. In-house military/civilian personnel, contractor services personnel in-house, outsourced services personnel, local nationals (OCONUS), or commercial utilities personnel can do DOIM functions (see AR 25-1, para 2-27, and the DOIM services listed in 6-4e). DOIM functions may include—

- (1) Installing telecommunication (voice and data) services.
- (2) Executing of IT policy and guidance as written by supervising organization.
- (3) Installing the help desk.
- (4) Installing trunked radio systems.
- (5) Information processing facilities.
- (6) Information assurance (see AR 25-2).
- (7) Printing and publications management.
- (8) Records management.
- (9) Visual Information.
- (10) Official mail and distribution management for the installation.
- (11) Information management support council.
- (12) Command automation reutilization programs.
- (13) Automation training.
- (14) Business process reengineering and functional process improvement analysis.
- (15) Data administration within the installation level of functions.
- (16) Common user video-teleconferencing facilities (VTFs).
- (17) IT metrics program.
- (18) Establishing Defense Message System (DMS) accounts.
- (19) Network management of installation/facility or designated common network(s) logical and physical structures and provides common network services and aid.
- (20) Establishing installation electronic mail accounts.
- (21) Installation content linked to the AKO portal.
- (22) Input for POM and unfunded request submissions for IT capital planning.
- (23) Preparing and administering SLAs.

- (24) IT architecture oversight.
- (25) Acquiring IT services.
- (26) Database administration/operational data services.
- (27) Validating IT acquisition compliance/compatibility with policy and guidance.
- (28) Oversight and NETOPS visibility for all Title 10 centralized servers located in their customer base centralized/installation-level processing services.
- (29) Installation enterprise licensing agreement program.
- (30) Generating military construction IT engineering designs and overseeing new construction.
- (31) Managing all common C4/IT data information structure.
- (32) Operation support for the Defense Red Switch Network.
- (33) Common C4/IT baseline services and above baseline services where mission dictates.
- (34) Defense messaging centers where still applicable.

d. The DOIM offers baseline and above baseline automation, communication systems support, information assurance, document management, and visual information support services to the installation customers. Army tenants reimburse for services over those in the common level support. For reimbursable services help, the DOIM starts a SLA with the customer. NETCOM works with the IMA to determine non-reimbursable common levels of support in DOIM support categories. NETCOM oversees how DOIMs establish reimbursable help (that is, what is listed in a SLA). Only reimbursable help is included in support agreements with installation customers. By providing such support, the DOIM—

(1) Recognizes the installation customer support base and considers unique needs and integration into the local architecture. The DOIM assesses supported communities to elect what services and advances customers believe would help their work.

(2) Provides an array of services to help customer IT needs. The potential services must be assessed and selected for each installation according to the following considerations:

- (a) The activity mission.
- (b) The size and characteristics of the customer population.
- (c) The hardware and software supported.
- (d) The makeup of the installation/activities staff.

(3) Selects services that best meet the needs of the customer group in compliance with the installation technical architecture.

(4) Educates customers in information assurance, system security, backup and recovery procedures, and provides technical advice to assist in taking actions necessary for needed controls.

(5) Identifies initial contact for problems relating to the use of standard Army systems.

(6) Explores new technologies for the utility and applicability needed to meet customer needs. In providing customers needed information on product research, evaluation, and application, the DOIM—

- (a) Appraises new technology to address current and future customer needs.
- (b) Conducts needed research and evaluation to set product standards and establish procedures.
- (c) Documents results of product evaluation and making these available to the supported community.
- (d) Tests equipment and/or applications to determine relevance to customer needs.
- (e) Determines how requests for nonstandard devices can be handled and integrated into the existing architecture.
- (f) Assists customers in defining and solving technical issues in a timely manner.
- (g) Gives, as needed, a virtual library at the computer desktop containing an inventory of installation standard operating procedures (SOPs) and other useful information.

(h) Initiates accreditation activities.

(7) Provides a common level of nonreimbursable help to Army tenants based on available resources. The C4/IT services list identifies the nonreimbursable service support programs the DOIM helps. The list can be found at the AKO site, KCC.

e. Additional DOIM services available for SLA negotiation include the following:

(1) *Migration planning.*

(a) Develops and carries out project plans and schedules for oversight and application of new or modified telecommunication, network, and automation services within framework of installation information infrastructure architecture (see related guidance in paras 1–9h, 1–10, and 2–3).

(b) Identifies and integrates advanced IM/IT technologies meant to satisfy new or modified customer services.

(c) Develops specifications for IM/IT solutions.

(d) Tests prototypes of hardware design as needed to validate design solution and minimize technical risk.

(e) Maintains a long-range outside plant plan and related drawings.

(f) Develops/modifies user software applications to support data utilized from or placed into an enterprise-wide database or various customer databases.

- (g) Conducts initial training for customers to use customized/integrated software/firmware products.
- (h) Performs system integration and re-engineering of legacy system interfaces.
- (i) Reviews and provides input as needed for construction project plans for IM/IT impact and compliance.
- (j) Designs, applies, and manages Internet/intranet Web sites.
- (k) Acquires/develops software for tenant users/installation staff.
- (2) *Acquiring materials and services.*
  - (a) Determines the proper purchase or lease process for IM/IT acquisitions and prepares packages for equipment and services.
  - (b) Processes and tracks IM/IT lease renewals in the same manner as for new leases.
  - (c) Assists customers in transfer of funds to proper Government accounts to cover costs of items/services procured/leased.
  - (d) Prepares requests for long-haul circuit support in response to customer requirements.
  - (e) Processes work orders for short-haul circuit installation, move, and disconnect services provided under separate Government contract.
  - (f) Records, processes, and executes relevant documents to acquire IM/IT equipment, components, or services.
  - (g) Purchases parts or external vendor repair services using existing Government service contracts or Government credit card as needed to complete work order repairs for supported IM/IT equipment.
  - (h) Receives, stores, and delivers to customers new IM/IT equipment, software, and parts and maintains necessary documents and inventory controls.
  - (i) Picks up excess serviceable Government-furnished equipment and process/warehouse items for internal reutilization or school donation.
  - (j) Turns in unserviceable equipment not being donated to schools directly to the Defense Reutilization Management Office (DRMO).
- (3) *Systems deployment.*
  - (a) Performs site surveys and validates customer needs before beginning new deployment, reconfiguration, or move.
  - (b) Oversees IM/IT work performed under separate Government contract to ensure proper installation. Verifies the statements of work.
  - (c) Performs turnkey deployment of hardware and software, including network and standalone computers, printers, and other peripheral devices, file servers, managed and unmanaged hubs, routers, and LAN and wide-area network (WAN) switches.
  - (d) Performs a serviceability technical inspection of all excess Government-owned IM/IT equipment that has been removed from active service and determines the reuse potential.
  - (e) Sets up, configures, checks out, and takes down IM/IT equipment supporting local area Government conferences per agreed upon SLA with the data owner/mission commander. This is a reimbursable service.
- (4) *Network and operational support.*
  - (a) Performs systems configuration, problem isolation and resolution, networking, terminal and other peripheral connection and interfaces, file and data archiving (backup), system booting and shutdown, user account administration, file system maintenance, basic operating systems programming for status and performance checks, software and data security, data transfer and conversion, and system improvements.
  - (b) Conducts daily oversight and upkeep of the LAN configuration and operational performance.
  - (c) Conducts daily planning, mapping, issuing, and documenting and database maintenance of IP addressing, and monitoring of the network firewalls and intrusion detection systems for security evaluations.
  - (d) Notifies security personnel of any incidents.
  - (e) Detection and resolution of degraded or failed LAN equipment problems.
  - (f) Performs daily operations and maintains performance of servers, including set up and maintain user LAN accounts, user groups, home directories, performance of e-mail accounts, servers, and routers.
  - (g) Performs daily operations and upkeep of Internet, intranet, and file transfer protocol servers and user accounts.
  - (h) Performs daily administrative support and checks of phone management system, including voice mail user account administration, system checks, and troubleshooting.
  - (i) Applies resources for hardware and software upgrades, replacements, and/or consolidations as directed by Government agencies.
  - (j) Develops and maintains Internet/intranet Web sites and pages.
  - (k) Coordinates, prioritizes, assigns, and conducts oversight of all technical response work orders.
  - (l) Performs installation of LAN/WAN and provides tenant unit LAN infrastructure support.
  - (m) Performs daily operation and upkeep of e-mail servers and user accounts in support of installation staff and tenant users.
  - (n) Performs remote and onsite technical troubleshooting, repair, and upgrade of existing standalone and network computers, software, and peripheral equipment.

*f.* There are many resources available to the DOIM to aid in starting and managing a help desk, such as the Help Desk Institute ([www.helpdeskinst.com](http://www.helpdeskinst.com)).

(1) Services provided by a help desk include—

- (a) IT problem resolution (available via phone, electronically, or walk-in service).
- (b) IT status information (for example, current status of network/e-mail/Internet availability and current information assurance guidance, availability of servers, and so on).
- (c) Hardware repair support.
- (d) Central store of technical advice, solutions, and frequently asked questions (FAQs).

(2) To assist in its operation, the use of a help desk software package is suggested. Many packages are available and provide such features as man-hour tracking per trouble/assistance call, automatic identification of user/equipment when a call is received at a help desk, identification of high failure rate items, vendor service calls tracking, and self-help information for users.

(3) A help desk can use automation tools to provide a more efficient operation. For example, a software package to automatically discover IT assets over the network is recommended. Such packages feed the results into the DOIM's Asset Management Program. Software packages that automatically push software installation/upgrades to the users' workstations based on settings established by the DOIM (such as time of day or bandwidth availability) are suggested. Tools are available that allow the help desk staff to give hands-on technical aid to the users without the help desk staff member leaving his/her office. Such software allows the technical staff to remotely control the user's workstation for troubleshooting.

(4) A help desk can be staffed permanently or on a rotating basis with trained technical personnel responding to trouble calls, giving instant first-call responses. If a nontechnical call center operation is established to receive and document trouble calls, a tiered technical referral system can be established to refer and solve incoming trouble calls on a timely basis. An efficient help desk is a key factor to the level of service provided by the DOIM.

#### **6-5. Information management office/officer concept and functions**

*a.* The term IMO is defined as the office/individual who reports to a commander/director/chief for coordination service. It includes management oversight, advice, planning, and funding coordination of all IM/IT requirements (business and mission) for their organization. The IMO assists the commander/director/chief in effectively managing the organization's IM/IT processes and resources that enable the organization's business and mission processes. General duties and functions of an IMO are to—

- (1) Monitor all common-user C4/IT baseline service delivery and support provided by the DOIM or signal battalion.
- (2) Identify, validate, and negotiate C4/IT above-baseline and mission-specific service delivery and support requirements with the DOIM or signal battalion, including usage sensitive services.
- (3) Implement and enforce IM/IT policies/procedures within their organization in coordination with their local DOIM or signal battalion and appropriate information assurance management personnel.
- (4) Identify funding to the commander/director/chief for C4/IT above-baseline and mission-specific service delivery and support requirements.
- (5) Act as the organization interface to the DOIM or signal battalion for troubleshooting of IT equipment, software, or process failures.
- (6) Maintain and update organizational data content and manage and monitor development of mission conventional and Web applications.

*b.* Specific tasks include—

- (1) Information assurance, to include—
  - (a) Certification and accreditation (nonclassified internet protocol (IP) router network (NIPRNET) and secure internet protocol router network (SIPRNET)), to include—
    - 1. Submitting request for accreditation to DOIM with copy to MACOM
    - 2. Complying with the DOD Information Technology Security Certification and Accreditation Process (DITSCAP).
  - (b) Certificates of authority for PKI, common access card, and others, to include—
    - 1. Providing organization input to DOIM.
    - 2. Ensuring compliance with DITSCAP.
    - 3. Implementing within Army mandated schedules.
  - (c) Content management, to include—
    - 1. Updating and maintaining content, classification, and protection of organization Web sites
    - 2. Developing and coordinating Web and FTP contents.
    - 3. Ensuring periodic Web and FTP site content review.
    - 4. Performing access management functions.
    - 5. Controlling access to LAN based on security requirements.
    - 6. Controlling access to specific applications.

7. Maintaining access lists in coordination with the DOIM.
  - (d) Web management, to include—
    1. Designing Web site content in accordance with Section 508 (29 USC 794d).
    2. Updating and maintaining content.
  - (e) Information assurance vulnerability assessment, to include—
    1. Monitoring information assurance vulnerability assessment compliance on the desktops.
    2. Ensuring information assurance vulnerability assessment on desktops.
  - (f) Disaster recovery (continuity of operations planning), to include—
    1. Regaining IT capabilities lost because of a natural or man caused disaster.
    2. Updating and maintaining content, coordination, and implementation.
  - (g) Computer network defense (CND) operations, to include intrusion detection and defense in depth to protect against hackers. The IMO task is to identify new requirements for CND capabilities.
    - (2) IT management, to include—
      - (a) C4/IT Resource management, to include—
        1. Providing C4/IT operational requirements to DOIMs.
        2. Developing C4/IT plans, requirements and strategic investment strategies in coordination with MACOM.
        3. Reimbursing for services above baseline.
      - (b) Requirements validation, to include—
        1. Identifying, validating, and consolidating requirements for submission to DOIM.
        2. Programming functional unique C4/IT requirements through MACOM.
        3. Programming all requirements above baseline services funding through MACOM.
      - (c) C4/IT performance management, to include—
        1. Assessing the effectiveness and efficiency of C4/IT support.
        2. Reporting effectiveness and efficiency of C4/IT support to MACOM.
      - (d) C4/IT metrics (as relates to installation status reports (ISRs)), to include—
        1. Measuring (or cause to have measured) those command/organizational items reportable through the C4/IT metrics program.
        2. Responding to reporting requirements of the supporting DOIM.
      - (e) C4/IT agreements, to include—
        1. Participating in the development of the SLAs as required by mission.
        2. Coordinating with MACOM on agreement and funding of above-baseline services.
        3. Developing enterprise architecture.
      - (f) Operational architecture, to include—
        1. Outlining and documenting missions, functions, business processes, and information requirements.
        2. Submitting C4/IT requirements to DOIM.
        3. Recommending to MACOM functional applications for their mission requirement.
      - (g) Systems architecture, to include—
        1. Recommending to MACOM applications for their mission requirement.
        2. Providing configuration layout and connectivity of C4/IT systems to DOIM.
      - (h) C4/IT architecture management, to include—
        1. Providing an integrated framework involving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals, information management goals and support to the soldier. Includes interoperability, scalability, and standardization.
        2. Acting as liaison to the DOIM on behalf of the customer population.
      - (i) Data management and interoperability, to include—
        1. Establishing the set of data standards, business rules, and data models governing the definition, production, storage, ownership, and replication of data used in the Army.
        2. Planning, creating, storing, and using data assets.
        3. Managing 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 DODAF.
        4. Facilitating internal, joint, and combined interoperability through the standardization and use of common data elements. Includes functional data proponent functions and data services.
        5. Enforcing data management and standards actions for the MACOM/functional.
      - (j) Acquisition and resource management of C4/IT and services for functional applications, to include the acquisition and resource management processes, begin when an organization's C4/IT needs are established in the appropriate capability document per AR 71-9. The process involves the planning, programming, budgeting and execution to satisfy the requirements established by the customer. The acquisition process also involves business process analysis, 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. Resource management will be tied to the C4/IT investment strategy, to include—

1. Submitting local C4/IT purchases requests through the DOIM.
2. Performing business process reengineering/ business case analysis for new or modified functional applications.
3. Recommending improvements to functional applications.
4. Acquiring and resourcing management of C4/IT and services for office automation, which includes desktop personal computers, laptop computers, notebook computers, hand-held computers, personal digital assistants, site licenses, software control and leasing of C4/IT. Peripheral devices include any device designed for use with PCs to facilitate data input, output, storage, transfer, or support function such as power, security or diagnostics. System software includes software required for PCs operations, for example, operating systems, and PC office automation applications, including word processing, spreadsheets, electronic mail, task management, graphics, and databases.
5. Coordinating office automation acquisition through DOIM.
6. Purchasing of office automation via Army enterprise contract vehicles.
7. Providing system specifications and functionality and obtain approval from the DOIM.
8. Obtaining a certificate of worthiness through the DOIM if office automation requires network connectivity/ Web-based application.
9. Inputting requirements to MACOM for input to PPBES for the life-cycle replacement of office automation equipment and software upgrades at the desktop level.
10. Capturing and reporting all C4/IT expenditures to DOIM (to include International Merchants Purchase Authorization Card card purchases).
11. Contracting support for short-haul communications/post, camp, station and base communications. Short-haul communications consist of local telephone systems and associated trunking to the nearest serving commercial central office. The IMO task is to identify requirements.
12. Managing C4/IT.
  - (k) Installation-level technical support and service to include testing equipment and evaluating software/hardware. The IMO task is to update and maintain content.
  - (l) Enterprise C4 systems, to include supporting software products that enable a desktop common operating environment and enforcing desktop configuration management, to include—
    1. Enforcing established policies.
    2. Providing mission unique application/data management.
    3. Supporting loaner equipment by providing temporary loaner equipment for repair, travel, and so on (for example, laptops, multimedia equipment, cell phones, pagers, and PDAs) and coordinating requirements through local DOIM.
  - (m) Synchronization of change; migration of modernization; change management, to include—
    1. Updating and maintaining site content.
    2. Submitting requests for worthiness to DOIM.
  - (n) Worthiness certification, to include—
    1. Issuing worthiness certificate before any new or enhanced system or capability is connected to the Army data information structure.
    2. Establishing policy and chairing the Army Enterprise Infostructure Management Steering Group as review council of negative results.
    3. Establishing worthiness criteria and submit systems, applications, or capabilities for testing.
    4. Providing C4/IT support services, which include—
      - a. Server management. The IMO task is to identify tenant servers for consolidation at Army processing centers and installations.
      - b. Functional processing center operations. The IMO task is to develop requirements and operate developed applications and systems.
      - c. Leasing C4/IT assets. The IMO provides for C4/IT mission accomplishment through equipment leasing. The IMO task is to develop cost analysis of leased versus purchase options.
      - d. Functional application development. The IMO publishes procedural guidance for mission/business based requirements analysis, functional applications and data requirements definition and specification. The IMO task is to develop requirements and operate developed applications and systems.
      - e. Systems administration (operate and maintain). The IMO provides procedural guidance for operation and management of servers, IA, and user accounts. Includes technical/operational aspects of server management. The IMO task is to develop requirements.
      - f. Content and access management. The IMO provides procedural guidance for management of the directories and associated authentication systems to enable authorized users to access the various systems and capabilities (to include

applications) within the data information structure. The IMO performs user “add, change, delete” operations for assigned data information structure capabilities.

(o) Help desk services, to include providing help desk and product support for COTS hardware and software, network support, repair service, including those dedicated to single applications and providing broad assistance for networks and desktop services (includes voice over internet protocol). Tasks include—

1. Providing first-line of assistance for the local user on hardware and software.
2. Establishing service level agreements with DOIM, provide funding for services above the established service level.
3. Identifying a primary organizational point of contact for problem identification and resolution.
4. Providing customer support (tier 1, tier 2, and tier 3 help-desk support). The IMO task is to provide requests for service to DOIM.
5. Providing database administration/operational data services. The IMO publishes procedural guidance for data ownership, access control, data management, data manipulation. The IMO task is to manage and administer organizational data.

(p) C4/IT hardware utilization/reutilization/disposal. The IMO publishes procedural guidance on reutilization and disposal of hardware, to include—

1. Maintaining property accountability for assigned equipment.
2. Identifying potential excess equipment.
3. Following procedures to determine excess equipment, removal from property books, opportunities for reutilization and/or disposal.
4. Accounting for property. For organizational control for hardware and software, the IMO publishes procedural guidance for proper accountability controls, including hand receipts, property books, and so on. The IMO task is to maintain property accountability records under current Army guidelines.

(3) Telecommunications and base services, to include overall management of an installation/facility or assigned area’s networks, to include those supporting DOD, DA, and MACOM initiatives. 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. This includes contingency planning, disaster recovery for managed LANs, and providing technical assistance to functional systems administrators. Network management also involves the preparation, submission, and tracking of procurement actions for network-related items. Common network services (for example, network infrastructure such as routers, hubs, switches, and so on). The IMO task is to perform information assurance security officers (IASO) tasks, if assigned.

(4) Long-haul and deployable communications, to include long-haul communications (review, approval, and funding of all requests for long-haul services). The IMO task is to request long-haul services from DOIM.

(5) Official mail management, to include providing official mail support. IMO tasks include—

(a) Designating a POC for official mail management to assist the installation official mail managers in carrying out official mail duties for their organization.

(b) Picking up official mail/distribution from the supporting official mail distribution center and delivering outgoing mail/distribution to the supporting official mail distribution center.

(c) Making distribution within contiguous organizational facilities.

(d) Coordinating official mail requirements with the installation OMM.

(e) Obligating official mail funds for activities within their organization.

(f) Ensuring that all large mailings are coordinated with the installation OMM.

(g) Ensuring receipt of non-reimbursable support upon the transfer to the Army of budget authority for the activity’s official mail program.

(h) Preparing semiannual official mail report, as required.

(i) Managing publications and forms.

(6) Publications management, to include provide publications and printing management, to include—

(a) Publications management, to include—

1. Developing, publishing, and implementing command/organizational policy and procedures.
2. Submitting nominees for annual Secretary of the Army Awards for Publications Improvements.
3. Providing assistance on development of new command/organizational functional pubs/changes to existing pubs.
4. Publishing/maintaining index of command/ organizational publications.
5. Editing, conducting 18-month reviews, authenticating/dating, and maintaining official file of command/organizational publications.
6. Reviewing and approving DA Forms 12–R (Request for Establishment of a Publications Account) new command/organizational accounts.
7. Publishing and distributing authenticated command/organizational publications.

8. Pursuing electronic digitization of command/organizational publications.
  9. Performing special surveys/studies/reports as required.
  10. Advising and assisting supporting installation-printing managers.
  11. Providing staff assistance visits as required.
  12. Advising and assisting command/organizational staff elements concerning printing policies and procedures.
  13. Participating in technology reviews.
  14. Conducting periodic command/organizational program assessment.
  15. Providing command/organizational reports as required.
- (b) Forms management, to include—
1. Developing organization/command-level forms procedures.
  2. Overseeing organization/command-level forms program and providing advice and assistance.
  3. Maintaining official file of current organization/command-level forms.
  4. Editing, reviewing, and approving organization/command-level forms.
  5. Maintaining master file of hardcopy/electronic organization/command-level forms.
  6. Publishing organization/command forms index and providing requirements to local DOIM and program funds to support forms needs, if provided by DOIM.
  7. For AKO and IMO, executing procedural guidance to ensure all personnel have access to AKO and registering on and using AKO.

## **Chapter 7**

### **Information Technology Management and User Principles and Procedures**

#### **7-1. Information transmission economy and systems discipline**

- a. Economy and discipline procedures include, at minimum, the following requirements:
- (1) Management oversight and controls must be set up at all echelons.
  - (2) Dedicated information services and facilities are reviewed at least every two years by the appropriate DOIM. The review inspects 800 numbers (for purpose and traffic volume), calling cards (originating and terminating calls), and cellular phone and pagers (originating and terminating calls). The review includes the examination of “back doors” and short- and long-haul circuits that do not go through the front door.
  - (3) Management and oversight of long distance use of telecommunications and computing systems, including the Defense Information Systems Network and cellular phones.
- b. Essential IT officials have the following functions:
- (1) Telephone control officers review and validate bills for toll-free (1-800, 1-888, and so on) service, pager service, cellular phone service, collect calls, and calling card usage; long distance, DSN, Federal Telecommunications System (FTS), and international direct distance dialing; commercial calls; and local-leased commercial service.
  - (2) Web site managers and maintainers install access control mechanisms for Web sites as required and protecting against the posting of sensitive information (see AR 25-1, para 6-4n for information on implementing access control mechanisms and prohibitions on posting specific information on public Web sites).
  - (3) Web site reviewers must conform to Army, DOD, and Federal standards on contact to ensure that sensitive personal or unit information has been removed from publicly accessible Web sites. For a list of the documents, refer to AR 25-1, appendix C-4e. See also chapter 8 of this document.
- c. Privacy and security provisions include the following:
- (1) The Privacy Act of 1974 (5 USC 552a) and the Freedom of Information Act (FOIA) govern the privacy requirements. Under the Privacy Act, an agency contracting on its behalf for the design, development, or operation of a system of records on individuals to accomplish an agency function applies the requirements of the Privacy Act to the contractor and its employees working on the contract. All sensitive data are protected from disclosure and from unauthorized modification or destruction.
  - (2) Users of telecommunications and computing systems, including intranet access and the use of e-mail, are notified that their use of this equipment is subject to monitoring and recording. Per DODD 5240.1, all systems contain the DOD banner telling the user there is no right to privacy on the systems. Use of Government telecommunications and computing systems is made with the agreement that communications are not secure unless protected by authorized encryption devices and properly labeled for level of clearance authorized. System managers may use monitoring tools to find improper use of IT assets IAW appropriate monitoring techniques located in AR 380-53.
  - (3) DOD has serious limits on the amount of information it is able to provide to our forces. Due to this, controls on bandwidth are vital in the near term. The sending of large nonoperational documents and briefings over networks may have serious operational impacts (see AR 25-1, para 6-4m). The following actions are recommended:

(a) Limit the use of graphics in e-mail attachments. Avoid rich context pictures needing large amounts of memory. Omit logos and seals on all but the title slide of a briefing.

(b) Limit official subscriptions to newsgroups to those supporting the organization's missions and functions. Reduce or eliminate individual personal subscriptions to newsgroups. Eliminate personal Web services needing constant bandwidth.

(c) Avoid using the "Reply All" e-mail feature when responding to an individual.

(d) When using the "Reply" and "Reply to All" e-mail feature, avoid quoted replies/in-line replies (that is, complete e-mail strings).

(e) Rarely use the "Return Receipt" e-mail feature. Use only on official e-mail when receipt must be verified (for example, where the e-mail has a direct bearing on the mission).

d. Emergency needs are generated by natural disasters, civil disorder, exercise situations, mobilization, or war. All installation organizations must plan for the use of resources during these situations. One of the keys to effective mobilization is the ability to offer command and control for the influx of troops into active duty. This may require a surge in information systems capability (see AR 25-2, para 4-5h, and AR 500-3, DODD 3020.26, and DODI 3020.37).

e. See AR 25-1, paragraph 6-1, for policy on the use of agreements. There are several types of agreements under which support is provided, including—

(1) Support agreements (DD Form 1144 (Support Agreement)), memoranda of agreement, and memoranda of understanding.

(2) SLA.

(3) Interservice agreements.

(4) Support to non-DOD Federal agencies.

(5) Customer service guide(s).

## **7-2. Official and authorized uses of telecommunications and computing systems**

a. Government telecommunications and computing systems resources are managed just as any resource. Commanders and supervisors appropriately manage telecommunication and computing usage in their jurisdictions. Installation/activity commanders provide for the development and enforcement of controls that promote effective telecommunications and computing systems management practices within the installation to ensure the best use of official telecommunications and computing systems.

b. Installation/activity commanders may approve emergency calls or system use (see AR 25-1, para 6-1 for the policy on official and authorized use of Government telecommunications and computing systems).

c. Persons known to have used phones in a way not authorized by AR 25-1, paragraph 6-1, or by the local commander, must pay the toll rates. The following procedures apply before recovering charges:

(1) Give a written notice of the proposed action. The notice includes a copy of that part of the investigation and supporting evidence on which the proposed action is based.

(2) Give the person a realistic opportunity to reply in writing and to submit relevant rebuttal material.

(3) Review and assess the reply before deciding what action to take.

d. The DOIM works with telecommunications providers in regards to calls in doubt after procedures have been completed and/or other efforts have been tried to resolve the calls.

e. Use of official telecommunications and computing systems service in personal quarters is covered in detail in AR 25-1, paragraph 6-4g.

## **7-3. Information technology support for official spouse volunteers and statutory volunteers**

This section identifies the options for issuing ".mil" accounts and password authorization to military spouses and statutory volunteers for the purpose of conducting military family support missions.

a. The spouse or statutory volunteer may obtain an AKO account under the military member's sponsorship. Once the family member receives access authorization, he/she may establish e-mail service for personal e-mail messages and establish a private Web site on the Knowledge Network for sharing documents or other files. The spouse or statutory volunteer may access an AKO account through his/her personal computer, but an AKO account alone would not authorize him/her to use a Government computer in quarters or be authorized access privileges on the Army network (see chap 3 for complete information on this type of account).

b. The spouse or statutory volunteer may obtain IT support as an official volunteer. In this case he/she would be permitted to access and use a Government-furnished computer (unclassified only) in quarters. Such use, however, would be limited to official volunteer duties; the spouse or statutory volunteer may not use a Government computer for personal activities.

(1) A spouse or statutory volunteer with "official volunteer status," pursuant to 10 USC 1588(f), may be authorized use of Government facilities (such as office or desk space), equipment, supplies, computers, and telephones, needed to perform assigned duties. The statute authorizes the use of appropriated or nonappropriated funds to pay for the

equipment and related charges. In addition, installation commanders have the authority to install telephone lines and other necessary telecommunication equipment and pay for the installation charges for the equipment when the official volunteer works out of the home. However, no Government services or equipment may be provided for a spouse or statutory volunteer who offers "gratuitous services" with no statutory volunteer status.

(2) The provisions for "statutory volunteers" are found in AR 608-1, paragraph 5-10, and DODI 1100.21, appendix E.3.7. The Army Community Service (ACS) director at each installation can explain the standards for volunteer service to family members and assist the family member in completing any requirements. The standards include, as a minimum, a volunteer agreement and a position description.

(3) The "statutory volunteer" status recognizes the family member's requirement to obtain Government services and support. Under this status, the ACS information management officer would advise on proper workstation and IT usage, help-desk information, and reporting/handling of computer incidents. The site security manager will give the spouse the same instructions provided to other Army computer users regarding information security (handling, storing, and transmittal of Government information) and personal security.

(4) AR 25-1, paragraph 6-4g, addresses telecommunications in private quarters for key personnel. When a military member is authorized residential network communications for official purposes, the Government will not install a second line in the same residence for the statutory volunteer.

(5) DOIMs should work closely with the ACS Directors to ensure that military spouses that are designated as statutory volunteers receive the support to which they are authorized under AR 608-1.

#### **7-4. Support for health, morale, and welfare/morale, welfare, and recreation telecommunications**

a. See AR 25-1, paragraph 6-1d for policy on the limits in using DSN for health, morale, and welfare (HMW) communications. HMW communications (voice/Internet protocol, video teleconference) will be primarily made over the HMW/morale, welfare, recreation (MWR) provided nonappropriated funded communications services.

b. DOD members assigned to a CONUS installation, MACOM, or other organization and deployed OCONUS may place HMW calls through a CONUS installation phone switch. Typical local procedures will have the following conditions:

- (1) Calls go only to a family member.
- (2) Deployed DOD members may ask family members to report to their unit at prearranged times to get their phone calls.
- (3) Emergency calls may exceed specified limits (per CJCSI 6215.01B) when approved by the commander.
- (4) The Government do not incur costs associated with the extension/off-netting of HMW calls.
- (5) If off-netting of HMW calls would incur a commercial toll charge to the installation, calls are extended only via collect calls (if the called party agrees to accept the charges), prepaid calling card, or commercial long-distance carrier calling card.
- (6) Calls are made only at routine priority.
- (7) DSN switchboard locations have been reduced because of base closures and force reductions. Another system for morale calls is the Automated Directory Assistance System (ADAS), installed on several Army CONUS installations. Calls made by deployed soldiers/authorized personnel to these ADAS sites will be connected to an automated call attendant and its voice-recognition morale call subsystem. Soldiers/authorized personnel can access the ADAS by DSN phone lines. The Government cannot pay toll charges for extending personal calls. The DSN directory ([http://www.disa.mil/gs/dsn/dsn\\_directory.html](http://www.disa.mil/gs/dsn/dsn_directory.html)) is a third source for possible off-netting of approved morale calls.

c. There are three methods of HMW e-mail. The first is through Family Readiness Group accounts established for each deployed unit and its rear detachment. The second is through a commercial Internet e-mail account that the DOD member establishes for personal use at no cost to the Government. The third is unclassified official e-mail accounts.

(1) DOD members and their family may use Family Readiness Group accounts created by their command to send personal e-mail messages. The subject line should identify the receiving party. Units may establish Family Readiness Group e-mail distribution and access procedures within their units. No e-mail is considered private; however, units are encouraged to ensure the Army member is allowed as much privacy as possible.

(2) Army members are allowed to use Government systems to access private e-mail accounts located on the Internet. This access is authorized as long as no private software is loaded onto the Government system and the Government incurs no additional cost. Access to Government computer systems for personal e-mail use will usually be after duty hours or at the discretion of the unit commander.

(3) Army members may use assigned e-mail accounts to send short messages to relatives, friends, and fellow employees. A rule of thumb is one page or less of text with no attachments.

#### **7-5. Information access for the disabled**

a. *General.* Section 508 requires all Federal agencies acquiring electronic and information technology (EIT) to ensure that Federal employees and members of the public with disabilities have access to and use of information and data that is comparable to the access and use by individuals who do not have disabilities. Unless an exception applies, all Federal/DOD acquisitions of EIT must meet the applicable accessibility technical standards and/or the functional

performance criteria (36 Code of Federal Regulations Part 1194 (36 CFR1194)) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board) (see AR 25-1, para 6-1g).

*b. EIT.* EIT has the same meaning as information technology except EIT also includes any equipment or interconnected system or subsystems of equipment that is used in the creation, conversion, or duplication of data or information. The term EIT includes, but is not limited to, telecommunication products, (such as telephones), information kiosks and transaction machines, worldwide Web sites, multimedia, and office equipment (such as copiers and fax machines). This applies to all contracts for EIT supplies and services awarded on or after 25 June 2001. Except for indefinite-delivery contracts, it is applicable to all delivery orders or task orders for EIT that are issued on or after 25 June 2001. This is applicable to all procurement actions for EIT processed by contracting offices, regardless of the customer being supported.

*c. Computer/Electronic Accommodations Program (CAP).* CAP is a centrally funded DOD program that provides assistive technology as a form of reasonable accommodation to enable a qualified person with a disability to perform the essential functions of the job. CAP's scope is to provide the assistive technology used to modify the computer and telecommunication environment for Federal employees with disabilities. Contact CAP at (703) 681-8813 for a consultation or to order equipment (see the CAP Web site at [www.tricare.osd.mil/cap](http://www.tricare.osd.mil/cap)).

*d. Accessibility standards.* Requiring officials must be knowledgeable of Section 508 accessibility standards and, unless an exception applies, ensure applicable standard(s) are included in all acquisition packages for EIT. Further, requiring officials must address Section 508 requirements throughout the acquisition process (market research, acquisition planning, and so on). Contracting officers should verify that, unless an exception applies and is appropriately documented, the Section 508 compliance specification is included in the technical requirements document (statement of work, statement of objectives, and so on).

*e. Exceptions.* Use of any of the exceptions stated below requires the requiring officials to provide written justification to the contracting officer with supporting rationale.

(1) *NSS.* This is defined in 40 USC Section 11103.

(2) *Undue burden on the agency.* The Department of Justice defines undue burden as "a significant difficulty or expense" consistent with language used in the Americans with Disabilities Act Section 508 also provides that if a Federal agency determines that compliance with the standards in procurements imposes an undue burden, any documentation by the agency supporting procurement shall explain why compliance creates an undue burden. In determining whether compliance with all or part of the applicable accessibility standards in 36 CFR 1194 would be an undue burden, the requiring officials must consider the difficulty or expense of compliance, and all agency resources available to its program or component for which the supply or service is being acquired. Note that undue burden cannot be established simply by demonstrating that, as between products that could meet the agency's need, the cost for a product that meets the accessibility standards is higher than that for a product that does not. Requiring officials should be aware that when there is an undue burden, the statute requires that an agency provide the person with a disability the information and data by an alternative means of access that allows the individual to use the information and data.

(3) *Contractor procured EIT that is incidental to the contract.* Section 508 does not apply to a contractor's internal workplace. EIT that is not used or accessed by Federal employees or members of the public is not subject to the 508 standards. Contractor employees in their professional capacity are not considered to be members of the public for purposes of Section 508.

(4) *Areas frequented only by service personnel.* Section 508 does not apply to EIT that is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment ("back office" equipment).

(5) *Micropurchases.* Purchases of \$2,500 and under are no longer exempted from Section 508. Contracting officers and purchase cardholders are to use the same accessibility standards in purchasing micro-purchases as any other EIT purchases.

(6) *EIT intended for use by able-bodied uniformed military personnel only.*

*f. Required documentation for Section 508 compliance.*

(1) Local requirement officials must complete a document showing the research and compliance or waiver to Section 508 standards and guidelines.

(2) For NSS exceptions, the document is completed and requiring officials must give it to the contracting officer with the procurement request package before going on with the purchase.

(3) Agencies are required by statute to document the basis for an undue burden. The requiring official must document the basis for an undue burden decision. The document should be coordinated through the CIO and legal.

(4) Contractor procured EIT that is incidental to the contract, and in spaces frequented only by service personnel. Document determination will be approved by the local requirements officials and provided to the contracting officer with the procurement request package before the start of procurement action.

(5) When acquiring commercial items, an agency must comply with accessibility standards that can be met with supplies or services available in the commercial marketplace in time to meet the agency's delivery requirements.

(6) When acquiring commercial items, an undue burden determination is not needed to address individual standards

unable to be met with supplies or services available in the commercial marketplace in time to meet the agency delivery requirements.

(7) The local requiring official must document in writing the non-availability, including a description of market research performed and which standards cannot be met, and provide documentation to the contracting officer for inclusion in the contract file.

*g. Section 508 noncompliance.*

(1) Failure to comply with Section 508 could result in agency administrative complaints and civil action against Army agencies. Administrative complaints should be filed with procurement offices and the Army's Equal Employment Opportunity office.

(2) Extensive information regarding Section 508, including an overview of the law and regulations, training, FAQs, and so on, is provided at [www.section508.gov](http://www.section508.gov). In addition, the CIO/G-6, SAIS-GKP is available to give technical and NSS assistance. E-mail SAIS-GKP at [armycio@hqda-dms.army.mil](mailto:armycio@hqda-dms.army.mil).

(3) All IT personnel and procurement offices (military, civilian, and contractors) should complete the online Web accessibility course offered by the GSA. The course, "Acquiring Technology: What Every Federal Employee Needs to Know," gives an overview of the roles required in acquisition planning and preparation as it relates to Section 508 of the Rehabilitation Act and explains how to identify needs and prepare a solicitation using market research.

## **7-6. Information technology support for telework/telecommuting**

*a.* Telework is defined as an arrangement in which a civilian employee and/or member of the Army Forces performs assigned official duties at an alternative worksite on either a regular and recurring or ad hoc basis (not including while on official travel). This alternative site is a place away from the traditional worksite that has been approved for performance of official duties. An alternate worksite may be an employee's home or a telecommuting center established for use by teleworkers. See additional information on the DOD telework program in DODD 1035.1 and on the DOD telework Web site, [www.cpmos.osd.mil/fas/telework/dod\\_telework\\_policy.htm](http://www.cpmos.osd.mil/fas/telework/dod_telework_policy.htm).

*b.* AR 25-1, paragraph 6-1*o* authorizes the use of Government-furnished IT equipment and supplies for use in an employee's home for regular and recurring telework arrangements. All telework agreements will address mandatory information assurance requirements and be approved by the designated approval authority prior to implementation.

(1) Local procedures address issues such as Federal/local laws, workplace requirements (safety, hardware/software issues, security/accreditation, and so on), and union requirements. The local command decides if telework/telecommuting is a suitable option and if the infrastructure is able to support a mobile force.

(2) CAP provides assistive technology as a form of reasonable accommodation (see para 7-5*d* for more information).

(3) Also, organizations may contact the Army POC via e-mail at [armycio@hqda-dms.army.mil](mailto:armycio@hqda-dms.army.mil).

*c.* Local installations and agencies decide how and when face-to-face conversations or meetings are needed. The resources of hardware, software, and training are local decisions based on mission and funding available.

*d.* Issues that need to be addressed are suitability of jobs for telework/telecommuting, business processes to be changed to support telework/telecommuting, arrangements of admission of technicians and others into a telecommuter's home, productivity measurements of remote workers, and general supervisory concerns. Some helpful URLs are—

(1) [www.telecommute.org](http://www.telecommute.org), to learn the design and implementation of teleworking programs and the development of the U.S. telework sector.

(2) [www.telework.gov](http://www.telework.gov), to get information on using telework in the federal Government. It contains telework policies of other federal Government agencies.

(3) [www.teleworkconsortium.org](http://www.teleworkconsortium.org), for information on building the business case for telework using advanced communications and collaboration technologies.

*e.* There are various types of telework categories and definitions (see [www.telework.gov](http://www.telework.gov) for more information).

*f.* Use of Government IT resources (such as computers, facsimile machines, modems, and so on) for telework is authorized under certain conditions, which can vary from one installation or activity to another. Government-furnished computer equipment, software, and communications, with appropriate information assurance safeguards, are required for any regular and recurring telework arrangement. A telework agreement that outlines the terms and conditions (including IT support) of the arrangement is required before the employee commences regular/recurring telework (see app B for more information). According to the AR 25-1, the designated approval authority and an O-6 or GS-15 must approve the use of employee-owned computers. The employee-owned computer must meet information assurance requirements. However, remote access software must not be loaded onto employee-owned computers for official purposes. Use of resources to fund limited operating costs associated with communications (for example, digital subscriber line, cable modems, and analog dial-up lines) within an employee's residence as an alternative worksite may be determined by the local commander. (Telework resources are not intended for individuals who occasionally check e-mail from their residences.)

## **7-7. Assuring information quality**

*a. Regulatory guidance.* Federal agencies subject to the Paperwork Reduction Act (44 USC Chapter 35) and the

Health Information Portability and Accountability Act are required to issue information quality guidelines for information the agencies distribute; establish administrative mechanisms that allow affected persons to seek and obtain correction of information distributed by the agencies that does not comply with OMB, DOD, or agency guidelines; and annually report the number and nature of complaints received by the agencies and how the complaints were resolved. The requirements set by AR 25-1, paragraph 1-12, focus on the neutrality, usefulness, and integrity of information used and distributed by Federal agencies and ensuring affected members of the public have an administrative mechanism to seek and obtain correction of information that does not meet quality standards. This pamphlet addresses the Department of the Army standards of quality, predistribution review of information, and administrative procedures for processing claims.

*b. General.* Information products are distributed in a variety of media and cover the spectrum of programs and functions. Therefore, each organization must ensure the standards, review procedures, and administrative mechanisms adopted not only address the objective of this program, but incorporate requirements by other specific programs (such as the National Environmental Policy Act and Government Performance and Results Act of 1993).

*c. Exempt information products.* Information products that are not distributed to the public are exempt from requirements of information quality guidelines.

*d. Predissemination reviews.* The intent of the Quality of Information (QI) Program is not to avoid or supersede present procedures and business practices. However, activities must review existing quality assurance or control procedures, staffing practices and other administrative measures to ensure adherence to quality standards and include adequate documentation of predistribution reviews.

(1) Agencies must allow “adequate” time for review, consistent with the standards required for the type of information being distributed.

(2) Informal and formal reviews ensure products meet a minimum quality level. To ensure accuracy, objectivity, and integrity, products may undergo technical, supervisory, editorial, and legal review based on the nature of the product.

(3) Reviews are done by several people with diverse areas of expertise appropriate for the type of information (independent subject matter expert, statistical expert, IT, visual information specialist, and accessibility specialist). Treat information quality as an integral part to every step in the development of information, including creation, collection, maintenance, and dissemination. When appropriate, conduct reviews through the various stages of data development.

*e. Claims processing procedures.* Figure 7-1 and the guidelines below should be reviewed for timelines, functions, and requirements associated with processing claims. Before processing a claim, the supervising activity for questioned information will—

(1) Ensure claims meet published program needs and contact the requester within 5 working days if the claim is incomplete or if the information disputed does not fall within the purview of the program.

(2) Decide whether the requester has suitably supported the claim that the information is not accurate, clear, complete, or unbiased, and that the requester is an affected person.

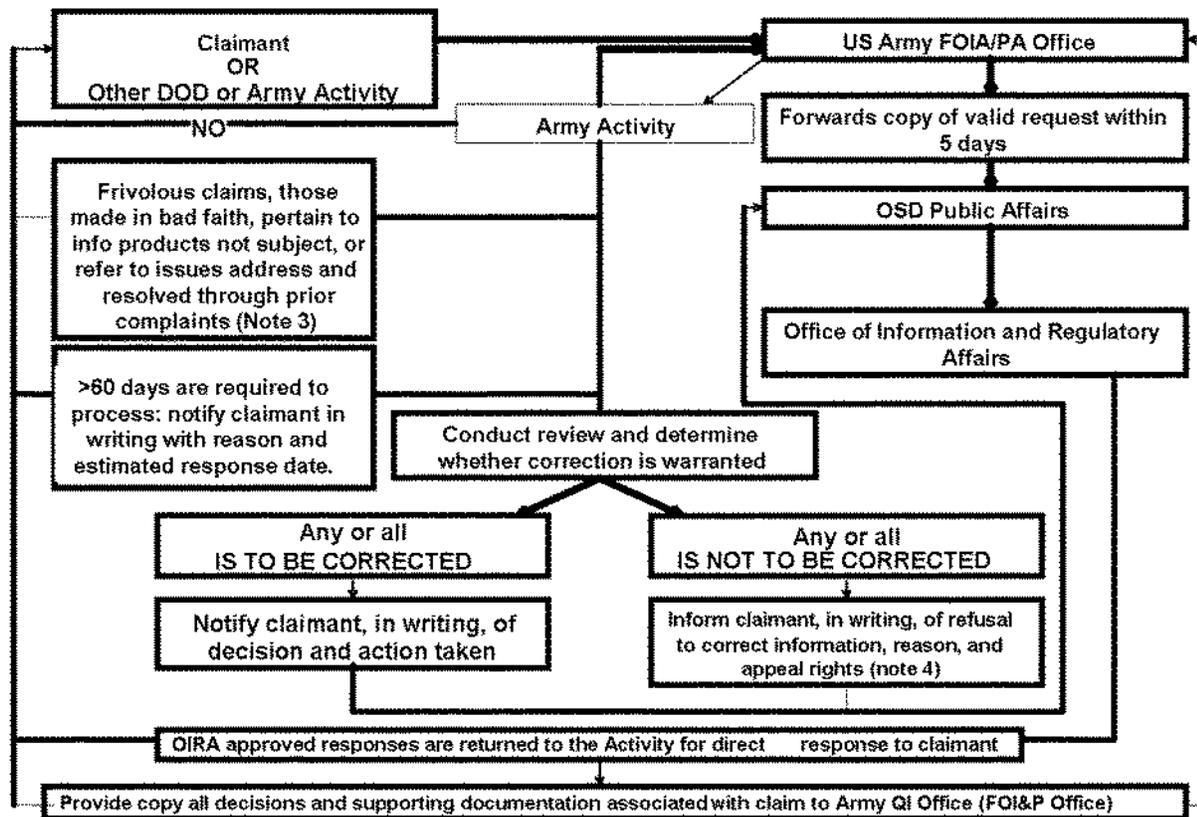


Figure 7-1. Claim processing matrix

(3) Allow the requester to support the claim with more information or justification. If the requester then submits a completed QI claim, processing of the request will immediately resume.

f. *Role of supervising activity.* The role of the responsible activity is to thoroughly review the information being challenged, the processes used to create and distribute the information, the conformity of the information, and its compliance with processes outlined in OMB, DOD, and Army QI guidelines. Limit the review of information to the aspect or aspects of the information that clearly bears on any determination to correct the information. These guidelines are found at [www.whitehouse.gov/omb/fedreg](http://www.whitehouse.gov/omb/fedreg), [www.apd.army.mil](http://www.apd.army.mil), and the DA Freedom of Information and Privacy Act (FOIA&PA) Division, [www.rmda.belvoir.army.mil](http://www.rmda.belvoir.army.mil).

g. *Claim processing expediency.* All efforts must be made to process the claim in 60 working days. If a claim needs more than 60 working days to resolve, the requester is notified in writing (by the activity) that more time is needed, the reason why, and a likely response date.

h. *Frivolous claims.* Frivolous claims, those made in bad faith, pertaining to information products not subject to QI guidelines, or refer to issues address and resolved through prior complaints are dismissed.

i. *Post review.* After the review is finished, the supervising activity decides whether a correction is needed and, if so, what corrective action will occur. Supervising activities are required to undertake only the degree of correction they deem appropriate for the nature and timeliness of information involved. The content or status of information is not required to be changed, or in any way altered simply because a request is made. If any of the information is to be corrected, notify the requester, in writing, of the decision and either an issued correction, or of the intent to correct and proposed related action. If there is disagreement with some or the entire claim, inform the requester in writing of the refusal to correct the information, the reason for refusal and the appeal procedures and requirements outlined below.

(1) If the requester disagrees with the activity's decision, an appeal may be submitted in writing within 30 working days of the notification of the determination.

(2) The appeal packet consists of: a written justification supporting the case for appeal, including the reason why the agency response is inadequate, a copy of the information originally submitted to support the claim, and a copy of the Army supervising activity's initial response.

(3) The requester must submit the appeal packets through the DA FOIA and Public Affairs Division.

(4) The QI designee within the FOIA and Public Affairs Division routes all appeals through the supervising activity that provided the original determination prior to submission to the Army appellate authority within 3 working days of receipt. That organization has the opportunity to reconsider the initial decision, address the justification submitted with the appeal packet, and contribute more documentation required for the Appellate to make a decision. The supervising activity forwards the appeal packet to the appellate within 7 working days of receipt.

(5) Appeal decisions are made within 30 working days of receipt. If an appeal needs more than 30 working days, the requester is notified in writing by the appellate office that more time is needed, the reason why, and an estimated response date.

(6) Submit a copy of the draft response to claims or appeals to the Administrator of the Office of Information and Regulatory Affairs at least 7 working days before its intended issuance. The address is: Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17<sup>th</sup> Street NW, New Executive Office Building, Room 10201, Washington, DC 20503. Army supervising activities do not issue a response until the Office of Regulatory Affairs has concluded consultation with the agency.

(7) Responding activities, to include the appellate, provide a copy of all decisions and supporting documentation associated with claims to the Army QI designee for recordkeeping purposes and inclusion in the annual report submitted to the Assistant Secretary of Defense for Public Affairs.

(8) Forward correspondence via mail: FOIA and Public Affairs Division, Quality of Information Program, 7701 Telegraph Road, Suite 144, Alexandria, VA 22315-3905, or fax Commercial: (703) 428-6522, DSN: 328-6522.

*j. Recordkeeping requirements.* Documentation is paramount and likely to play a key role in processing claims and appeals. It is vital that activities create and maintain documentary evidence, which supports pre-distribution reviews and decisions made in processing claims. Retention schedules for records in support of this program are in the development stage. Until then, keep the documents that support the predistribution review and processing of claims (decisions made during the processing of claims, coordination, and actions taken as a result of processing claims) in the current files area until retention schedules are published.

## **7-8. Training**

### *a. User requirements.*

(1) Training is a key service of the DOIM. In establishing a training program, the DOIM considers factors that impact the types of training offered to the users supported, such as— the DOIM's published list of supported products; AKO core services; IT management training; regulatory requirements such as computer security training; and IT support personnel training requirements (for example, IMOs and IASOs), as well as special training for requirements of a single unit or segment of the DOIM's customer base.

(2) Training consists of a standard COTS office suite package (word processing spreadsheet, presentation, database management, and so on), the DMS e-mail package in use, and operating systems. DOIMs also provide training in IT management, regulatory requirements such as computer security, IT support and personnel training requirements (for example, IMOs and IASOs) as well as special training for requirements of a single unit or segment of the DOIM's customer base.

(3) The DOIM determines and publishes a standard list of items to be supported. The software applications included in the list serves as one component of the DOIM's training program. Typically, these products consist of a standard COTS office suite package (word processing, spreadsheet, presentation, database management, and so on), the DMS e-mail package in use, operating systems, as well as other applications such as Web authoring tools. Training for supported software may be found at the Army's e-Learning portal, [www.us.army.mil](http://www.us.army.mil)—select "My Education" under "Self-Service," click on "Army e-Learning" at the top of the page.

(4) Regulatory required training may be included in the DOIM's training program. User certification training is needed to ensure that personnel in charge of managing Government computing resources or access Government computer resources are aware of proper operational and security-related risk and procedures. DODD 8500.1 requires heads of DOD components to establish and maintain an IA training and awareness program for all DOD military, civilian, and contractor personnel needing access to information systems. Information on IA training can be found in AR 25-2, paragraph 4-3. Successful completion of user certification training includes a thorough exam and the signing of a statement to indicate users understand the training and will follow the procedures presented.

(5) The unit IMO, IASO, and local IT management specialists need technical training above that of the standard user to carry out their functions. Much of this training is tailored to the local environment, SLAs, and the DOIM's established operating procedures. Regular follow-on training for this staff ensures that they are kept abreast of newly fielded products and systems.

### *b. Sustaining.*

(1) The primary means by which IT training is to be accomplished is distance learning. For more information, see the Army e-Learning portal.

(2) The DOIM training program coordinator publishes information about the training program on the installation's local intranet. This includes: a description of each training course offered, along with its prerequisites; a schedule of

available and upcoming courses; instructions on registering for a course; a way for the student to initiate registration electronically; and a point of contact, in case the student needs more information or assistance.

*c. New technology.*

(1) The array of IT products and services provided to the DOIM's customer base is ever changing. Continual growth is expected in the automation of business processes and enhancements in technology. DOIMs should plan for new technology training for the DOIM staff, the unit's IT personnel, and the user. Many vendors include some level of training, at little or no charge, when they are onsite to install their system/program. Many training companies offer a way for the DOIM to have representatives come and conduct onsite technical training at less cost than the typical off-site training.

(2) The Army provides an array of programs for personnel to get technical training. In addition to the Army's e-learning portal, the ITM CP-34 gives funding for education and training through the Army Civilian Training, Education, and Development System.

(3) When new technology is presented as part of a new system or service to be given to the user, the DOIM plans for user training as part of the system's fielding plan. The user's training is reinforced with a written user guide. If the technology is being fielded as a result of a PM-fielded or top-driven system, the office fielding the system may offer the DOIM and support staff the needed training, based upon the agreement in place.

## **7-9. Directories**

*a. General.* This section contains special instructions for promoting good phone service, to include—

- (1) A description of abbreviations used in the telephone directory.
- (2) Instructions on military use and privileges of the military phone system.
- (3) Listing and use of phone priorities.
- (4) Procedures for requesting new phone installations or moves.
- (5) Reporting of phone installations or moves.
- (6) Reporting of phone complaints.
- (7) Security instructions.
- (8) Clearances.
- (9) Procedures for placing various types of on-installation and off-installation calls.
- (10) Procedures for making trouble reports and information calls.
- (11) Procedures for payment of phone bills and filing personal telegrams.
- (12) DSN procedural guidance prepared by the DISA, including Joint Uniform Telephone Communications Precedence System and troubleshooting procedures.

*b. Authorization.* IMA Regions, MACOMs and designated subordinate commands are authorized to print information systems directories for their units/installations in authorized field printing plants, if they do not go over production limits established for the printing plant equipment. When field printing needs exceed established local limitations of duplicating facilities, then commercial procurement is authorized if the procurement is accomplished through the area Government Printing Office or Regional Printing Procurement Office. The installation/activity commander, as part of the command's printing requirements program, authorizes the funds needed.

*c. Standardization.* Publication of the information systems directory is in a standard style to provide Army-wide commonality, thereby aiding use of the directory as well as easing preparation and maintenance. The arrangement, content, and procedures applicable to the preparation and distribution of the information systems directory are followed to the maximum practical extent.

*d. Information systems security monitoring.* In accordance with AR 380-53, paragraph 2-5a(1), official U.S. Army phone or communications directories must display appropriate warning banners and labels.

*e. Master directory.* Each IMA Region, installation, MACOM or other organization keeps a master directory for collection of revised directories. Master directories are kept using automation equipment, word processing, or simple card file, depending on volume and availability of equipment. Procedures to keep the master directory current are developed by the DOIM. The goal is to maintain master directory data on media capable of being updated and printed without re-keying the entire directory.

*f. Miscellaneous.* This section contains an alphabetical listing of functional activities using the private branch exchange system, such as airline ticket agencies, American National Red Cross, banks, barbershops, finance office, installation locator, commercial enterprises, and pay phones. Activities may be listed under their popular name or their official title; for example, Red Cross may be listed under "R" or "A" for American Red Cross. This section may include commonly called DSN numbers.

(1) The DOIM prepares the installation information systems directory.

(2) Printing and binding of information systems directories follow the procedure and guidance established in AR 25-30. Expensive and elaborate printing formats are avoided. All information systems directories are published under the control of the installation, MACOM or other organization's commander. Installation commanders may elect to

include an information systems directory section in the installation civilian enterprise guide or directory, in lieu of printing an information systems directory.

(3) Information systems directories are published in the following format:

(a) The "OFFICIAL" designation (or code name of the command served by the telephone exchange or area covered by the directory); military address to include ZIP code; date of publication; Army or activity emblem (Optional); area code; commercial phone number; and number of the private branch exchange. Emergency numbers such as fire department, ambulance, and military police, with special instructions for their use, if needed, appear in bold print on this page, preferably blocked. Illustrations serving a command purpose may be used as a part of the front cover, but not so as to distract from the goal of the information systems directory.

(b) The following statement is to be printed across the top of the inside cover in bold face or other easy-to-read type: "This publication is the property of the U.S. Government. Distribution is limited to activities and individuals who receive their telephone service from the installation, MACOM or other organization telephone system, and other Government offices on an individual request basis." A duty office phone number of each major installation activity and frequently needed service numbers (for example, utilities, billeting, and phone service) are listed.

(c) For convenience of the phone customer, a form for listing frequently called numbers (name, office, and quarters telephone numbers) appears on unused pages and the inside back cover.

(d) Air raid warning information appears on the outside back cover. Other information, such as location of fire alarm boxes, pay station locations, and bus schedules, may also appear on this cover.

(4) The telephone directory is prepared in the following format:

(a) The first page contains an alphabetical and numerical page guide of major classifications in the directory, giving types of service, and page numbers.

(b) The next index page contains any emergency phone numbers listed on the front outside cover, telephone numbers of activities called in lesser emergencies, and frequently called numbers (utility services).

(c) This section contains an alphabetical listing of organizational activities served by the PBX system, and includes the phone numbers of specified elements within each activity. Building numbers are included. Names of individuals are not listed. When an organization/activity has more than one phone number, one of which is a class C number; the class C number is listed in the directory as the primary number.

(d) At the discretion of the IMA Region, installation, MACOM, or other organization's commander, illustrations serving a functional purpose or giving instructional directions (such as installation maps or time conversion charts) are used on a limited basis.

(e) Card index separators and foldout pages should not be used.

(5) The information systems directory clerk revises information systems directory manuscripts for the DOIM, using inputs that comply with Privacy Act and FOIA requirements, as submitted by information systems subscribers.

(6) Each section of the information systems directory is headed with the title of the section and is identified by markings on the front cover and outside borders of section pages.

*g. Directory changes.*

(1) It is vital that information concerning changes, additions, and removal of information be distributed swiftly throughout the installation. This may be done by information bulletins or similar publications.

(2) Staff sections, units, and tenant organizations submit information systems directory changes to the supporting DOIM office. The report includes all changes, additions, and/or deletions to an organizational section not previously submitted. The format of the current information systems directory is used as a guide in preparing the report.

*h. Other.*

(1) The installation civilian enterprise newspaper, information system directory, transit guidebook, and the civilian enterprise guidebook (AR 360-1), which contains a directory, are the only publications with advertising authorized to be distributed through official mail and distribution channels on the installation/activity. Any other phone directory, commercial or otherwise is a non-DOD commercial publication. Requests to distribute such a publication are a solicitation and are processed per the procedures in AR 210-7, AR 600-20, and AR 360-1. Distribution of a commercial, non-DOD telephone directory must follow AR 210-7 and AR 360-1.

(2) The DMS directory is the best source for addresses used to do organizational messaging. Separate regulations containing the policy procedures, operations, and maintenance of the directory are being developed.

## **7-10. Information technology requirements in military construction projects**

*a. IT included in the prime contract.* U. S. Army leadership directed that military construction (MILCON) projects give a complete and usable facility at beneficial occupancy date and, to meet this goal, directed that all IT be included in the prime contract.

*b. IT definition.* In the context of MILCON, IT refers to the facility's distribution system (the building's IT infrastructure) and the outside cable plant (consisting of cable pathways with installed copper and/or fiber optic cables). The project's capital investment (other procurement, Army funded) items, such as phone switch/switch upgrade, phones and LAN equipment, are not included in this definition. These items are normally user/DOIM-procured and put in by

the beneficial occupancy date. The incorporation of IT within the prime contract consolidates IT requirements under the U. S. Army Corps of Engineers (USACE) contracting authority.

*c. DOIM functions.*

(1) The DOIM documents the project's IT requirements; develops the DD Form 1391 (FY\_\_\_ Military Construction Project Data), Tab F "Information Systems Cost Estimate" (ISCE); and provides this ISCE to the director of public works (DPW) for inclusion in the project's DD Form 1391.

(2) When developing the ISCE, the DOIM defines the IT requirements in technical and functional terms. This includes IT infrastructure/equipment relocations; IT equipment upgrades; and/or IT equipment acquisitions needed to support the project.

(3) Parts of the DOIM staff interview the intended users of the proposed MILCON project to gather data for defining the technical/functional IT requirements. The DOIM develops requirements for related outside cable and duct plant upgrades to support new facilities. Based upon the overall IT architecture for the installation's outside plant infrastructure, the DOIM ensures that the outside plant supports both the needs of the project as well as the long-term growth of the installation.

(4) The DOIM provides the DPW with a dated and signed copy of the ISCE for inclusion in the project's section 17 of DD Form 1391, Tab F, establishing the initial ISCE for the MILCON project. The user requirement must be thoroughly identified in order to complete the cost estimate. The DOIM reviews, revises, and updates Section 17 if the project scope or building functional requirement or site location is changed. The MACOM and the U.S. Army Information Systems Engineering Command (USAISEC)—Fort Detrick Engineering Directorate (FDED) review, validate, and certify the IT requirements and cost estimate for the MILCON projects.

(5) The DOIM develops the initial cost estimate for the project using the ISCE software provided by the USACE. The ISCE software is a freely distributed PC tool developed jointly by USACE and USAISEC as an aid for the DOIM in producing a project's initial ISCE. The DOIM incorporates a minimum amount of project information combines with user requirements to generate an ISCE. After reviewing the ISCE and making any required modification, the DOIM forwards the recommended ISCE to the MACOM for review and concurrence.

*d. Design agent.*

(1) Engineering of the IT is the function of the design agent designated by the DOIM. The design agent may be one of three agents: the USACE, the AMC represented by the USAISEC, or the DOIM.

(2) USACE is normally designated the design agent. As the design agent, USACE ensures that the IT requirements are integrated into the project's overall design by the assigned architect/engineer. Since IT design is not an area of expertise for the USACE, it relies upon USAISEC for oversight of the project's IT designs. NAF projects are reviewed by the USAISEC- Fort Detrick Engineering Office (FDEO) in coordination with HQDA, U.S. Army Community and Family Support Center NAF construction office.

(3) USAISEC-FDEO exercises oversight of MILCON IT. USAISEC-FDEO performs these functions:

(a) Provides planning, programming, and budgeting input to the United State Army Communications-Electronics Command for procurement of IT end instruments and switching equipment in support of IT in MILCON-funded construction.

(b) Reviews user IT, in functional terms, and reviews the user-developed information systems cost estimate for each proposed MILCON project submitted, and provides certification to the Department of the Army, ACSIM ATTN: DAIM-FD, prior to the project review board (PRB).

(c) Gives the installation, the RCIO or the MACOM, and the USACE district with current cost estimates, including related MILCON cost and other appropriations based on design documents.

(d) Participates in updating technical specifications (Corps of Engineers guide specifications) for information systems.

(e) Monitors quality of IT during design and construction reviews for MACOMs.

(f) Participates in HQDA ACSIM PRBs for all MACOM military construction programs.

(g) Provides IT expertise to USACE design and construction reviews for MACOMs.

(h) Prepares IT requirements in support of medical MILCON projects.

*e. ISCE functions.* The ISCE provides the funding justification for the project's IT solution. A good ISCE captures and identifies reasonable costs for technical and functional requirements established by the DOIM in conjunction with the user. The ISCE is begun as early as possible in the project's development cycle and updated throughout the design cycle. In this process, the following agents play major roles.

(1) *RCIO or MACOM functions.* The RCIO or MACOM reviews and certifies the DOIM's ISCE for the project. The RCIO or MACOM may use a variety of methods to complete this task including the ISCE for Windows software, internal staff reviews, and assistance from USAISEC-FDED.

(2) *USAISEC-FDEO functions.*

(a) The USAISEC-FDEO plays several roles with respect to the project's ISCE. As an agent of the ACSIM, USAISEC certifies the ISCEs intended for the MCA program prior to the PRB. This certification ensures that the ISCE is a reasonably accurate estimate of the costs related to the project. USAISEC-FDEO routinely reviews and updates the

ISCEs of MCA projects as they go through the design process under ACSIM control and USACE execution. As subsequent design reviews (from the initial reviews through the final reviews) are completed, USAISEC-FDEO updates the ISCE and gives copies to USACE, the MACOM, and the DOIM involved with each particular project.

(b) USAISEC-FDEO routinely reviews and updates the ISCEs of MCA projects as they progress through the design process under ACSIM control and USACE execution. As subsequent design reviews (from the parametric design phase through the final engineering design reviews) are completed, USAISEC-FDEO updates the ISCE and gives copies to USACE, the MACOM and the DOIM involved with each particular project.

(c) USAISEC-FDEO participates as a member of the planning charrette as the technical advisor to the DOIM, RCIO, and MACOM. Coordinates with the installation DOIM to determine the telecommunication requirements for the project.

(d) USAISEC-FDEO integrates the ISCE into the project's overall requirements and tracks subsequent ISCE throughout the project.(4).

## **Chapter 8**

### **Army Public Web Site Management**

#### **8-1. Web site planning and sponsorship**

a. *Target audience.* Web sites should be made publicly accessible on the Internet only when the target audience includes the public at large. Information that is for Army personnel only should be moved to AKO or other approved private Web site. Private (intranet) Web sites must migrate to AKO per AR 25-1, paragraph 3-9.

b. *Accurate information.* Users of Army public Web sites must be assured access to accurate official information, regardless of whether the site is linked only to other Government Web sites or also to private sector Web sites.

c. *Web Site purpose and plan.* Each Army organization that establishes a public Web site (or Web presence) must have a clearly defined purpose and Web site plan supporting the organization's mission. The plan should be approved by the organization's parent command or organization. The Web site plan addresses at least—

- (1) Web site registration.
- (2) Identification of Webmaster contact information.
- (3) Procedures that explain administration of the Web site on—
  - (a) Posting of information.
  - (b) Reviewing the site for content and format.
  - (4) Contingency and continuity of operations.

(a) The plan should state what the sponsor will do with the Web site(s) during disasters or emergencies, including important information and services to be provided to the public.

(b) Web site plans will be documented in the organization's continuity of operations plans.

d. *Domains.* New Army public Web sites are established in the army.mil domain to show that they are official sources of Army information. This applies to all Web sites. Organizations using non-.mil domains should execute plans to transition Web sites to the army.mil domain in order to comply with Federal Web site policy. Exceptions to the use of the army.mil domain should be submitted to the Army CIO/G-6, SAIS-GKP.

e. *Web site listings on the Army HomePage.* The Army HomePage (<http://www.army.mil/>) provides public Web site locator information for the Army's units and installations (Army A-Z). Organizations and installations with public Web sites will ensure that their sites are posted on the page. Fill in the Web maintainer and sponsor contact information for the Web site and the URL in the contact us link at the bottom of the page.

f. *Registration approval.* Registration for army.mil domain requests is achieved through the following processes:

(1) Army Internet registration is a part of the mission of the CONUS Theater Network Operations and Security Center (CONUS-TNOSC), <http://www.conus-tnosc.army.mil>. CONUS-TNOSC is part of NETCOM/9th ASC. NETCOM supports Army installations needing to apply for Internet protocol addresses via the NIPRNET and SIPRNET.

(2) DOIM or others with registration duties select the Internet registration option on the TNOSC Web site and inform the Army community they support. These online instructions lead the user to downloadable templates for providing the required information. When the template is completed, users send it directly to [domain-request@aims7-army.mil](mailto:domain-request@aims7-army.mil).

g. *Web records administration.* Web records must be managed per OMB Circular A-130 and guidance from the National Archives and Records Administration (see 36 CFR 1220-1238 and [www.archives.gov/records\\_management/index.html](http://www.archives.gov/records_management/index.html)).

h. *Web masters/maintainers.* Army organizations assign a Web master for each public Web site they sponsor. The Web master/maintainer has technical control over the registration process, managing the site's content, and ensuring the site conforms to Army Web site requirements.

i. *Sponsorship display.* Army public Web sites must clearly display "U.S. Army" on every page along with the organization's official name and include a statement that the Web site contains official Government information. Home

pages and second tier pages include a page title, as part of the metadata, with the organization's name identified as the site sponsor.

*j. Labeling.* Accessible information will be labeled to indicate the following where appropriate:

- (1) Draft policies, regulations, and other predecisional information are not posted on public Web sites.
- (2) Copyrighted information for which releases from the copyright owner have not been obtained.

*k. Web site linking.* Army public Web sites will follow these requirements when linking to other Web sites:

- (1) Use only text or hyperlink text to direct users to non-Army software download sites.
- (2) Post a link to a "process for linking to non-Army sites" and include guidelines for selecting and maintaining external links. The decision to use a link to an external source must exhibit sound public policy and support the Army's mission. Organizations linking procedures must explain why some links are chosen and others are not. The links must be chosen fairly and in the best interest of the public (see AR 25-1, para 6-4n).

(3) The linking policy found on FirstGov.gov is suggested as an example for developing Army public Web site linking policies. Hyperlinks to Web resources other than official U.S. Government Web resources are permitted only if the organization's mission requires them (see AR 25-1, para 6-4n for policy on linking to non-Government Web sites).

*l. Date posted data.* Army public Web sites will clearly state the date the content was posted or updated for every Web page, indicating to visitors that the content is current and reliable. Web masters/maintainers should include a statement such as, "Last updated on \_\_\_" or a date stamp to each page altered or reviewed.

## **8-2. Content propriety and quality**

*a. Information of value.* Army public Web sites should only post information of value to their visitors. These visitors include users from Army organizations, other Government agencies, academies, the private sector, and citizens with an interest in the missions performed.

*b. Content limitations.* Army public Web sites content will comply with the following content limitations:

(1) Abbreviations should not be used on the front page but may be used on sub-pages if the words are spelled out first.

(2) The .mil Web sites may not be directly linked to or refer to Web sites created or operated by a political campaign or committee.

(3) The Army Web content owner ensures that information submitted for posting to an Army public Web site is current, timely, and cleared for applicable release by the public affairs officer or other designated official to ensure compliance with AR 25-1, paragraph 6-4n, and at appendix C.

*c. Content organization.* Information should be organized by subject/topic, by audience group, by geographic location, or by any combination of these factors, based on an analysis of the visitor's needs.

*d. Content focus.* The content should be the main focus for the target audience and serve as a general index to all major options available on the Web site. Home pages will minimize extraneous content to allow visitors to get to the content it needs and wants most.

*e. Exclusive information.* Web sites should not contain information that is meant exclusively for organization employees and is of little or no use to the private sector except in emergency or other exceptional situations. Information for an organization's exclusive use should be contained in AKO or other approved intranet site.

*f. Public Web site content.* Web masters/maintainers should provide the following content in each Army public Web site:

(1) A link to a page entitled "Contact Us" or "Contact (Organization Name)" from the home page and every major point of entry. Contact information will be generic and will include—

(a) Organization's street address, including addresses for any regional or local offices.

(b) Office phone number(s), including numbers for any regional or local offices.

(c) Means to communicate by electronic mail (for example, organizational e-mail address or Web-based contact form (for example xxxwebmaster@us.army.mil)).

(d) The organization's policy and procedures for responding to e-mail inquiries, including whether the organization will answer inquiries and the expected response time.

(e) Contact information, as required by information quality guidelines.

(f) Contact information (office names/titles/phone numbers) for small businesses as required by the Paperwork Reduction Act.

(g) Means to request information through FOIA. Make FOIA information requests by e-mailing FOIA@rmda.belvoir.army.mil.

(2) Main entry point Web sites (for example, Army Home Page, Army Reserves, Army National Guard, MACOMs), which should include a link to a page entitled "About Us" or "About (Organization Name)" from the home page. Organizational information will include at least all of the following:

(a) A description of the organization's mission, including its statutory authority.

(b) A strategic plan, vision, or set of principles.

(c) An organizational structure, including basic information about parent and/or subsidiary organizations and regional and field offices, as appropriate.

(d) Contact information, which may include e-mail addresses, phone number, office, name, or position.

(e) Information about jobs at the organization. The preferred method is to link to Civilian Personnel On Line (<http://acpol.army.mil/employment/index.htm>).

(f) A link to a site map or subject index that gives an overview of the major content categories on the site. At a minimum, a link to the site map or subject index will be provided from the home page.

(g) A link to a “Common Questions” or “Frequently Asked Questions” Web page providing basic answers to questions the organization receives most often.

(h) Easy access to existing online citizen services and forms that are applicable to the general public. These items should be displayed as prominently as possible, and based on an analysis of customer needs.

(i) Information about professional opportunities in organizations.

(j) Links to a portal for the most frequently requested publication(s).

(k) Web site policies and important notices. Organizations will post (or link to) a page entitled “important notices” at the footer of every Web page. The important notices page describes the principle policies and other important notices that govern the Web site, especially those mandated by law. At a minimum, this page will include—

1. Privacy policy. Include in this policy a statement that the site does not use “persistent” cookies or any other automated means to track the activity of users over time and across Web sites.

2. Security policy.

3. How to request information under FOIA.

4. Accessibility policy.

5. Information quality guidelines.

g. *Assessing the user’s satisfaction.* Army public Web site sponsors should conduct an annual assessment of user satisfaction with the Web site, including usability to identify needed improvements.

h. *Army installation newspapers.* Army installation newspapers are authorized and established according to AR 360–1. Though generally public domain, these newspapers are part of the Army internal information program. While publishing installation or organization newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited access Web site represents global release. Some information appropriate for installation newspapers is not appropriate for public Web sites. Army organizations may reproduce the content of installation newspapers for the Web if that content meets the restrictions provided in AR 25–1, paragraph 6–4n. These restrictions include prohibitions against posting names, locations, and specific personal identifying information about employees and military personnel and their family members. Advertisements appearing in private sector newspapers should not be posted on Web sites.

i. *Commercial use of communications systems.* Use of communications systems for commercial purposes in support of for-profit activities or for personal financial gain is prohibited (see AR 25–1, para 6–1f).

### 8–3. Usability criteria

The usability guidelines contained at <http://www.usability.gov> may be a valuable tool for Web site designers.

a. *Accessibility.* Army public Web sites must be accessible to all citizens (see to AR 25–1, para 6–4 and para 7–5, above).

b. *Public Web site requirements.* Public Web sites should be developed according to the following guidelines:

(1) Web master/maintainers will ensure that pages are designed, developed, and tested for multiple browsers, operating systems, connection speeds, and screen resolutions, based on an analysis of an organization’s Web site visitors. Army public Web sites will, to the maximum extent feasible, minimize page download times for their visitors.

(2) Web sites should be compliant with Section 508, designed to make online information and services fully available to citizens with disabilities. The important notices page described in paragraph 8–2e(8) must include a link to an accessibility policy that describes compliance with the Act.

(3) Information should be presented using plain language which considers the knowledge and literacy level of the typical visitor. The text must be gender neutral and be accessible to persons who, as a result of national origin, are limited in their English proficiency. Understandable language and content criteria are included in any customer satisfaction survey.

(4) File formats used will be based on operational needs of the organization and the needs of the customers. Organizations will provide information in a format that does not require the public to use plug-in or additional software, if it imposes a burden. When a Web page requires an applet, plug-in or other application in order to interpret the page content, the page should provide a link to a plug-in or applet. When choosing the file format, the organization will consider—

(a) The intended use of the material by the target audience.

(b) The accessibility of the format to the target audience.

(c) The level of effort required to convert the material to the format.

(5) Organization Web sites that link to documents requiring downloading will provide sufficient contextual information so visitors have a reasonable understanding of what to expect when they view the material.

(6) Proprietary formats are only used when the audience is known to have easy access to software able to read the format. Raw data files provide the greatest flexibility for the public and are preferred over proprietary formats requiring specific commercial software. Consistent navigation schemes between and within all Army public Web sites will be used.

(7) Visitors are more likely to get what they need from a site if changing navigation doesn't confuse them. Standard navigation criteria is provided as follows:

(a) Common items appearing on most Web pages will, if possible, be in the same location on each page and have the same appearance and wording. A navigation item that is shared by a group of pages (such as a set of pages on a single topic, or for a division of the organization) will also have the same location, appearance, and wording on each page.

(b) Navigation items of the same type will look and behave like each other. For example, if a set of pages on one topic has subtopic links in the left navigation bar, pages on other topics will have subtopic links in the left navigation bar that are similar.

(c) If a set of Web pages requires specialized navigation, that navigation is applied to the largest possible logical grouping (such as a topic, an audience, or a complete organizational unit). The specialized navigation will be similar in appearance and behavior to your overall navigation scheme.

(8) Web masters/maintainers should include either a search box or a link to a search page from every page of the Web site. The search box or link will be entitled "search." Place subject and keywords in source code to aid content searches. Focused searches may be given to search within sets of information, databases, or applications. Web sites that are narrow in scope or under 200 pages may substitute a site map or A to Z index rather than implement a search engine. Army public Web sites will have the following minimum service level standards:

(a) What is the extent of search engine crawling and indexing? What types of documents are crawled and indexed? How often are they crawled and indexed?

(b) What are the best ways to search your documents or collections? Will visitors enter phrases or keywords? What other hints can you give visitors?

(c) What is the expected search response time? For example, 95 percent of searches get a result set returned within 5 seconds.

(d) How can customers use the search engine for more precise searching and browsing (that is, minimum chaff) or for recall (that is, maximum wheat)? For example, if searching for a specific marketing report, include the country name, the year, and the type of report, for example, strategic planning.

(9) Include the following five meta tags on all home pages and major entry points:

(a) Page title.

(b) Description.

(c) Creator/sponsor (in most cases, the organizational name).

(d) Date created.

(e) Date reviewed.

(10) Web site visitors will be informed about major proposed and implemented changes to the Web site. Webmasters/maintainers should place a notice on the home page informing visitors about the change, insert redirect notices when page destinations are changed, and clarify changes on the Help page.

#### **8-4. Training and compliance**

*a. Sponsor functions.* Army public Web site sponsoring organizations must ensure that Web site development, maintenance, and operations staff understand applicable requirements specified herein. The sponsor ensures that the public affairs officer or other appointed official reviews and clears the Web content during the establishment of the site and conducts quarterly reviews of updated content. (AR 25-1, para 6-4*n*, and appendix C-4 contain Army policy on Web site prohibitions for content pertaining to operational security, privacy, sensitive information, pre-decisional information, information exempt from Freedom of Information Act, copyrighted information, commercial sponsorship and advertising, and others.)

*b. Training.* All individuals appointed to be Web masters/maintainers, reviewers, and content managers must complete training and certification, as necessary, equal to the duties assigned to them. Web-based training is available at AKO (<https://iatraining.us.army.mil>). This course is mandatory for all webmasters/maintainers.

#### **8-5. Consistent and nonredundant information**

*a. Redundancy.* Content and services provided via Army public Web sites should not be redundant or in conflict with each other. The following requirements will be implemented by all Army public Web sites so that this is achieved.

*b. Links to information.* Web sites should link to existing Government-wide portal or specialized sites when applicable, rather than recreating these resources themselves.

(1) Before creating new information, the organization determines if that same or similar information already exists within their organization or on another Army, DOD, or Federal Web site.

(2) When an organization Web site provides information or services for which there is a corresponding Government-wide portal or specialized site, the organization will link to the Government-wide portal or site from its pages on that topic.

(3) When a Government-wide portal or specialized Web site is available on a subject that the public would expect to find on an organization's site, but the organization does not provide that information, the organization will link to the Government-wide portal or site in a logical and useful location.

(4) Organizations should not link to Government-wide portals or specialized information unless they are related to the organization's mission or function or might be seen as being related. Links that are not related to a Web site's content can be deceptive and confusing.

(5) Organizations should not re-post documents that other organizations originated. Instead, they should provide links to those documents that are posted on the Web sites of the content owners. Organizations should consult with each other to find ways to share or coordinate content and to mitigate duplication.

(6) As with all links, organizations will review links to the content on other organization Web sites or to portals and specialized Web sites regularly to ensure they are current and accurate.

*c. Home page link.* To improve Web site utility, each Web page links back to the Web site home page. If an organization uses a graphical link, it contains text indicating that it links to the home page. Headquarters staff elements and major commands should provide a link back to the Army home page ([www.army.mil](http://www.army.mil)). Subordinate elements of a major command should provide links back to the respective major command and the Army Home Page.

*d. Firstgov.gov link.* Major organizational home pages (Army Home Page, MACOM, HQDA staff element) should link to the FirstGov.gov home page ([www.firstgov.gov](http://www.firstgov.gov)) with the entry: "FirstGov: U.S. Government Web Portal."

## **8-6. Federal law, regulation, and policy compliance**

*a.* Army public Web sites comply with applicable Federal law, regulations, and policies.

*b.* Refer to AR 25-1, paragraphs 6-1 and 6-4*n*, for official and authorized use of Government communications and prohibited usage and for Army Web policy, respectively, and appendix C-4 for Web policy management controls. Refer to at [www.defenselink.mil/webmasters](http://www.defenselink.mil/webmasters) for DOD policy and guidance and [www.firstgov.gov/webcontent/index.shtml](http://www.firstgov.gov/webcontent/index.shtml) for Federal policy and guidance.

## **8-7. Director of information management Web site administration**

*a. DOIM functions.* DOIMs are required to—

(1) Develop and disseminate local procedures and controls for security and access for installation-hosted Web sites (see AR 25-1 and AR 25-2 for Army Web policy).

(2) Control all Internet connections, to include military-controlled access paths and alternate Internet access paths, such as Internet service providers.

(3) Ensure all traffic destined for other military sites (within the ".mil" domain) is only routed through military controlled networks (that is, traffic destined for military sites will not be routed through an ISP and traffic from an ISP will not be routed through the receiving base network to other military networks).

(4) Ensure "army.mil" network domains are not advertised through ISP connections and are protected by an Army reverse proxy server.

(5) Ensure access to the Internet is secured to acceptable risk levels.

(6) Audit the network continually to locate unauthorized public access Web servers and unapproved limited-access Web servers. For unauthorized public access Web servers, the DOIM or designate contacts the supervising Web site owner moves data to the NOSC/NOSC-D/NCC/NCC-D server, and takes action to disconnect the unauthorized public-access server from the network. Take appropriate action to ensure the network and the information are protected.

*b. Procedures.* DOIMs or other IT providers should establish procedures for their customers on governing the administration of the Web server environment. As a minimum, procedures should address—

(1) Operation of the Web server environment.

(2) Security of the Web server environment.

(3) Maintenance of access and security control features and ensuring that warning and consent to monitoring notices are installed as appropriate.

(4) Process to ensure DAA approval is re-issued if any Web server environment configuration is changed.

(5) Process to ensure all links from pages under DOIM control is appropriate and valid.

(6) Procedures for content providers and page maintainers to post on the Web server.

(7) Granting and monitoring write-access privileges.

(8) Maintaining and evaluating audit control logs.

(9) Gathering and analyzing performance data.

(10) Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

(11) Coordinating mirror or replication sites with other system administrators, as required.

(12) Implementation of security and access controls requested by content providers and page maintainers as required.

(13) Access list for administration/maintenance.

(14) A feedback mechanism for users' comments in accordance with the Paperwork Reduction Act of 1995..

(15) Compliance with federal policies on privacy and data collection on Web sites. Privacy (and security) policies should be clearly posted and easily accessed on the front page of the Web site.

(16) Cooperation with AWRAC for notification of a violation. DOIMs will ensure that Web sites links are disconnected until corrections have been completed (see AR 25-1, para 6-4*n*).

(17) Compliance with Section 508 provisions to make information on Web sites accessible to employees and the public. See Federal accessibility standards at <http://www.section508.gov/index.html> for the latest information. At a minimum these include—

(a) A text equivalent for every nontext element will be provided (for example, via "alt" (alternative text attribute), "longdesc" (long description tag), or in element content.

(b) Web pages designed so that all information conveyed with color is also available without color, for example from context or markup.

(c) Pages designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.

(d) Documents organized so they are readable without requiring an associated style sheet.

(e) Web pages updated for equivalents for dynamic content whenever the dynamic content changes.

(f) Redundant text links instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(g) Client-side image maps whenever possible in place of server-side image maps.

(h) Row and column headers identified for data tables.

(i) Markup to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(j) Frames titled with text that facilitates frame identification and navigation.

(k) A link to a plug-in or applet providing equivalent information on an alternative accessible page, when a Web page requiring that an applet, plug-in, or other application be present on the client system to interpret page content the page.

(l) A text-only page, with equivalent information of functionality, to make a Web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page will be updated whenever the primary page changes.

(m) A method that permits users to skip repetitive navigation links.

(n) When pages utilize scripting languages to display content, or to create interface elements, script-provided information identified with functional text that can be read by assistive technology.

(o) When electronic forms are meant to be completed online, a form to allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(p) When a timed response is required, the user will be alerted and given sufficient time to indicate more time is required.

*c. Army Web risk assessment cell (AWRAC).* The AWRAC reviews the content Army publicly accessible Web sites (.mil and all other domains used for communicating official information) to ensure they are compliant with DOD and Army policies and best practices. The AWRAC—

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

(2) Ensures inappropriate security and personal information is removed from publicly accessible Web sites.

(3) Ensures that Army sites are compliant with other Federal, DOD, and Army Web site administration policies (for example, GILS registration).

(4) Notifies the Web site owner with operational authority and the Information Assurance Program Managers of respective command/activity of violations and suspense dates for reporting corrective action.

(5) As required, reports deficiencies and corrections to the Army CIO/G-6 and JWRAC.

*d. System security considerations.*

(1) Each organization will establish information system security certification and accreditation procedures in accordance with DODI 5200.40.

(2) Operators of Web server environments should be trained in technical information security best practices, or should have immediate access to appropriately trained individuals. Security maintenance and administration should be

considered an essential element of Web site operation and maintenance at all times. It is essential that Web server environment be implemented and maintained by certified personnel. Day-to-day maintenance of the hardware and software, including security patches and configurations, is essential to the system security of Web server environments. See also National Institute of Standards and Technology (NIST) Special Publication 800-44.

(3) A formal risk assessment should be conducted at each organization operating a Web site to determine the appropriate risk management approach based on the value of the information; the threat to the Web server environment and the information contained thereon; the vulnerability of the Web server environment and the information contained thereon; and the countermeasures employed by the Web server environment. A security policy should be written for each Web server environment or multiple sites furnishing similar data on the same system infrastructure or architecture based on the results of the risk assessment.

(4) Web servers that are externally accessed should be isolated from the internal network of the sponsoring organization. The isolation may be physical, or it may be implemented by technical means such as an approved firewall. The server software will be compliant with Federal Information Systems (FIPS) 140-2, with all security patches properly installed. Approved security protocols will be used for all Web servers. Additional security measures should also be employed consistent with the risk management approach and security policy of the individual Web site. Examples of additional measures to be considered include—

- (a) Disabling IP forwarding, avoid dual-homed server.
- (b) Employing least privilege.
- (c) Limiting functionality of Web server implementation.
- (d) Employ tools to check configuration of host.
- (e) Enabling and regularly examining event logs, to include—

1. Back-up methodology as part of the Web site architecture. Information should be replicated to the backup environment to ensure that the information will not be lost in the event that the Web server environment is corrupted, damaged, destroyed, or otherwise compromised.

2. ID and password protection. The internet is an unsecured network where compromise of user ID and password can occur during open transmission. IDs and passwords should not be transmitted without encryption. Secure protocols (for example, secure sockets layer protocol) provide a transmission level of encryption between the client and server machines (see AR 25-2).

## **Chapter 9**

### **Software and Hardware Asset Management**

#### **9-1. Acquisition**

The best method of acquiring software and hardware is through solutions based on COTS or a reuse of Government-off-the-shelf products that comply with Army specified standards. The suitability of products for satisfying operational requirements must be evaluated before initiating a development effort. This evaluation is performed by local installation DOIMs or the program executive office (PEO) associated with this acquisition. The evaluation should also determine integration risks associated with the COTS products.

a. *Enterprise Software Initiative (ESI)*. It is DOD policy that before purchasing any COTS software product, the Army acquiring official determines if it is managed under the ESI. Enterprise software agreements (ESAs) negotiated with specific software publishers or their agents offer the best prices and terms. OSD has authorized each service to manage various categories of software applications (for example, database, desktop, graphics, operating systems, and servers) for all of DOD. The Army acquiring official coordinates the acquisition with the designated DOD ESA product manager for that product prior to entering any agreement with any COTS vendors.

(1) If an existing ESA does not contain desired terms or prices, the acquiring official must notify the ESA product manager and allow them to improve the existing ESA before executing other agreements. The Army Small Computer Program (ASCP) is the Army's software product manager. As the designated software product manager, ASCP is responsible for managing the Army's ESA products. Army customers must request waivers for commercial software not being acquired from a DOD ESI agreement at the ASCP Web site, <https://ascp.monmouth.army.mil>. The DOD ESI homepage lists all ESI managed software and is located at [www.esi.mil](http://www.esi.mil).

(2) The Army entered into an enterprise license agreement for word processing, spreadsheet, database, and presentation software products. Details and ordering information are provided on the ASCP Web site. As organizations increasingly turn to COTS application package solutions for requirements that were met before by in-house or contractor software development projects, care must be taken to ensure that the selected COTS solution meets the organization's requirements. The suitability of COTS or Government off-the-shelf applications for meeting operational requirements must be gauged before starting a development effort.

b. *ASCP office*. The ASCP is the primary source for purchase of COTS software, desktops, and notebook computers regardless of dollar value, and for all other IT purchases greater than \$25K. All commercial IT purchases must be

submitted to the ASCP office. If the ASCP office is incapable of fulfilling a request, a waiver may be granted allowing the purchaser to acquire IT hardware, software, and services from GSA or another approved source. The ASCP Web site is <http://ascp.monmouth.army.mil>.

*c. COTS planning.* To increase awareness and provide a more successful COTS solution, the following steps should be taken:

(1) Early in the process, get a full understanding of the functionality of the COTS or hardware package. If possible, obtain hands-on experience with the system. Consider prototyping or piloting the package in your environment. At least visit another organization that is using the software.

(2) Look at the gap between business processes supported by existing systems and future requirements and those supported by the COTS package to meet unique organizational needs. Ensure that the organization can accept this gap without degrading performance.

(3) Incorporate lessons learned. Actively solicit and rigorously incorporate lessons learned by similar organizations into the implementation plan.

(4) Because the implementation of a COTS product could notably impact the business functions of an organization, it is vital that the planning process involve the user community from the outset. In addition to technical issues, understanding business issues lessens the risks associated with COTS implementation.

(5) Verify the product's capabilities with other users to ensure that the capabilities support the needs of the organization. For example, confirm that the product has previously supported the number of users and geographic locations that the organization will require. Test the COTS product in the operating environment to ensure compatibility.

(6) Ensure that new or existing software uses the Federal Information Processing Standards for the 4-digit date format for data exchange. PMs are required to identify Government off-the-shelf/COTS software that uses the 2-digit date windowing technique and then modify it to the 4-digit standard. Modification requires either replacing the system with a later version not employing the 2-digit date windowing technique or installing 4-digit software that removes the problem date formats. After the system is modified, it is then re-certified.

(7) An implementation involving a COTS product with a successful track record is less risky than one involving new, unproven capabilities. It is crucial to utilize mature, road-tested COTS products. Ensure that a reputable and reliable vendor is and plans to be available to support the product.

(8) Fully understand contractual conditions.

(9) Completely understand details associated with the product contract, including the licensing agreement.

(10) Find out who owns the source code, what rights are provided relative to source code modification, and what arrangements will exist at contract expiration.

(11) Validate that the agreement sufficiently meets the organization's needs.

*d. Standardization.* The acquiring official must ensure the COTS/Government off-the-shelf and hardware products acquired comply with the standardization required by the current version of the DOD IT Standards Registry (DISR) and the NETCOM technical control on desktop and server standardization. The goal is to ensure standardization and interoperability in each system. To ensure interoperability, the acquirer must clearly identify types and versions of the software supported. Before acquiring and using products that are not DISR or NETCOM technical control compliant, the acquiring official must follow the waiver process described by DISR or NETCOM technical control guidance (see DISR at <http://disronline.disa.mil>, AR 25-1, and chaps 4 and 5 of this pamphlet).

*e. Accountability.*

(1) IT and computing resources account for a significant portion of an organization's budget. DOIMs may reference existing supply regulations (for example, AR 710-2) for guidance on IT resource accountability. The DOIM's close coordination with the Property Book Officer (PBO) assists the DOIM in developing a sound asset management program. It is vital that the DOIM be given prompt notification of the receipt of computing resources at the installation. This information assists the DOIM in providing a more complete service to customers in the area of computing resources acquisition. With regular feedback from the PBO, the DOIM can help ensure a customer's order is received in a timely manner. Once software/hardware is received, it is placed in the DOIM's asset management and life-cycle management programs.

(2) The property accountability threshold has changed to \$5,000 for property accountability below the stock record account. The change supersedes all previous guidance concerning property accountability thresholds. The new threshold aligns Army requirements with the rest of the DOD. The new threshold does not relieve personnel of command, supervisory, custodial or personal functions. It is recommended that asset management software be used for accountability and reporting.

(a) Hardware will be accounted for using the appropriate supply regulations addressing property book accountability. Software is treated as a durable item. Although software does not require property book accountability, it will be controlled by the using organization's IMO. Durable property is personal property that is not consumed in use, does not require property book accountability, but because of the nature of these items, they must be controlled and functions assigned.

(b) The Defense Property Accountability System is the installation property accountability system for nondeployable

units and installations and can record, track, calculate depreciation, and facilitate the annual reporting of general property.

(c) The checklist in AR 25-1, appendix C, is to assist HQDA, field operating agencies, MACOMs, and installations in evaluating the key management controls; it is not intended to cover all controls for IT accountability. Answers must be based on the actual testing of management controls. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years.

(3) For information on the screening, redistribution, and disposal of IT equipment, refer to para 11-3 of this document for information on the Defense Reutilization and Marketing System (DRMS).

(4) The organization's IMO plays a key role in the accountability of computing resources. When software or hardware products are received, either the IMO or the DOIM maintains the accompanying license. If software is installed and accessed from a central server maintained by the DOIM, the DOIM maintains the license. If the hardware is installed and accessed as part of the installation server plan and is maintained by the DOIM, then the DOIM maintains the warranty and registration. When a product is not a centrally maintained package, but rather a specific package for the unit or section, then the unit/section's IMO maintains the license and issues the software to individuals using hand receipts. The DOIM/IMO may also maintain a set of the accompanying manuals as a reference set for the users.

(5) When a computer system or software is transferred, the hand receipt holder ensures that property accountability is also transferred. The software is removed (or uninstalled) from the hard drive before the system is transferred or turned-in, even if the software is being transferred to the same site. This reduces the possibility of confusion in the serial number of the software on computers and the serial number on original diskettes and documentation.

(6) In cases of lost, stolen or damaged hardware, software, or documentation, the user reports the incident to their supervisor and IASO, providing details of the incident and asset identification information per AR 735-5. The IASO reports the incident to the IMO, who then conducts an investigation.

*f. Life-cycle management.*

(1) The DOIM's implementation of a strong life-cycle management (LCM) program ensures that a sound base of automation tools is available to aid the organization's mission. The LCM program also helps ensure that the unit has a more effective internal control program by greatly assisting the organization in projecting and managing its annual IM costs. The user is better able to address automation requirements, as only new requirements must be considered, while existing requirements are kept current via the LCM program (see AR 25-1, para 6-2m for guidance concerning the DOIM's LCM program).

(2) An effective LCM program requires the coordination of many parts of an organization. As automation equipment or software is received at the unit, key information is maintained by the PBO and sent to the DOIM, including purchase date, cost, vendor data, warranty data, and specific identifying data about the hardware or software itself such as license/registration numbers of the product and the method of disposal. All information may be kept in a database created for the LCM program. As the device or package is fielded, the user, unit, and location data are put into the database, which likely requires coordination between the IMO/IASO and the DOIM. Other data are added, either initially or through the life cycle of the hardware or software, as the DOIM sees fit. An example of such data is the dates when the device or package required servicing or the user required assistance with its use.

(3) Use of software tools to automate the requirements of a LCM program boosts its utility to the organization. There are software packages that discover equipment over the LAN and aid in making the task of developing and maintaining a LCM database easier. There are tools to tie the LCM program into automation tools used by the organization's help desk. These tools are available in various configurations to meet specific needs and size of an organization.

(4) The LCM program at a level higher than the installation considers the needs of the particular headquarters location and the consolidated requirements of its subordinate units. Coordination between the headquarters and the subordinate units cannot be overemphasized. This approach is beneficial to the POM process and provides the opportunity to reduce automation procurement and maintenance costs.

*g. Software and hardware control procedures.*

(1) Once hardware or software has been received, the DOIM, PBO, or hand-receipt holder provides the product and registration card to the unit IMO. The hardware or software is then installed and the IMO or IASO registers the product with the vendor. This process is dependent upon the organization's development of good business practices to ensure all software registration cards are given to the IMO.

(2) Use of personally owned hardware or software is highly discouraged and, following technical review and initial approval by the DOIM, needs approval of the IASO and commander. For hardware, the property is accredited and registered using hand receipts. The owner signs a release of liabilities in case of theft, loss, damage, or malfunction, and acknowledges that all work-related products are the property of the Government. Once the user's personally owned hardware has been accredited, it can be used for processing of Army information.

(3) When software is due for updating, the IMO ensures software updates are installed by the appropriate personnel. The procedure is different for antivirus software. This software is updated either automatically when the user logs into

the LAN, or when the IASO receives the antiviral software (or update) and ensures that all systems within their area of authority are updated. Sometimes concurrence is required for this action, for example, in response to a major information system security incident. DOD employees may use antivirus products on their own personal computers at their homes. This reduces incidents of virus infiltration from home computers owned by DOD employees. It may be used by DOD contractors working on DOD-owned PCs but not by DOD contractors working on company-owned PCs at their workplace. It may not be used by DOD contractors on personal home PCs. The antivirus software for home use is found at [www.cert.mil/antivirus/antivirus\\_index.htm](http://www.cert.mil/antivirus/antivirus_index.htm).

(4) The DOIM and IMO develop procedures and training and awareness programs to ensure compliance with software copyright laws and trade agreements. All commercial software is proprietary, and unauthorized reproduction or distribution is in violation of Federal law (17 USC Chapters 1 and 2) (see AR 25–1, para 6–21).

(5) Software is a durable item. Though it does not require property book accountability, the organization IMO or IT officer controls software use. To maintain this accountability, organizations should:

(a) Establish and maintain a record keeping system for hardware and software documentation and materials showing compliance with legal requirements governing use of the organization's products, including original licenses, certificates of authenticity, purchase invoices, and copies of completed registration cards. The use of product management computer programs is recommended. If feasible, store such records, as well as any original software media, in secure, designated locations within the organization.

(b) Develop hardware and software use policies that include provisions concerning the downloading of software from the Internet by the organization's employees, and the use of privately owned products on organizational computers. Ensure that such use complies with applicable licenses and organizational policy.

(c) Develop and adopt procedures for monitoring compliance with product management policies, addressing reports and incidents of alleged violations of the policy, and disciplining employees who knowingly violate the policy or Federal copyright laws.

(6) To ensure that all users understand licensing and copyright restrictions, the DOIM or the organization's IM/IT officer has users sign a statement of understanding for use of commercial software. This statement may be a memorandum stating that the user agrees to adhere to all licensing restrictions. It must inform the user of the consequences of violating licenses or copyright agreements. All users of Government systems must read and sign the statement before access to a Government computer system is granted. The statements should be kept on file with the IM/IT officer.

(7) Organizations require DOIM support in determining the acceptability of privately owned military, public domain, and shareware software packages. Before installation of these types of software, written authorization must be obtained from the IASO to ensure that the software does not conflict with or corrupt Government-owned resources.

*h. Reutilization/disposal.*

(1) COTS software licenses and hardware no longer needed for their original purpose must be reported for internal DOD redistribution screening unless redistribution goes against the licensing agreement or the licenses are exempted per the IT Asset Redistribution Program. The reporting activity must ensure adherence to vendor licensing agreements.

(2) Before disposing of excess products, organizations should request disposition instructions from the DRMO. Disposition instructions may include transferring to other Government or private sector organizations or destruction (see para 11–3). Software and hardware providing direct security protection to automation or telecommunications equipment systems that process classified information, or is designated under DOD 5200.1–R and NAF-procured software items are non-reportable IT assets for redistribution screening. Some examples are products:

(a) Vital to weapons, intelligence, command and control, or tactical data systems.

(b) Software ineligible for upgrade or maintenance by a commercial vendor.

(c) Modified beyond the specifications of the commercially available version.

(d) Licensed under provisions that restrict use to a specified machine, system, site, or is otherwise restricted from redistribution within DOD.

(e) Locally or centrally purchased by nonappropriated funds. These systems are returned to the control of the Installation NAF manager and administered per AR 215–1.

## **9–2. Information processing services**

*a. General.*

(1) Within their service regions, Army DOIMs must offer an array of support services to a diverse user community. Continued growth in the use of technology increases the competition for DOIM resources. This competition requires users to involve DOIM staffs at the start of planning if new or changing office automation requirements are projected. DOIMs should maximize the use of existing products and services to satisfy needs before looking at unique solutions.

(2) User requests that cannot be satisfied internally by the DOIM office are carefully examined. DOIMs should suggest nontechnical alternatives when viable, such as changing processes. If the DOIM cannot provide a needed automated solution, the DOIM assists the customer in procuring the capability from other sources.

(3) DOIMs make every effort to respond to critical requirements. However, the ability of DOIMs to respond is affected by customer requirements. DOIMs should work closely with customers to prepare for unusual requirements,

such as unscheduled production runs, surging transaction volumes, program modifications needed to satisfy directives from higher sources, etc. Advanced planning allows enough time to analyze the requirement, adjust priorities among other users, and ensure that all involved in the effort are advised.

*b. Individual facility operations.* Army DOIMs typically support the following functions:

- (1) Operation and maintenance of common user computer resources, including—
  - (a) Operating system maintenance and system administration.
  - (b) Job scheduling and execution.
  - (c) System operation.
  - (d) Database administration.
- (2) Managing installation computer networks, including—
  - (a) Local area networks.
  - (b) Gateways to communications service.
  - (c) System administration of common-user systems such as e-mail.
  - (d) Connectivity with DA systems.
- (3) System analysis and programming support for system development, including—
  - (a) Assisting in performing feasibility studies and developing cost/benefit analyses.
  - (b) Systems analysis.
  - (c) System design.
  - (d) System development.
  - (e) Programming.
  - (f) System test.
  - (g) System documentation.
- (4) Assisting users in procuring support if DOIM resources are unavailable.
- (5) Security guidelines.

*c. Systems support coordination.* In providing support, DOIMs focus on integration and standardization that brings efficiencies to operations and customer satisfaction. DOIMs support the installation of standard Army systems or other externally developed systems to be used at the installation, including—

- (1) Providing site preparation guidance for incoming equipment.
- (2) Participating in acceptance testing.
- (3) Integrating new systems into existing installation architecture.

*d. Standardization.* Standardization of the office automation environment across the Army and across each installation provides the Army with major economies of scale, ease of maintenance, and cost avoidance in several areas. Soldiers and civilians trained and experienced on a common suite of office automation products do not need costly retraining when moving to new duty stations. Performance is maximized as learning curves are minimized. Commonality of office automation products ensures that outputs are easily shared between MACOMs and installations without conversion, data loss, or re-keying. Army DOIMs must adhere to a common office automation product set in their service areas, as DOIM funding, help-desk training, and other resources cannot support multiple product lines. Army- or DOD-wide contracts should be the first consideration when obtaining standard office automation software, hardware, and services. Users are required to procure, maintain, and fully support such products within their own resources, subject to all requirements to register software, prevent software piracy, maintain security, and so on.

### **9-3. Technical documentation**

*a.* Documentation is the process of recording information produced by a software/information system life cycle process or activity. Documentation should be tailored according to the complexity of the system or software. (For availability of COTS documentation, check the license or contact the software distributor.)

*b.* The documentation process consists of a set of activities that plan, design, develop, produce, edit, distribute, and maintain documents needed by managers, engineers, and users of the system or software product. The documentation activities are implementation, design and development, production, and maintenance.

*c.* Electronic information generated by, or contained in, an information system is considered a record. R 25-400-2 provides record keeping guidance on retention standards and documentation requirements. The disposition of electronic records is determined as early as possible in the life cycle of the system. The functional value and program needs of electronic records determine the retention period. All electronic records are accompanied by documentation sufficient to ensure that the information is accessible and usable. Minimum documentation consists of identification of the software programs and operating systems used to create the documents to the extent that the technical specifications, file arrangement, contents, coding, and disposition requirements of the files can be determined. Software and system documentation are maintained for as long as the related information is retained.

*d.* Preparation considerations include the following element:

- (1) Ease of use. Documentation is prepared for the average reading skill level of the intended audience per AR

25–30. Functional user documentation should be written in terms clear to functional area specialists rather than computer specialists.

(2) Mission-essential requirements. Conditions such as war, exercises, mobilization, and civil defense emergencies may affect system processing. Documentation should reflect these variables.

(3) Classification markings. The applicable classification should be clearly marked on each documentation unit.

*e.* ISO/IEC 12207: 1995 is an international standard adopted for use by DOD. It replaced MIL–STD–498 as the DOD standard for software documentation. ISO/IEC 12207 establishes a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry. It contains processes, activities, and tasks to be applied during the acquisition of systems containing software, a stand-alone software product, and software services. It applies to the supply, development, operation, and maintenance of software products. Software includes the software portion of firmware. This standard provides a process for defining, controlling, and improving software life-cycle processes. The Institute of Electrical and Electronic Engineers and the Electronic Industries Association (IEEE/EIA) 12207 is the U.S. implementation of ISO/IEC 12207. It consists of three parts:

(1) IEEE/EIA 12207.0–1996 provides a basis for software practices that would be usable for both national and international business.

(2) IEEE/EIA 12207.1 provides guidance on life cycle data from the processes of 12207.0. It describes the relationship among the content of the life cycle data information items, references to documentation of life-cycle data in 12207.0, and sources of detailed software product information.

(3) IEEE/EIA 12207.2 summarizes the best practices of the software industry in the context of the process structure provided by ISO/IEC 12207.

#### **9–4. Server consolidation**

*a.* Army is focusing on server consolidation to yield numerous benefits including reduced total cost of ownership, more simple and manageable operations, a more secure network, increased capacity, and better system reliability and availability. The replacement of many small servers with fewer, larger, centrally managed servers encourages standardization on operating systems, server platforms, applications, and databases.

*b.* The Army must also reduce servers to provide for reinvestment of recovered dollars into higher priority IT requirements.

*c.* To that end, DOIMs are initiating plans for consolidating servers in coordination with tenant activities for review by RCIOs. The DOIMs on each post are consolidating servers for Army tenants residing on the post to a minimum number of server locations. The only activities exempt from consolidating servers within DOIM facilities are those agencies that are defense funded and support other federal agencies or joint commands (Corps of Engineers, Intelligence and Security Command, Medical Command, Special Operations Command, Space and Missile Defense Command, Military Surface Deployment and Distribution Command) to include deployable assets, nonappropriated fund activities, and tenant organizations receiving processing services from another centralized location (USAR, NGB). These activities may elect to obtain IT services from the local DOIMs on a reimbursable basis. These activities are required to consolidate their IT assets within their server locations under the technical control of NETCOM, follow the Army's network security policies, coordinate active directory implementation with NETCOM, and report server baseline data and consolidation status to their servicing DOIM.

*d.* HQDA functional proponents and MACOMs assist the DOIM in consolidating servers to those server cluster locations specified by the DOIM. DOIMs coordinate with their Installation Commander and Army tenants to develop the requisite Memorandums of Agreement to provide the resources needed to support server consolidation.

*e.* In accordance with the Server Consolidation Guidance document under AKM Goal 3, DOIMs baseline and report quarterly consolidation status for all unclassified server assets for all Army tenants residing on or satellite off the installation, including exempt activities. Status of server consolidation is reported to senior Army leadership on an as-required basis through the Army CIO Executive Board and the Strategic Readiness System. It is vital that DOIMs monitor and report savings achieved through server consolidation as a means to measure success.

*f.* When developing server consolidation plans, DOIMs should consider continuity of operations, network access, and facility improvements (for example, backup power, heating, ventilation, air conditioning, and storage) required for enhanced system availability and reliability. The DOIM may designate other server cluster locations to accommodate floor space limitations. To assist DOIMs, the PEO for Enterprise Information Systems, in coordination with NETCOM, has established a core team, known as the Enterprise Business Integration Center, to develop, engineer, and implement server consolidation plans on a reimbursable basis.

*g.* The scope of consolidation includes all server systems at Army locations except classified and tactical/deployable assets. However, the DOIM should consolidate classified servers to the maximum extent possible without impacting operational missions or national security. In the interest of obtaining immediate results, initial efforts should harvest benefits from server systems supporting e-mail, file, print, and Web services that can be most conveniently consolidated. Consolidation of servers supporting applications may need to be deferred if these assets require re-accreditation or re-engineering of system(s) or network(s).

## **9-5. Document management**

a. Document management is computerized management of electronic and paper-based documents. Document management systems generally include the following components:

- (1) An optical scanner and optical character reader to convert paper documents into an electronic form.
- (2) A database system to organized stored documents.
- (3) A search mechanism to quickly find specific documents.

b. Document management systems are becoming more important as it becomes more obvious that the paperless office is an ideal that may not be achieved. Instead, document management systems strive to create systems able to handle paper and electronic documents together. A good Document management system—

- (1) Is compatible with company and computer industry standards
- (2) Is scaleable over the entire company and its range of applications.
- (3) Provides search facilities, based on categorization, content or metadata (information such as document descriptions, keywords, purpose, scope, and so on).
- (4) Controls "check in" and "check out" for document creation and review.
- (5) Provides standard versioning.
- (6) Is usable by all networked workgroup employees.
- (7) Provides configurable, multilevel security.

c. The services required include support for document creation, storage, retrieval, tracking, and administration in an organization. By providing these services, users are able to efficiently retrieve the information required to support their processes.

(1) The process for documents outlines the flow of working draft copy documents from submission to final storage. This process varies slightly from the final document process. All documents for storage are submitted in soft copy form for control and sent via e-mail.

(2) All working draft copies of document must be marked DRAFT.

(3) Before storing the document, entering the documents into the database, and submitting the document, the administrator assigns the identification of a document.

(4) After documents are created, services are needed that eliminate the burden on individuals to determine where they should be stored. Automated routines are needed that determine the specific location to store the document. This is similar to determining in which file and file cabinet to physically store the document. It should be the function of the individual to do this. They should determine the location based on specific information about the document such as the individual creating the document, the content of the document, and the business process it supports.

(5) A vital aspect of document management is making all documents secure from unauthorized access. Each document varies in the type of security required. Document management services that provide mechanisms for assigning a variety of access rights to each document are needed. The release document is placed under "locked" document control. Copies of this document may be issued, but at no time is the master copy allowed outside of the document repository physical control. A second "locked" document is also created for storage at an off-site facility.

(6) All working draft documents are entered into the database archive. Previous version(s) of a document have a change document created between the two indicating the changes made. On previous versions, the change document and the current version of a document are posted. Older versions are archived in storage (both on and off site).

## **9-6. Electronic signatures**

a. An electronic signature is an electronic sound, symbol, or process attached to a record by a person with the intent to sign the record.

(1) Electronic signatures are generally divided into two categories: digital signatures and electronic signatures. The primary distinction between the two is the presence or absence of public key cryptography.

(2) Digital signatures are the most secure electronic signatures because of asymmetric key pairs used within a PKI. PKI allows strong user authentication, maintains data integrity, and aids nonrepudiation .

(3) Digital signature capabilities are required to meet legislative and DOD policy mandates for non-repudiation, e-commerce, and paperless processing requirements.

(4) Visibility and recognition of these requirements become more evident to senior leaders as PKI deployments provide new digital signature capabilities for messaging and use of digital signatures in support of manual business processes is viewed as the next logical step.

(5) Through adoption of Electronic Document Interchanges, XML, and Web-based business processes, Government and industry widely recognize the value of electronic signatures.

(6) Requirements for handwritten signatures often represent the largest delay in an otherwise automated or electronic system.

(7) To support migration to a paperless office, the U.S. Government acknowledged the importance of electronic signatures with the Government Paperwork Elimination Act. This act requires agencies to provide for the use and

acceptance of electronic signatures. Common access card and PKI provide a valuable framework for the paperless office.

(8) An enterprise solution is needed to aid the Public Key Enabling of applications requiring digital signatures and derive the benefits of this infrastructure.

*b.* The Army is working toward an enterprise form and digital signature solution that is fully interoperable. The following Army digital signature specifications using the term (document) refer to any such form of electron media to include but not limited to word processing documents, data elements, objects, images, and forms.

(1) The solution allows the recipient to verify the identity of the signer.

(2) The solution allows the recipient to verify the certificate used to sign.

(3) The solution supports network-supplied trusted time stamping or synchronized time stamping.

(4) The solution allows for multiple signing of documents with the ability for signatures to be invalidated if the document is modified after signing (unless document requires sectional signing).

(5) The solution is able to include sectional signing and a hierarchical approval chain.

(6) Based on the business process, the solution prevents persons from changing information within a specific section after that section has been signed.

(7) The solution shows invalid digital signatures and allows for removing invalid signatures only by the person whose signature it represents.

(8) The solution can sign forms that depend on multiple signatures as well as sectional signing to accomplish approval of the document.

(9) The solution is able to support digitized signatures.

(10) The solution offers a template for selecting data elements needing a digital signature in a form.

(11) The use of the digital signature is protected by DOD PKI security measures (for example, personal identification number or password for the common access card, identification key, and soft certificates).

(12) The solution provides an application programming interface and software development kits to work with third-party security solutions.

(13) The solution complies with DOD regulations about the use of mobile code.

(14) The solution offers a feature to store digital signatures in a secure storage area, such as a database or file system.

(15) Digital signature storage requirements do not significantly increase the storage requirements of the application.

(16) The solution offers secure storage of information needed to revalidate digital signatures.

(17) The solution allows for administrator customization.

(18) The Army identified XML based signatures as one of the mandatory requirements.

(19) The solution provides a Web-based capability and a desktop application capability.

*c.* The point of contact for electronic signatures is Army CAC/PKI Programs, NETCOM Information Assurance Directorate.

## **9-7. Army information technology registry management and user principles and procedures**

*a.* The AITR is the Army's single, definitive registry of IT systems. The AITR provides data on—

(1) The inventory of Army systems/applications.

(2) Current status of webification.

(3) System milestones for reduction/webification.

(4) Tracking of Federal Information Security Management Act data.

(5) Privacy impact assessment data.

(6) Accreditation information.

*b.* The AITR supports IM/IT resource management and business/functional process improvement efforts, provides input to the SRS, and compiles information for Federal Information Security Act status reports to OMB and Congress. Privacy impact assessment fields are included as they are required by the provisions in OMB Memorandum dated 26 September 2003. The following is the process associated with adding, deleting, and editing systems within the AITR.

(1) CIO/G-6 Governance Division maintains oversight and management for the online AITR.

(2) Each MACOM and HQDA proponent assigns a single POC for all systems within area of authority; POCs manage the listed systems in AITR for their organization.

(3) Systems and applications should be added to the AITR if they meet the definition of a system, are owned by your organization, and are not already in the AITR. To add a new system, send an e-mail containing the information identified in 9-7b(6) to the MACOM/HQDA POC. The MACOM/HQDA POC reviews requests and, if approved, creates a record in the AITR. Before adding new systems, the MACOM/HQDA POC checks the AITR to determine whether the proposed system is already in the AITR. Descriptions for each of the fields in the AITR are described in system documentation available on the AKO linked AITR Web site.

(4) MACOM/HQDA POCs or an appointed representative can edit basic record information.

- (5) POCs can directly edit the fields identified in 9-7b(6) for those AITR records assigned to them.
- (6) The following are POC editable application fields:
- (a) System name.
  - (b) System acronym.
  - (c) System description.
  - (d) Acquisition category.
  - (e) Functional area.
  - (f) Secondary functional area.
  - (g) Tertiary functional area.
  - (h) Project manager.
  - (i) PM title.
  - (j) PM organization.
  - (k) PM commercial phone.
  - (l) PM DSN phone.
  - (m) PM e-mail.
  - (n) Budget initiative number.
  - (o) Interfaces identified.
  - (p) Contingency plan.
- (7) All requests to register a system in AITR must include the following information:
- (a) Owning MACOM.
  - (b) System name.
  - (c) System acronym.
  - (d) System AITR ID number.
  - (e) Primary functional area.
  - (f) (Add the fact that you want to change mission criticality from (specify current criticality) to (specify desired criticality)).
- (8) Requests to change mission criticality are coordinated with and approved by the functional proponent (the AITR POC from the functional proponent can provide this prior to submission to the AITR help desk). Requests for change should be e-mailed to appropriate MACOM/DA staff AITR POC for coordination with the functional proponent. The MACOM/DA staff AITR POC e-mails the coordinated response from the functional proponent to the AITR help desk for execution (aitr.help@us.army.mil). Table 9-1 contains the list of functional proponents.

**Table 9-1**  
**Table of functional proponents**

Functional areas	Proponent
Allies	G-3
Chemical, biological, radiological, and nuclear and high explosive	G-3
Civilian personnel and readiness	ASA(M&RA)
Command and control	G-3
Communications	CIO/G-6
Communications security	CIO/G-6
Economic	ASA(FM&C)
Environmental security	ASA(I&E)
Facilities	ACSIM
Finance	ASA(FM&C)
Health/medical	OTSG/MEDCOM
Human resources	ASA(M&RA)
Information management	CIO/G-6
Inspector general	DAIG
Intelligence	G-2
Legal	OTJAG

**Table 9-1**  
**Table of functional proponents—Continued**

Functional areas	Proponent
Logistics	G-4
Military personnel and readiness	G-1
Nuclear	G-3
Nuclear, chemical, biological operations	G-3
Operations	G-3
Personnel and readiness	G-1
Procurement/acquisition	ASA(ALT)
Reserve Components	OCAR or DANG (depending on system ownership)
Scientific and engineering	ASA(ALT)
Space and weather	G-2
Test and evaluation	DUSA-OR
Trainers	G-3
Transportation	G-4
Weapons	G-3
N/A	CIO/G-6

(9) Requests for webification exemptions. System POCs and MACOM/DA POCs can enter initial projected webification dates into AITR themselves. Once the information has been initially entered, CIO/G-6 needs to be involved to change those dates. Secretary of the Army and CSA guidance is to webify all systems. Waivers are not automatic. Waiver requests must support the AKM vision and clearly explain why a system should be exempt from the webification mandate.

(a) MACOM/DA staff sections must review webification requests and state whether their CIO/IMO supports the request. CIO/G-6 expects the MACOM/DA staff section to review the request, not just forward all requests to CIO/G-6 for judgment.

(b) Each request for an exemption should be in a separate e-mail, so it may be routed to the appropriate staffers.

(c) The title of the e-mail should read, “Webification Exemption Request for (insert system acronym and AITR ID # here)” or “Projected Webification Change Request for (insert system acronym and AITR ID # here)” as appropriate. The e-mail will be sent to the AITR help desk for execution; the appropriate CIO/G-6 approval authority will then be contacted (see table 9-2 for information to include when requesting a webification exemption). In addition to 9-7b(7), one should—

1. Indicated need for a webification exemption or a projected webification change.
2. Indicate reason for the exemption or change in projected webification dates. This should be one or more of the reasons from table 9-2.

**Table 9-2**  
**Addition information required when submitting for webification exemption**

If your reason for exemption is—	Then submit—
System is being retired	Name and AITR ID Number of system replacing the retiring system (if replacing system is not Army owned, list owning agency instead of the AITR ID number. Include the date the system will be retired.
System processes data at the Top Secret or higher level	No additional data needed.
System cannot be webified because of insurmountable technical challenges	Describe the challenges, and why your analysis proves them to be insurmountable.
System is a database that has no user interface; it merely collects data from other applications and databases and shares this data with other applications and databases.	Describe what the system does. List the systems (with AITR ID numbers) that this system pulls data from or provides data to. If these are not Army systems, state the owner instead of the AITR ID number.

**Table 9-2**  
**Addition information required when submitting for webification exemption—Continued**

If your reason for exemption is—	Then submit—
System is not worth webifying from a cost/benefit standpoint	Submit the business case as to why webification is not justified. Remember, the waiver authority has no knowledge of your system, so make sure your business case is complete. If the issue is financial, include all the numbers that make your case.
Other reasons (specify)	Provide all details necessary to make your case.

(d) CIO/G-6 needs to review these actions. Initiate request by sending e-mail to appropriate MACOM/DA staff POC. The MACOM/DA forwards e-mail to the AITR help desk for execution once information is coordinated. The following guidance is to be followed when requesting a change:

1. Each request for a change should be in a separate e-mail, so it may be routed to the appropriate staffers.
2. The title of the e-mail should read “Completed Webification Change Request (insert system acronym and AITR ID # here)” or “Revision to Webification Exemption Request” as appropriate.
3. In addition to the requirements listed in 9-7b(7), the e-mail should—
  - a. Add what is required, Completed Webification Change or a Revision to Webification Exemption (that is, a previously exempt system can now be webified) as appropriate.
  - b. Add the reason for change.
  - c. Include MACOM concurrence and comments. State why CIO/IMO concurs with the request.
  - c. System records are maintained by the owning organization. When the owner of an AITR system record determines another organization should own the record, send an e-mail in the format listed below to the current owning MACOM POC. The MACOM POC endorses the request and forwards it to the MACOM POC at the organization identified to gain the system record. The gaining organization considers and responds to the request by e-mail to the requesting MACOM. Once concurrence is reached, the MACOM POC from the losing organization e-mails the AITR help desk with the concurrence. There can be only one owner. If it is funded, fielded, and maintained by a MACOM/DA staff agency, it belongs to that MACOM/DA staff agency. If it is a DOD system, it does not belong to any Army MACOM/DA staff agency. If multiple organizations fund a system, they must determine the “lead,” which becomes the owner. To transfer a system, submit the e-mail in the following format:
    - (1) The title of the e-mail should read, “System Transfer Request (insert system acronym and AITR ID # here)”
    - (2) In addition to the requirements listed in 9-7b(6), the body of the e-mail should add the fact that you want to transfer the record
  - d. Systems should be deleted when they are no longer in use anywhere in the Army. Systems that are being transferred to another MACOM need to follow the transfer procedures in Section 9-7c. Send an e-mail in the format listed below to appropriate MACOM POC. The MACOM POC endorses the request and forwards it to the AITR help desk, which submits it to the CIO/G-6; if approved, the system is deleted.
    - (1) The title of the e-mail should read “System Deletion Request (insert system acronym and AITR ID # here)”
    - (2) In addition to the requirements listed in 9-7b(6), the body of the e-mail should contain the reason for the deletion. This should be one or more of the following (use these exact words):
      - (a) System has been retired. The replacement system is (specify system name and, if an Army owned system, AITR ID#, and include the retirement date).
      - (b) System is a duplicate record (specify system name, owning MACOM, and AITR ID# of system that will remain in AITR).
      - (c) System is not owned by Army (specify name and point of contact of organization that owns the system).
      - (d) System does not meet definition of an information system (specify).
      - (e) Other reasons (specify).
    - e. AITR data are uploaded quarterly to the DOD IT Registry. The Army CIO/G-6 certifies the uploaded data every year by 15 July. Certification is accomplished in two parts. The functional proponent certifies the importance of the system and the owning MACOM/DA staff agency certifies the accuracy and completeness of the data.
    - f. To determine what is in the DOD IT Registry, contact the AITR help desk with the name and acronym of a system and they will query the DOD IT Registry and provide a report.

## Chapter 10 Telecommunications

### 10-1. Network systems

#### *a. LAN/WAN.*

(1) Per AR 25-1, paragraph 6-1, the DOIM plans and manages WAN equipment on the local installation and integrates installation LAN resources into the installation, Army, and DOD plans and standards.

(2) The DOIM advises user organizations about procurement of LAN equipment.

(3) If an organization opts to engineer, furnish, install, and maintain LAN equipment on their own, that organization is required to obtain interface verification from the installation DOIM to access the installation WAN.

(4) Waivers against using the DOIM's installation infrastructure must be coordinated with the supported tenants to the NETCOM/Enterprise System Technology Activity.

(5) If an existing requirements contract is available, the LAN system or service is obtained from that contract to the maximum extent viable. If a requirements contract is unavailable, the DOIM must give data to support a competitive procurement.

(6) See the PM-Defense Communications and Army Switched Systems (PM-DCASS) Web site at <http://www.eis-army.mil/dcass> for information on LAN/WAN installation, SOPs, and component information in CONUS installations.

#### *b. Wireless LANS.*

(1) Wireless LAN (WLAN) may be used as an extension of the departmental LAN (DLAN) or the common user installation transport network (CUITN) where fixed infrastructure connectivity is unavailable. A 10BaseT patch cable to the DLAN hub or the CUITN area distribution node router provides the interface.

(2) Standard interfaces for WLANs are IEEE 802 series. WLANs operate in the 2.4 to 2.484 GHz and 5.743 to 5.830 GHz range. Operating WLANs in the above GHz range requires no Federal Communications Commission license.

(3) DOIMs analyze user needs to spot possible WLAN applications and help user organizations request WLAN equipment needed to meet requirements.

(4) Wireless networks needing remote or local access to the NIPRNET submit their requirement through the NIPRNET connection approval process.

(5) See the PM-DCASS Wireless Working Group knowledge center on the AKO Web site at [www.us.army.mil/suite/folder/1072442](http://www.us.army.mil/suite/folder/1072442) for information on WLAN installation, SOPs, and component information in CONUS installations.

#### *c. Internet access via Terminal Server Access Control System (TSACS).*

(1) TSACS gives remote access for authenticated Army users to their e-mail accounts and allows access to the Internet as needed for conducting official Government business. TSACS uses authentication servers, dial-in servers, and user IDs and passwords to prevent nonauthorized access to the IP router network. Dial-in service is given through local terminal servers or over remote 1-800 service.

(2) Army MACOMs must migrate unclassified dial-in connections to TSACS to prevent unauthorized access to NIPRNET. TSACS gives Army authorized users global access to local servers that give them the ability to read their e-mail and send data over NIPRNET. NIPRNET can handle data up to unclassified but sensitive.

(3) The installation DOIM, or designated official, appoints a service provider who issues Army personnel a valid user ID and password via the TSACS Web page ([www.tsacs.army.mil](http://www.tsacs.army.mil)). Once the process is complete, the user may dial into TSACS and access e-mail servers via NIPRNET. Questions may be sent to the NETCOM/9th Army Signal Command (9th ASC), U.S. Army Networks, Engineering and Telecommunications Activity, Army Networks and Systems Operation Center help desk at 1-800-305-3036; commercial 520-538-6798/6858. TSACS phone numbers and OCONUS numbers may be obtained from the TSACS Web.

(a) Some OCONUS numbers are not published because of other considerations and may be obtained from the local DOIM when in country. Whenever possible, the Army user should first dial into TSACS by using a local phone number and then enter the user ID and password. Local dial-in access incurs no extra phone charges to the Army.

(b) TSACS access may also be accomplished by dialing the 1-800 service. The 1-800 number is available for CONUS access and may be obtained from the installation service provider.

(4) DOIMs and service providers help to better manage the dial-in access by—

(a) Advising TSACS users that the 1-800 service should be used as a last resort.

(b) Obtaining local dial-in access numbers for TDY locations before going TDY. Access numbers for locations visited may often may be programmed into a laptop.

(c) Helping users in setting up a laptop computer to limit online time. The laptop may be set up to first view e-mail headers so users select ones to download. Messages are worked off-line and users re-log on to send responses.

(5) Exceptions to this are those approved community of interest networks and non-Army enterprise information structure system or network operating as an isolated enclave to the installation network.

## 10-2. Network operations

a. NETOPS are the operation and management of the LandWarNet (LWN). LWN is the combination of infrastructure and services across the Army. It provides for processing, storing, and transporting information over a seamless network. NETOPS are the organizations, procedures, and technologies needed to monitor, manage, coordinate, and control the LWN as the Army part of the GIG (the organizing and transforming construct for managing information technology (IT) throughout the DOD). Single-authority operation and management of the LWN offer better capabilities and services to constituencies. These capabilities are implemented over time, but the vision establishes a target set of capabilities so the organizational, procedural, and technical changes needed to achieve them can be planned and coordinated.

b. NETOPS ensure information dominance and enable command speed for warfighters and establish a technical framework to create a network common operational picture (NETCOP). Figure 10-1 shows NETOPS mission areas and functions. NETOPS give IT situation awareness, protect information flow, and integrate service and network management, IA, and integrated data management.

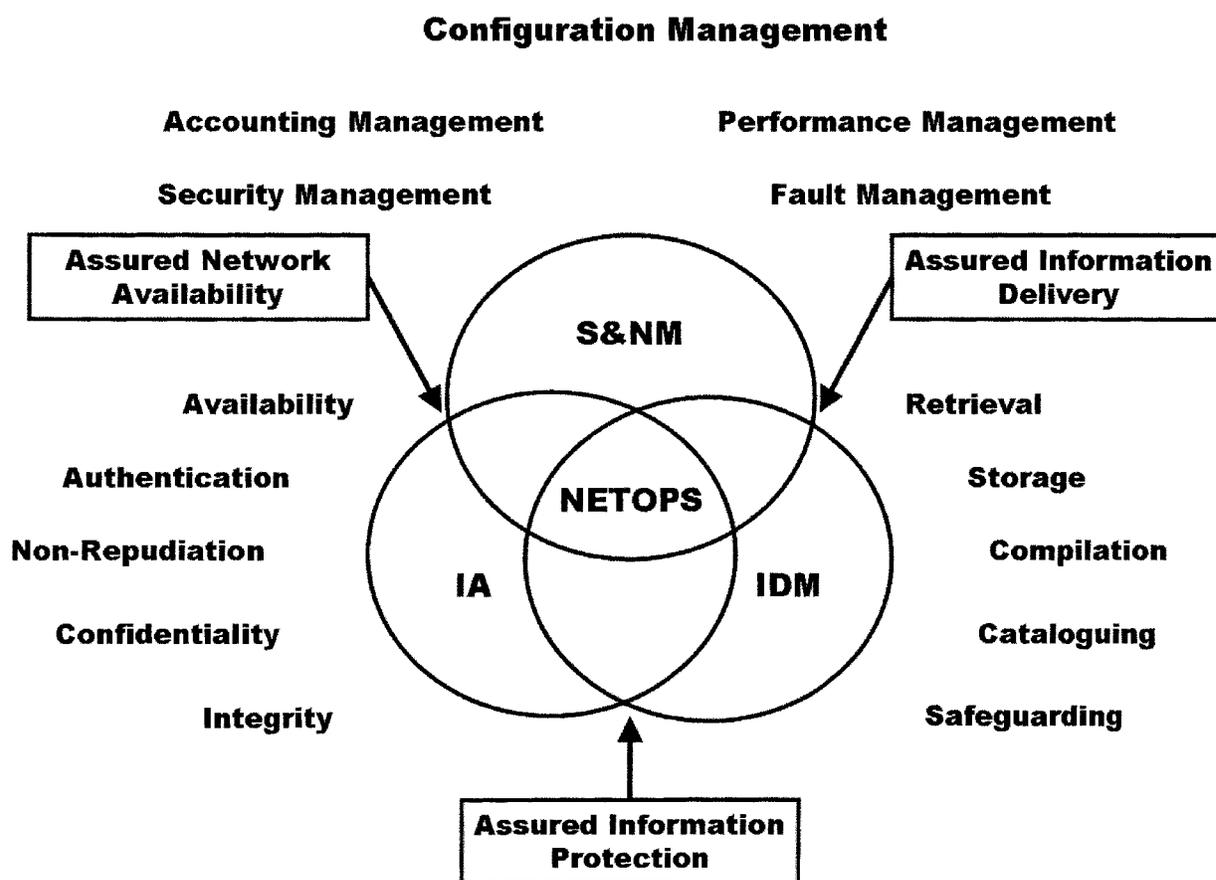


Figure 10-1. NETOPS mission areas and function

---

c. The objective state for Army NETOPS capabilities should result in the provision of the following key capabilities:

- (1) Enable universal secure access to official information structure services to Army customers within the Army information structure in order to secure single sign-on plug-and-play capability.
- (2) Correctly show total and integrated situation awareness of the LWN.
- (3) Expect impacts on LWN of varying systems and operational contingencies.
- (4) Redirect and reallocate LWN resources in near real-time to support Army response to crisis anywhere in the Army information structure operational area (AOR).

(5) Provide a consistent and robust level of information structure services to authorized Army customers as economically as possible in Army operational constraints.

(6) Provide above base level information structure services to Army customers on a reimbursable basis.

(7) Perform continuing and non-intrusive technology insertion to improve service levels and reduce cost of providing current base-level services.

(8) Provide continuity of operations plan capabilities.

(9) To achieve this objective state, the Army must streamline the operations and management of its information structure. The goal is to maximize standardization and consolidation of information structure operations, based on the three-fold criteria of operational support to the warfighter, technical viability, and cost effectiveness.

(10) The standardization and consolidation of NETOPS functions across the enterprise allow the Army to better utilize personnel needed to perform these tasks and increase the quality of service provided to the end-users while at the same time reducing the total cost of providing this service.

(11) Another goal of NETOPS is to move the Army toward an installation environment as close as possible to the implementation of the most efficient and effective Army enterprise operation for IT and its applications. NETCOM has a TNOSC supporting each Army theater AOR, to include one in CONUS.

(12) NETOPS are capabilities that enable assured network availability, information protection, and information delivery to ensure the warfighters have critical information resources needed to accomplish their missions.

d. The Joint NETOPS concept of operations directs each service to develop and spread a NETCOP for their part of the GIG.

(1) NETCOP offers the ability for combatant commanders, service components, subunified commands, joint task forces, and deployed forces to rapidly identify outages and degradations, network attacks, mission impacts, C4 shortfalls, operational requirements, and problem resolutions at the strategic, operational, and tactical levels.

(2) The Army NETCOP is an integrated capability that receives, correlates, and displays a view of voice, video, and data telecommunications networks, systems, and applications at the installation/tactical, region, theater, and global levels through the installations/deployed tactical forces, network service centers, TNOSC, and the Army network operations and security centers, respectively.

(3) Coordination with DISA provides agreement on the information passed between DISA and other agencies. Agreements are made for information to be pushed throughout Army network operations and security centers from that and other Army enterprise requirements. At each level, the required “push” data are collected for analysis along with other required data at that level (see fig 10–2, which shows an example of NETOPS CONOPS). The NETCOP at each level reflects status, performance, and IA. At a minimum, the NETCOP includes telecommunication/system/application fault and performance status as well as significant information assurance reports such as network intrusions or attacks.

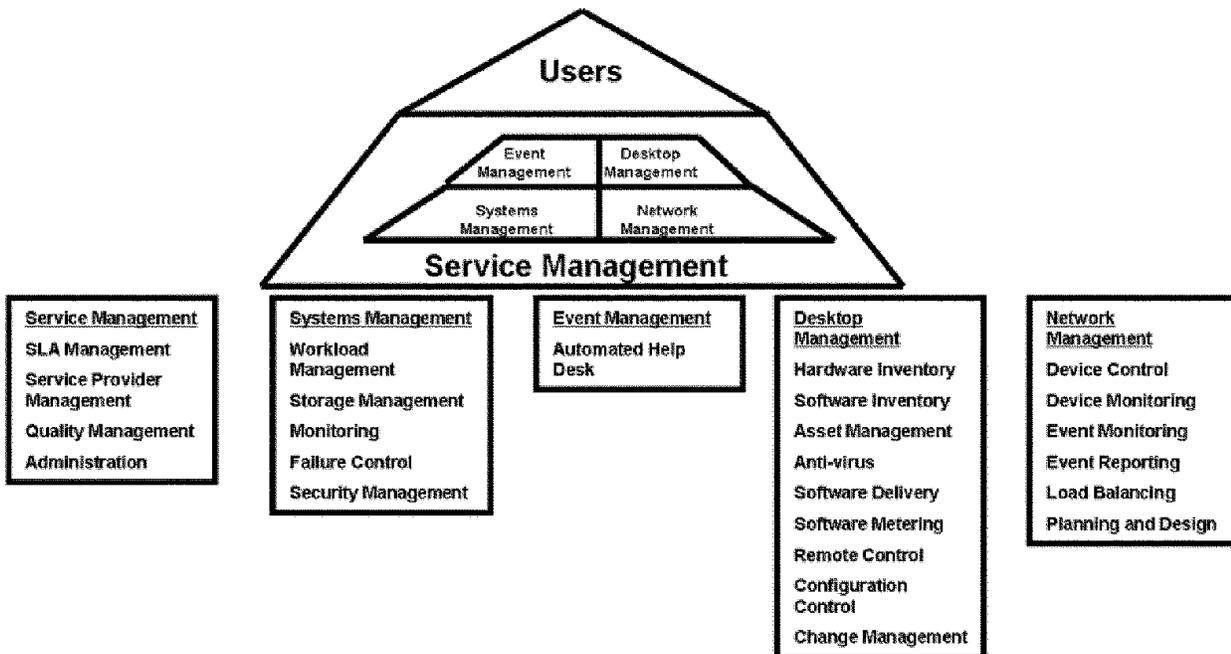


Figure 10–2. Information management services

e. The tactical portion of the LWN extends from Army component commanders to deployed forces supporting a joint, combined, or single-service task force. Deployed forces will access reach-back applications through a standardized entry point or teleport site.

(1) NETCOM, through its Army Theater Signal Command, supervises the operation and maintenance of the Army's portion of the GIG in theater.

(2) In theater, the GIG is composed of enclaves of service-controlled assets connected by a network of DISA-controlled assets. The complex nature of the GIG in theater requires that component NETOPS organizations work together closely, under the direction of the J-6 to ensure reliable operation of the GIG. NETCOM, through the Army network operations and security centers, will operate and manage the Army's cross-theater C4/IT support to various warfighter commands.

f. Authority for operation and management of functional applications—such as personnel, logistics, financial, training, and medical—remains with their functional owner for the near-term. The long-term vision is to separate the link between application management and the management of the underlying networks and processing systems. The functional owner is monitors applications and content management while NETCOM provides the communications and processing services necessary to meet the functional owner's service requirements.

g. Some of the biggest changes resulting from LWN transformation are in end-user support. The objective is to standardize and centralize to the maximum extent possible, resulting overall in more effective service and reduced total cost of ownership. The Army baseline service levels are validated by the LWN Management Steering Group and approved by the Army CIO/G-6 and the ACSIM. Services provided to the end user include—

- (1) Standardized, consistent services for end-user devices (desktop, laptop, and so on) and software applications.
- (2) End user devices delivered with pre-installed software.
- (3) Remote desktop software upgrades and patches.
- (4) Virtual desk side assistance (remote, real-time problem finding and resolution).
- (5) Single account/logon using PKI/CAC.
- (6) Single, integrated help desk or "one-stop" problem reporting and resolution.

h. Infostructure management focus areas are identified to highlight key concepts of the new AKM paradigm needed to achieve the Goal 3 vision and effectively manage the LWN as an enterprise. A high-level description of each area is provided below.

i. The CM process covers all aspects of the infostructure configuration. The Army controls introduction of new services and functionality to the end-user community without disrupting existing services by the process. CM is also the process required to ensure compliance with operating and security policy.

(1) The LWN Technical Configuration Control Board is the primary organizational entry point into the process. NETCOM, in conjunction with the LWN Technical Configuration Control Board, will manage the configuration process.

(2) The CM process solicits input from the users and allows the supporting organizations to glean the best of these items.

j. The service-level management (SLM) process defines, delivers, measures, and improves C4/IT services. The SLM process is expected to become the cornerstone of how the Army operates and manages the information structure to deliver quality IM and telecommunications services. Figure 10-3 depicts the process model for developing and modifying baseline service levels and SLA extensions to baseline services.

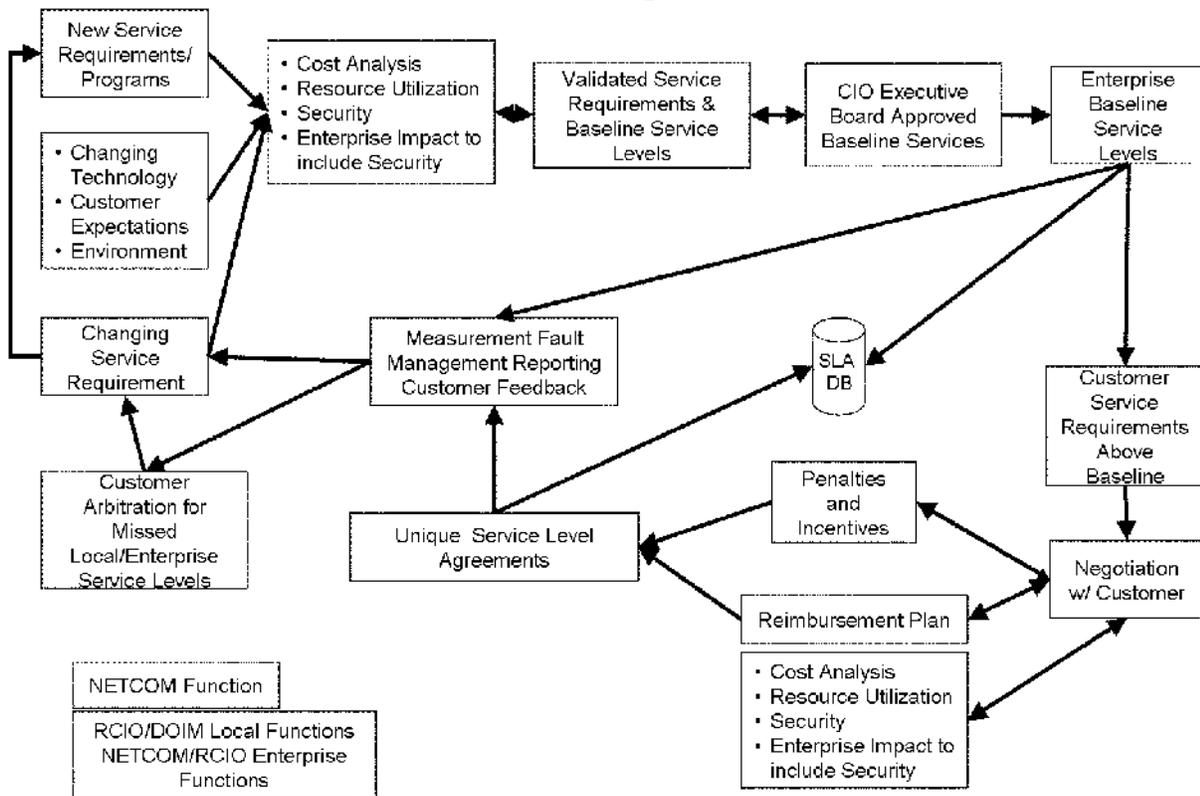


Figure 10-3. Service-level management process

k. AR 25-1, paragraph 6-3g, requires a "Networthiness Certification" process that identifies and continually refines required support for a C4/IT system, particularly in the areas of supportability, interoperability, sustainability, and security. The process ensures that a C4/IT system does not adversely impact the network and that it is sustainable through its lifecycle.

l. In order to effectively manage the information structure as an enterprise, reduce total cost of ownership, and optimize return on investment, the Army has to identify and control its assets.

(1) Asset and Resource Management (ARM) touches most of the enterprise. These assets include physical property as well as nonphysical (logical) property. Physical property is an item that can be touched, such as a computer, a hub, or a gateway. Logical property is much less obvious because it is represented by symbols such as numbers, names, and time. IP addresses, domain name space, directory name space, processes, procedures, unused central processing unit time, and unused bandwidth are all examples of logical property.

(2) The ARM process defines how both physical and logical property items are cataloged in terms of identification and use. The ARM process supports the identification of duplicative systems and their subsequent elimination by integrating the functionality and the data into a common system. The ARM process is complementary to the CM and SLM processes but includes nonconfiguration items and is focused on the accurate representation and use of property.

(3) The identification of physical property is performed using enterprise system management tools. If duplicate property management systems exist, their data and functionality are migrated to a common system that meets all user functions. Information structure unique property accountability requirements will be included in the requirements for the Army's standardized property tracking and accounting systems.

(4) There is no standard method for identifying all types of logical property, although national (and international) standards and methods exist for some types of logical property (for example, internet protocol addresses, domain name space). A key part of the ARM process is to address this lack for logical property and to develop an accepted methodology to accurately represent the characteristics of logical property.

(5) The usage portion of the ARM process defines how information structure items are utilized. The first task is to track usage. Usage is generally expressed as a percentage of some estimated capacity to perform work (for example,

central processing unit (CPU) utilization). Other key usage components are the tasks, processes, and procedures and organizational missions an item supports.

(6) A main goal of the ARM process is to understand how efficiently and effectively the information structure is operating. This benchmark can then be monitored for improvement as efficiency initiatives are begun and completed. The difficulty for the ARM process is that the whole information structure cannot be realistically assessed in this manner. However, limited segments (for example, the server and application consolidation effort) can be assessed using this method to demonstrate the feasibility of a given infrastructure change on the operations and maintenance cost of the information structure.

(7) The end result of the ARM process realizes the following objectives:

- (a) Reduce total cost of ownership.
- (b) Provide a measurement system and infrastructure to optimize and leverage investment in the LWN.
- (c) Link basic asset tracking with associated contract, maintenance, and financial information.
- (d) Decrease time spent in the procurement cycle.
- (e) Manage suppliers, charge-back reporting, and audit compliance more effectively.
- (f) Provide accurate decision support for planning, forecasting, and administration.

m. Table 10–1 depicts the mapping of the four levels used in the Joint NETOPS concept of operations to the organizational level names used in this document.

**Table 10–1**  
**Joint to Army levels mapping**

Joint name	Army NETOPS name
Strategic-national level	Global level
Strategic-theater level	Theater level
Operational level	Regional level
Tactical level	Installation level, tactical level

(1) The global level contains organizations that have missions and functions that span all Army elements located around the world. They may or may not be deployed globally; geographic dispersion is not critical to determining the global scope, mission, or impact an organization might have. Most of the organizations contained in the global level are DA staff, MACOMs, major Army funded programs, or DOD organizations.

(2) The theater level refers to large geographic areas. These geographic areas may have a close correlation to a continent or portions of multiple continents. The unified combatant commander supported generally defines the specific geographic area supported. For example, the European Theater is linked to the U.S. European Command that supports most of the European continent and most of the African continent. For the purpose of this document, CONUS is considered a theater.

(3) Organizations defined in the theater level generally have relationships with organizations at both the global and regional levels. The majority of the organizations defined at the theater level have a command relationship with a single organization in the global level. This same organization may or may not have subordinate units in the regional level.

(4) The regional level refers to a geographic area equal to or smaller than a theater. A region is always a component of a theater, but some smaller theaters may only contain a single region. The number of regions contained in a theater is determined by the technical and operational needs of the theater.

(5) The installation level also refers to a geographic area. In many cases, it refers to a single installation; however, it can also refer to many installations located in the same area. The geographic area being referred to at this level is moderately small, frequently the size of a medium-sized U.S. city. It can also be thought of as being synonymous with the phrase "post/camp/station."

(6) Organizations at the institutional level have relationships primarily with the regional level due to the implementation of centralized installation management. This concept is already in place in OCONUS with the Area Support Group structure. With the IMA region and the establishment of a regional director, installations in CONUS are also organized on a regional basis, as the regional director supervises all installations within the assigned geographic region. Organizations at this level may form relationships with organizations at the theater and global levels, but these relationships are far less common than regional relationships.

(7) The tactical level refers to the operational Army—Future Force, stationing of modular brigade combat teams, units of action and units of employment in garrison, and all users deployed away from their home station. This includes users on travel and training and deployed in a CONUS scenario and in an OCONUS scenario.

(8) Many relationship types exist between the organizations depicted in these levels. Many of the relationships are normal Army command relationships. However, the most common relationship type is referred to as cooperative. A cooperative relationship is formed when two or more organizations share some duties to perform some specific portion of a larger mission. This is achieved when all of the tasks defined in the cooperative relationship are performed correctly. This document does not define these tasks, but it defines the relationships and their roles and functions.

(9) Organizations exist within each level. The names of these organizations may change over time, but the functions related to the entities should remain relatively constant. Some of the organizations discussed in this section already exist, but other organizations are still being defined as of the writing of this document. Table 10–2 shows the levels used in this document and the existing and new organizations currently identified on that level. Each of the entities are described in additional detail.

**Table 10–2**  
**Organizational levels to entities mapping**

Level	Entities
Global	DISA global network operations and security center, Army network operations and security centers, DA CIO/G–6, PEO, NETCOM, MACOM, Army Computer Emergency Response Team
Theater	DISA regional network operations and security centers, theater network operations and security centers, regional computer emergency response team, NETCOM RCIO (OCONUS)
Regional	Network Support Center, RD, NETCOM RCIO (CONUS), regional network operations and security centers (Europe)
Installation/tactical	DOIM, supporting signal unit

### 10–3. Local leased base communications services

*a.* Base communications (BASECOM) consist of facilities, equipment, and services used to support the electromagnetic dissemination, transmission or reception of information via voice, data, video integrated telecommunications, wire or radio within the confines of an installation, camp, station, base, installation, headquarters, or a Federal building. This includes local interconnect trunks to the first service commercial central office providing service to the local community and off-premise activity interconnections that are located in the geographical boundary serviced by the first service connecting commercial central office. BASECOM is differentiated from long-haul telecommunications, which are commonly referred to as services that cross the first service commercial carrier’s Local Access and Transport Area (LATA) boundaries.

*b.* BASECOM services encompass the following types: Centrex service, direct in-dial/direct out-dial trunking, 2-way touch-tone, inward flat-rate trunks, flat-rate combination trunks, unlimited flat-rate touch-tone business lines, hunting, integrated service digital network-primary rate interface/basic rate interface access for circuit switched data, calling line identification, multiple directories, forwarding arrangements, foreign exchange trunks, off premise extensions, dedicated intra-LATA circuits, 1.554 megabit channels, digital signal level 3, voice mail, integrated voice/data stations, and intra-LATA tolls, teleconferencing, cellular service, pagers, and so on. This list is not inclusive of every service offered by the local exchange carrier but is intended to serve as a guide of service offerings.

*c.* Local-leased telecommunications services are provided to authorized users based on the best value to the Government, commensurate with mission accomplishment and with adherence to established regulations of the state’s Public Utilities Commission and the FCC. Services can be acquired using a communication service authorization and commercial communication work order, or other contract format, per the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS), as the contractual vehicle. FAR PART 12 is incorporated into solicitations as a preference in order to streamline the acquisition process.

*d.* The U.S. Army Telecommunications Directorate (ATD), NETCOM, administers and manages local leased telecommunications requirements for Army installations and facilities CONUS-wide, including Puerto Rico, under the provisions of the FAR/DFARS. The ATD works closely and directly with the DOIMs’ appointed telecommunications coordinating officers (TCOs) to facilitate the acquisition of local lease telecommunications services. Mailing address and phone numbers for ATD: Commander, U.S. Army Network Enterprise Technology Command/9<sup>th</sup> Army Signal Command, ATTN: NETC–EST–T, 2133 Cushing Street, Fort Huachuca, AZ 85613–7070 DSN 879–8679/7222/8101/8537 or commercial (520) 538–8679/7222/8101/8537.

*e.* Additional information on procedures for acquiring local leased base communication services are contained in the ATD’s BASECOM letter of instruction (LOI). The LOI can be found on the NETCOM/9<sup>th</sup> ASC restricted Web page. Individuals with a need to know can obtain access to the Web page by sending an email to: ato\_automation@hqasc.army.mil.

*f.* Requests for leased commercial phone service are submitted by memorandum or local service request to the installation DOIM. The memorandum or local service request must be reviewed by and have the original signature of

the unit's TCO before submission. User should submit requirements to the DOIM at least 90 days (120 days for 1-800 service) in advance of required service date. This will allow the DOIM to deal with such issues as cable availability and workload management. The DOIM should be advised as soon as a requirement is identified.

(1) If the user needs service such as FTS, calling cards, 800, and so on, it is ordered via the Defense IT Contracting Office (DITCO). The DOIM initiates a request for service on behalf of the customer.

(2) Activities must provide funds for the request.

(3) The following information must be included in the memorandum:

(a) A statement that "Funds are available for this request."

(b) The fund cite from which the monthly bills will be paid and the existing account number to which service is being added or the billing address for new service. It is the function of the requester to perform the funding coordination. Requests received without proper funding will not be processed.

(c) The original signature of the initiating activity's fund certifying officer, to include the phone number, e-mail address, complete mailing address, unit name, office symbol, street, building, room, and stop numbers.

(d) A thorough justification for the requirement.

(e) POC name, phone number, e-mail address, complete mailing address, unit name, office symbol, street, building, room, and stop numbers. POC must be thoroughly familiar with requirement and available to answer any questions.

(f) Service location addresses, including street, building, room, and stop numbers. Furnish a diagram showing exactly where service is to be located in the room or building. Service will be provided according to the diagram. If the address is not a street address or a building number, as frequently occurs in exercise requirements, provide driving directions in simple terminology. If available, reference civilian phone pole or pedestal numbers. A current map, showing major roads and geographical features, should also be submitted with the request. Last-minute changes in desired service location will cause major delays in providing service.

(g) Type of equipment (phone or modem) and any special configuration requirements.

(h) Complete mailing address, unit name, office symbol, street, building, room, and stop numbers to receive the monthly call detail report. The unit TCO must certify all charges on the monthly call detail report.

(i) The type of service. Types of leased commercial service and additional information required for each are—

1. Provisioning of local leased commercial services with FTS long-distance services required on local phones, or local voice/data circuits such as toll free dedicated/switched, voice on net, calling cards, long distance dialing (local and international) and/or frame relay.

2. Telephone calling cards. Provide the number of cards required. (See AR 25-1, paragraph 6-4, for authorized usage and management control.)

(j) Local leased commercial phone service (voice). Give number of lines including area code and exchange for the local calling area required.

(k) Off-premise extension circuits. Give number required.

(l) Local-leased commercial phone service (data). Give type/bandwidth of circuit (56Kb up to T1) and number of circuits required.

(m) Integrated services digital network (ISDN) service. Give number of ISDN basic rate interface or ISDN primary rate interface required.

(n) Number of toll free numbers required and installation extension number, for example, 1-800 service will ring on (for example, 301-677-XXXX) with the desired number of rollovers. Furnish usage estimates as follows: estimated monthly minutes of usage, expected busy period, expected number of calls during busy period, expected seasonal volume, expected busy hour percentage increase after 6 months. Provide the plain language address message addresses for the initiating activity and the initiating activity's MACOM.

(o) Cellular phone service activities must provide estimates of usage as follows:

1. Monthly minutes of peak air time usage, monthly minutes of off peak air time usage, monthly minutes of long distance usage, monthly minutes of roaming usage, monthly roaming days, and number of calls per month.

2. Cellular phone equipment and services may be procured through normal procurement procedures.

g. Coordination is important to successfully installing a local leased service. Information regarding the service should be shared with the DOIM. The DOIM should be contacted anytime there is any change in the status of a local leased requirement.

h. Documentation of phone calls from service providers concerning status of a service is important for follow-up. The TCO or other official should record the name of the person calling, the name of the company represented, the caller's phone number, and the status of the circuit action.

i. An in-effect report is submitted by the DOIM when service has been installed and is working. The DOIM is informed by the POC as soon as possible after service has been provided. Information needed includes the date and time service was provided, the phone number(s), and whether or not the service is working satisfactorily.

j. The TCO performs these functions for leased commercial phone service:

(1) Reviewing and signing requests for leased commercial phone service.

(2) Keeping a current list of leased commercial phone service for their activity.

(3) Completing the biannual review and revalidation (R&R) of all leased commercial phone service and return to the DOIM by the suspense date. The R&R requires the following:

(a) A current and thorough reason for keeping services. A memo should be sent to the DOIM requesting disconnection of services no longer required.

(b) Current funding information including the original signature of the funds certifying officer.

(c) The original signature of the TCO.

(4) Picking up and signing for all phone calling cards.

k. For information on the billing of telecommunications systems use, including cable TV (CATV), see appendix C.

#### **10-4. On-installation telephone services**

a. The installation DOIM programs switches for least-cost routing of official phone calls to ensure calls are placed over the most economic route.

b. Phone services are provided on Army Installations or comparable activities under BASECOM. BASECOM funding pays for the local and long distance commercial services for host and tenant activities on the installation. IMA will ensure installation DOIM's BASECOM services are fully funded to support host and tenant activities on the installation.

c. Classes of phone services. Army phones served by either Government-owned or commercial phone systems are classified as official (Classes A, C, and D) or unofficial (class B) (see chap 6; glossary, section II; and AR 25-1, app B, for additional description of these classes).

d. Official phone services in support of Army commissary stores.

(1) Official phone service is authorized for use by commissary store activities when essential to commissary management. Management functions include statistical data gathering and reporting, personnel management, official communications with other Army installations MACOMs or other organizations and Government agencies, and procuring contractual services.

(2) Class A-2 and C phone service is provided CONUS commissary officers, their assistants, and administrative control sections.

(3) Cashiers are authorized Class A-3 phone service for use with the local banking facilities for check verification and collection. This service is provided on a non-reimbursable basis. Class A-3 phone service is installed in locations where only cashier personnel have access to the service.

(4) Managers of meat departments, produce departments, grocery departments, warehouses, and associated commissary annexes are authorized Class C phone service for their operations. This service is provided on a nonreimbursable basis only in the office of the department warehouse and annex manager. Unofficial service is used in these areas for off-installation communications.

(5) At installations where the commissary officer is not authorized to contract for phone service, the DOIM may provide support for the requirement. In such a case, a host/tenant communications support 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.

(6) Official phone services are authorized for use by commissary stores overseas (including Alaska, Puerto Rico, Hawaii, and Panama) on a nonreimbursable basis.

e. Field operating activities (FOAs) located on an Army installation, or through mutual agreement when stationed nearby, are furnished the following phone services:

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

(2) Class A-2 service when the FOA is performing an other than military function.

(3) A mix of Class A-1 and A-2 service when the FOA is performing both military and other than military functions. The distribution of type service is mutually determined at the local level.

f. Telephone service for the Army and Air Force Exchange Service (AAFES).

(1) Headquarters, AAFES, exchange regions, area exchanges, exchange managers, main store managers, and military clothing sales store operations may be authorized Class A-2 official phone service in CONUS and OCONUS on a nonreimbursable basis for the conduct of command management functions (which constitute official business) with AAFES activities, military departments, and other DOD activities. Access to commercial circuits for the conduct of AAFES business is on a reimbursable basis.

(2) All AAFES directly operated activities such as administrators, sales, and service are provided Class C phone service.

(3) AAFES commercial contracted concessions use commercial phone service. Class B service may be provided if commercial service is not available.

g. Telephone service for contractors.

(1) Contractors providing nonappropriated fund type services use commercial phone service when available. Class B service may be provided if commercial service is not available.

(2) Contractors providing appropriated fund type support can receive official service. The contracting officer

determines if such service is advantageous to the Government and is mission essential. Determination is made on a case-by-case basis. Authorized service is specified in the contract as Government furnished equipment. Reference CJCSI 6215.01, paragraph 3 for authorized use of the DSN by contractor personnel.

(3) When official phone service is authorized, the DOIM, contracting officer, or contracting officer's representative determines what Class A and/or Class C service is provided for specific contracts. The contracting officer, in coordination with the DOIM, determines which service can be advantageous to the Government.

*h.* All private phone service in bachelor quarters, barracks, or other housing will be through AAFES or the local telecommunications service provider. MACOMs and installations will not establish phone service for soldiers in the barracks outside of the AAFES contract. Access to other voice and data services is dependent upon local agreements.

*i.* Phone service provided for occupant use in category A (official lodging (Army Lodging)) should be acquired through AAFES contract.

*j.* 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 (see to app C-3).

### **10-5. Off-installation telephone services**

This paragraph outlines special considerations for phone services provided to activities not residing on an Army installation or comparable location. Services provided by the DOIM to off-post customers are generally reimbursable.

#### *a. ARNG phone service.*

(1) Local phone services provided to off-installation ARNG units, activities, and detachments are funded by the ARNG.

(2) Local phone service is provided to the ARNG activities permanently assigned on an Army installation will be consistent with current Army reimbursement policy and at a level consistent with the proscribed IT Baseline Services on a non-reimbursable basis. Service is also extended to ARNG units, activities, and detachments during ARNG training periods on an Army installation.

#### *b. USAR phone service.*

(1) The user reimburses for local phone services provided to off-post USAR units and activities.

(2) Local phone service is provided to Army Reserve units and activities permanently assigned on an Army installation on a non-reimbursable basis. This service includes Army reserve units and activities during training periods on an installation. All long-distance toll or special type equipment charges are on a reimbursable basis.

#### *c. The U.S. Army Accessions Command (USAAC).*

(1) The educational institution often provides on-campus phone service supporting the ROTC detachment and Junior ROTC instructors.

(2) All USAAC recruiting elements not on an Army installation will be provided services centrally from the USAAC HQ.

(3) The USAAC may work within the DOIM, NETCOM, DISA, General Services Administration, or direct with FTS 2001 providers for services. These services might include on/off net from a nearby Army installation. All services will be subject to reimbursement by the requesting USAAC. All available services, including FTS/FTS-2001, are considered before approval of commercial services.

### **10-6. Messaging services**

*a. Electronic mail.* Official organizational electronic mail is to be migrated to DMS-compliant message products while commercial e-mail is used for medium grade messaging protected using the CAC card and DOD PKI. For additional information, see the PM DMS-Army Web site at: [www.dms.army.mil](http://www.dms.army.mil).

#### *b. DMS.*

(1) The DMS is the DOD-mandated replacement for the Automatic Digital Network system. It is the only authorized electronic medium for the exchange of organizational messaging within the DOD, other Government agencies, and allied nations. DMS originally was a writer-to-reader capability but has evolved into a diverse implementation of several message delivery systems, (DA, Defense Message Dissemination System).

(2) Organizational message users generally are considered to be those that formally represent the command and have authority to release messages. Classic DMS installation on a PC typically includes the DMS user agent and FORTEZZA card reader. DMS is undergoing a modernization that will allow users to access their organizational messages using their common access card and a Web browser by using proxy user agents (PUAs) operated at centralized locations. FORTEZZA tokens are located at the PUA where incoming messages are decrypted and profiled into users' mailboxes. Users access these mailboxes across a PKI encrypted Web link. Users can also send messages through the Web interface to the PUA which will address, sign, and encrypt them using FORTEZZA before sending them to the DMS backbone for delivery. Organizational users are able to send and receive signed and encrypted messages using the PUA without having to have a DMS-modified e-mail client or a FORTEZZA card on their desktops.

*c. Commercial e-mail.* Individual message users will use DMS-compliant commercial electronic mail, which interfaces directly to the DMS messaging. See para 9-1 of this document for use of enterprise software licenses.

#### *d. Record communications (legacy systems).*

(1) The DMS Transition Hub (DTH) Legacy System is a multilevel secure, worldwide network that provides command and control, intelligence, logistical, and administrative record communications service for the DOD and non-DOD organizations. DTH is a secure, computer-controlled, store-and-forward message switching communications system managed by DISA. The network is composed of DTH Switching Centers, Interswitch Trunks that interconnect the DTHs, and various-speed subscriber access lines. The DTHs are operated and maintained by the Army and Navy. Additionally, the Army serves as the lead military department for the Government-owned DTHs throughout their life cycle.

(2) DTH is a common-user network that processes traffic for two distinct communities of interest. The first community is the general service community. The other is the Defense Special Security Communications System. The two communities are handled separately; one community is not permitted to cross over to the other community. Some subscribers can receive both types of traffic on their circuit, but the message texts are never mixed.

(3) Procedures for preparation of DTH messages are provided in AR 25-11.

(4) The DTH legacy system will be phased out as organizational users transition from DTH to DMS.

*e. United States Message Text Format.*

(1) This format is a program designed to enhance joint communication through the standardization of message formats. Standard message formats with information exchange procedures ensure that the warfighter stays in contact. MIL-STD-6040 is the mandated standard for messages used to communicate throughout the joint staff, service component commands and combatant commands.

(2) The program applies to all character-oriented message text formats used in DOD operations and national security IT systems. For more information pertaining to the preparation of these messages, refer to <https://disain.disa.mil/usmtf>.

## 10-7. Long-haul services

*a. Defense Information Systems Network (DISN).* The DISN, under the management of DISA, comprises the DOD consolidated worldwide enterprise-level telecommunications infrastructure which provides the end-to-end information transport for supporting military operations, National Defense Command, Control, Communications and Intelligence requirements, and corporate defense requirements. DISN provides the primary transmission path to support the Defense Information Infrastructure. DISN features a backbone capability in the CONUS with Synchronous Optical Network (SONET) transmission. This transmission is integrated with military and commercial leased communication satellites, switched voice and data services, SONET bandwidth managers, and teleconferencing services.

(1) *DSN.*

(a) The DSN is the primary information transfer network for DOD and is a major subset of the DISN. The DSN provides the worldwide voice, secure voice, data, facsimile, and video teleconferencing services for DOD C2 elements, their supporting activities engaged in logistics, personnel, engineering, and intelligence, as well as other Federal agencies.

(b) DSN is under the operational direction and management control of the DISA.

(c) To order DSN usage and precedence service, see paragraph 7-2.

(2) *DISN IP router service.*

(a) The NIPRNET connects several LANs and users through the use of routers and Asynchronous Transfer Mode Switches (ATMS), which are interconnected using high-speed digital trunks. It uses several inter-networking protocols to allow all types of traffic to traverse the network. These protocols include IP, transmission control protocol, FTP, Telnet, hypertext transfer protocol (HTTP), and simple mail transfer protocol (SMTP). The NIPRNET provides access to the Internet through the use of gateways. E-mail can be transferred to internet users since the NIPRNET mail addressing system is recognizable to the Internet.

(b) Remote NIPRNET access can be accomplished using dial-up connections. Communications servers have modem banks that are connected to DISA routers allowing modem users to access the NIPRNET. Access is restricted by use of the Extended Terminal Access Controller Authentication Control System (XTACACS) which requires a login and password. For information on how to obtain access, see the network information home page at [www.nic.mil](http://www.nic.mil).

(c) Deployed U.S. forces can access the NIPRNET through the use of the Integrated Tactical-Strategic Data Network.

(d) All requirements for NIPRNET must be properly registered per CJCSI 6211.02A.

(3) *SIPRNET.* The SIPRNET is a WAN that is separated both physically and logically from other networks. Each access circuit and backbone trunk is encrypted to ensure integrity of information. It uses several inter-networking protocols to allow all types of traffic to traverse the network. These protocols include IP, transmission control protocol, FTP, Telnet, HTTP, and SMTP. The SIPRNET supports many of the important programs, such as the DMS, the Global Command and Control System and the Global Combat Support System.

(a) Remote SIPRNET access can be accomplished using dial-up connections. communications servers connect to DISA routers using secure devices (for example, Secure Telephone Unit III) to access the SIPRNET. Secure Telephone Unit IIIs restrict access to only authorized users by use of an access control list, which is loaded into the Secure Telephone Unit III at the node site. Users must have a secret-level SIPRNET user key to be allowed connection to the

communications server. Further protection is added by use of the XTACACS, which requires a login and password. For information on how to obtain communications server access see the network information home page.

(b) All SIPRNET requirements must be properly accredited per DOD policy and procedures. This process can be found in DODI 5200.40.

b. *FTS 2001*. The FTS provides Government users with up-to-date, cost-effective, and easy-to-use telecommunications services. The program is designed to enhance the goals of the National Information Infrastructure and to support implementation of key IT recommendations of the National Performance Review. The FTS provides the bulk of the telecommunications services for the emerging Government Services Information Infrastructure. The FTS program comprises many contracts and acquisition activities of which FTS 2001 is one.

(1) Flexible and efficient service is generally aided when end-to-end service is available. Thus, the majority of telecommunications services for FTS 2001 includes both accesses and transport. Access is defined as the portion of the service between the user and the contractor's point of presence (POP), while transport is defined as the portion between the contractor's POPs. Generally, a service will therefore comprise an originating access portion, a transport portion, and a terminating access portion.

(2) FTS 2001 includes all services necessary for the Government to satisfy its worldwide telecommunications requirements. It includes all telecommunications services, features, functions, and offerings that will be generally available as a part of commercial offerings in the marketplace plus services for which there may not be commercial offerings.

(3) Mandatory service offerings include circuit switched service (CSS), switched data service (SDS), and dedicated transmission services (DTS).

(a) CSS provides connectivity on a dial-up basis between Government users, from Government users to the public at large, and from the public to essential Government services. These services include the traditional switched voice and toll free services and the increasingly important 900 and Circuit Switched Data Service (CSDS). CSS includes—

1. Switched voice service (SVS), which supports connections for voice and for analog data up to at least 9.6kb/s using an International Telecommunications Union-Telecommunication Standards Sector (ITU-TSS) V.32 modem and 56 kb/s using an ITU-TSS V.34 modem. It allows voice calls, initiated from on-net locations as well as from off-net locations after verification of authorization code, to be connected to all on-net and off-net locations by direct station-to-station dialing. SVS includes basic voice, calling card and audio conferencing services. SVS access is delivered directly to the user's terminal equipment including, but not limited to, the following types: single-line phones; multiline key phone systems; conference-room audio equipment; electromechanical, analog, and digital PBXs; Centrexes; data circuit terminating equipment (9.6 kb/s using ITU-TSS V.32 modem and 56 Kbs using ITU-TSS V.34 modem); T1 Multiplexer; ITU-TSS Group I, II, and III Facsimile (FAX) apparatus; ITU-TSS Group IV FAX (for digital access); Government secure voice and secure data equipment (for example, Secure Telephone Unit II and any other equipment typically found or proposed for use on customer premises for connection to public and private switched voice networks.

2. CSDS, which provides a synchronous, full duplex, totally digital, service delivery point (SDP)-to-POP service at data rates up to digital signal one (DS1), including certain integral multiples of digital signal zero (DS0) data rates to on-net and off-net locations. However, for calls terminating to off-net locations, the bandwidth requested by the originating on-net location is limited to the bandwidth limitations in the public switched network between the terminating POP and the terminating location. CSDS dedicated access should be delivered directly to user's terminal equipment, including but not limited to, the following types: Data Terminal Equipment (DTE) (for example, workstation, host computer, PC, video codec, Group 4 FAX, and other communicating office equipment), digital private branch exchange, or intelligent multiplexer.

3. Toll-free service (including 1-800, 1-888, and other Service Access Code (SAC) services as they develop), which allows the caller to be connected from on-net or off-net locations to pre-designated stations or locations by dialing certain toll free and message-unit-free (for example, 1-800 and 1-888) SAC numbers.

4. 1-900 service (including other equivalent SAC services as they develop), which allows the public to be connected from off-net locations to pre-designated users and information providing systems (by dialing certain 1-900 and its equivalent SAC numbers), located at Government designated location(s), to receive information provided by prerecorded messages and in combination with voice response systems or answering agents.

(b) SDS provides a synchronous, full duplex, totally digital, SDP-to-POP service at data rates up to DS1, including certain integral multiples of DS0 data rates to on-net and off-net locations. However, for calls terminating to off-net locations, the bandwidth requested by the originating on-net location should be limited to the bandwidth limitations in the packet switched network between the terminating POP and the terminating location. SDS includes—

1. Packet switched service (PSS), which is based on the X.25 protocol and is the traditional solution to the problem of consolidating multiple networks using different protocols. It provides reliable end-to-end packet-switched, connection-oriented, data transmission service at data rates up to DS0. PSS access is delivered directly to the user's terminal equipment. The user's terminal may be either packet-mode DTE which supports X.25 protocol or nonpacket-mode DTE or terminal, which does not support X.25 protocol. User equipment supported should include, but not be limited to, multiplexing/switching devices such as private branch exchanges, channel banks, routers, or multiplexers; DTE (or

packet-mode DTE); asynchronous ASCII terminals; IBM binary synchronous communications protocol terminals; IBM SNA/synchronous data link control terminals; Unisys poll/select terminals. The contractor should provide packet assembly/disassembly capability.

2. Frame relay service (FRS), which provides reliable, high speed, frame-switched, connection-oriented, data transmission service at data rates up to DS1 between user locations. The flexibility and reliability of the service make it an attractive alternative to private line networks. FRS access is delivered directly to user's terminal equipment, such as intelligent multiplexing/switching devices, or to LAN routers, or to DTE (for example, host computers). The user's terminal equipment can be both frame-relay capable equipment, which supports frame relay protocol, and nonframe relay capable, which does not support frame relay protocol.

3. IP internetworking service (IPS), which supports connectionless service between users (IP hosts) for execution of applications based on protocols, such as FTP, SMTP, HTTP, and connection to remote hosts (TELNET). IPS access is delivered directly to IP-terminals (for example, router, computer) operating under IP protocol standards, as well as to LANs operating under LAN protocol standards, such as IEEE 802.3 Ethernet, 802.5 token ring, fiber distributed data interface, through an IP-router operating under IP protocol standards.

4. ATMS supports the transmission and aggregation of a broad range of user information, including voice, data, and video via circuit-mode and packet-mode transmission. ATMS uses cell switching and multiplexing technology that conforms to asynchronous transfer mode forum, ANSI, and ITU-TSS standards. ATMS access is delivered directly to user equipment, such as PBX, asynchronous transfer mode edge switches, router, or multiplexer. ATMS should support the router for IEEE 802 LANs (token ring, ethernet) and fiber distributed data interface at a minimum.

(c) DTS, which includes dedicated transmission service between an SDP and a POP. The connection between the locations receiving this service should be permanently established unless a service request for modification, move, or disconnect is received. This service can be used for any application, such as voice, data, video, and multimedia. DTS access connections are delivered directly (via dedicated access line) to equipment, such as analog terminal equipment (for example, analog PBX, modem), data terminal equipment (for example, computer, Group 4 FAX, video codec), and also to a digital private board exchange, multiplexer, or LAN router. Both analog and digital mode of transmission should be supported. Analog DTS will be delivered as an analog signal with a nominal bandwidth of 4 kHz.

(4) For information on value-added services (optional services) under the FTS 2001 program, visit the DOD FTS 2001 Web site, [www.gsa.gov](http://www.gsa.gov) and consult the Army's point of contact listed on the site. The services are—

(a) Wireless services:

1. Cellular voice service.
2. Wireless digital packet data service.
3. One-way paging service.

(b) Satellite services:

1. Mobile satellite service.
2. Fixed satellite service.

(c) Electronic mail service:

1. X.400 based electronic messaging service.
2. SMTP-based electronic messaging service.

(d) Electronic commerce service.

(e) Video teleconferencing service.

c. *Dedicated services.*

(1) Army MACOMs and subordinate elements can acquire point-to-point and multipoint services from DISN. Worldwide transmission services are provided by DISA via a mixture of terrestrial and satellite communications infrastructure which uses either dynamic multiplex or asynchronous transfer mode technologies.

(2) The services within the CONUS are primarily leased telecommunications infrastructure and overseas via an infrastructure that is a mixture of Government-owned and leased services.

(3) DISA is providing wideband fiber-based transmission bandwidth for a DISN CONUS SONET backbone and wideband, generally fiber based, transmission bandwidth connectivity to user locations at approximately 600 DOD user locations in CONUS.

(4) The SONET backbone employs optical fiber and provides information transport between the DISN Bandwidth Managers acquired under the DISN switched/bandwidth manager services—CONUS contract. For the access areas, the vendor will provide information transport for the aggregate bandwidth of all customer service delivery points homed off the bandwidth managers located in their respective access areas.

(5) At the customer access locations, transmission bandwidth interfaces at below T1, T2, T3 and SONET can be provided. The long-distance vendors will team with local access providers as required accomplishing the access area bandwidth requirements.

(6) Services can be obtained through the normal organizational channels via submission of an request for service (RFS) provisioning process. If further information is required, refer to [www.ditco.disa.mil](http://www.ditco.disa.mil).

d. *Provisioning long-haul services.*

(1) Web order entry (WebOE) has been initiated by DISA to facilitate the provisioning process as a means of ordering telecommunication services and equipment. The ATD, NETCOM/9th ASC is the point of contact for administration and maintenance of the Army's WebOE information. Customers must register for specific approval roles as part of the WebOE process.

(2) The ATD, as the central long-haul billing office for the Army, has the final funding approval role for all Army telecommunication requests. To contact ATD for more information, send an e-mail to [ato\\_automation@hqasc.army.mil](mailto:ato_automation@hqasc.army.mil).

## **10–8. Video teleconferencing**

*a. Defense Video Services–Global (DVS–G).* DVS–G provides video conferencing services that allow two or more locations to communicate real-time utilizing audio and video information within CONUS and OCONUS. The video services can be classified up to Top Secret (U.S. and allied), bridging requirements with the intent to provide video teleconferencing (VTC) services to all U.S. Armed Forces deployed worldwide in support of Joint and combined operations. The services can be point-to-point or multipoint and connectivity can be dedicated or dial up. Additional services include a reservation center and connections to other networks. These services are provided in CONUS through three video hubs and OCONUS through additional hubs as required. The video hubs have the necessary bridging hardware and software to provide the required for interconnectivity within DOD.

(1) All video transmissions (with the exception of point-to-point dial up video services) pass through the video hubs. Point-to-point dial up between video teleconferencing facilities (VTFs) provided by the DISN Switched Services Network do not require an interface with the video hubs. The DISN Transmission Services—CONUS contract provides the network transport between video hubs and to the video hubs or the DISN switched services network from the customer SDP. The DISN Switched/Bandwidth Manager Services-CONUS will provide switch and bandwidth management capabilities. In addition, the DVS–G provides system integration, technical and programmatic support, and operations support for the worldwide DISN.

(2) The DVS–G video services interoperate with Government VTFs with multiple central processing equipment configurations, ranging from desktop and rollabout systems, to fully equipped studios.

(3) A video services reservation center is available. Customers submit requests for conference support to the reservation center to schedule a conference. An on-line directory service that provides pertinent information about all DOD video users in CONUS and OCONUS will also be provided.

(4) Connections to other networks (through video hubs) include—

(a) FTS 2001.

(b) Global commercial phone system.

(c) The service provider (global business video service).

(d) Sprint meeting channel.

(e) Tactical/deployed users of the DISN transmission system.

(5) In addition, if a Government customer identifies a requirement, the video hubs can provide access to virtual private line switched service (1–700 service) of the commercial interexchange carriers and access to other commercial video service providers.

(6) Government facilities will monitor the status and performance of the DISN video services and resources through the RNOSCs. Video services management includes fault management, accounting management, performance management, and security management.

(7) The network master hub is located in CONUS. In addition, there are two other CONUS hubs. OCONUS hubs are located in the European and Pacific theaters. All hub-to-hub video traffic will be transported on Government-provided T1 circuits.

(8) The DISN Video Services Division (GS25) assists in defining operational requirements for new customers, subscribes users to the DISN video services network, and provides support to current customers. DISN video services are only available to DOD and the Federal Government. Information regarding DISN video services is available by visiting the program Web site at <http://disa.dtic.mil/disnvtc/>.

*b. DOIM-hosted VTC.* All new DOD procurements for VTC equipment should conform to Industry standards that are developed to ensure that devices (including video) can “talk to each other.” The ITU–TSS is the worldwide body for setting industry standards for, among other things, VTC. In order to protect users and to ensure that all VTC equipment works together, the ITU–TSS developed the H.320 family of standards. The H.320 family covers many different aspects of video teleconferencing, from conducting VTC over standard phone lines to LAN. H.320 is the baseline for VTC.

(1) The DOD recognizes Federal Telecommunications Recommendation (FTR) 1080B–2002 as the official standards-based reference document for VTC users and H.320 as the minimum acceptable standard. Conforming to these standards simply means that equipment purchased for use with the DVS Network will be able to communicate at a common level.

(2) Equipment used to connect to the DVS Network must, at a minimum, be capable of operating over one and two channels at quarter common intermediate formal resolution, operate at variable rates from 56 to 1,544 kbps, have a

coder-decoder that is capable of coding at a minimum of 6 frames per second and decoding at a minimum of 7.5 frames per second.

(3) The DVS network is covered by FTR 1080B–2002, appendix A, which reiterates the minimum operating environment but allows the use of advanced capabilities. Any advanced capabilities desired may be added, such as importing video clips, computer graphics, "whiteboard" applications, or document sharing/collaboration. It should be noted that the other VTFs conducting a conference may not support the advanced capabilities.

*c. DVS capabilities.*

(1) In addition to connecting to unclassified VTFs, DVS has the capability to support up to, and including, Top Secret (U.S. and allied) bridging requirements with the intent to provide VTC services to all U.S. Armed Forces deployed worldwide, in support of Joint and combined operations. Customers needing this service should contact their cryptographic material systems custodian for assistance with security requirements and certification criteria for their facility. In order to operate classified VTCs on the DVS Network, specify on your DVS site registration form and the type(s) of service needed and submit a completed/signed access approval document, a copy of your ATO or Interim ATO, and a diagram of the equipment configuration. Annex F, from the DVS key access approval document manual, provides further guidance on the connection approval process. Annex F and the access approval document and instructions can be downloaded from the DVS homepage at <http://disa.ditc.mil/disnvtc>.

(2) DISA provides standard contract vehicles for VTC equipment and services that are available for use to satisfy VTC requirements. Army activities request exceptions to the CIO, G–6 and DISA for other contracting vehicles.

(3) Dial-up customers acquire and pay for transport access to the DVS hub. DVS hubs accept calls on three types of transports—commercial switched service, FTS switched service, and DSN. DODI 8100.3 provides guidance on use of the DSN, noting that it is the first-choice nonsecure DOD interinstallation telephony service (voice, dial-up data, and dial-up video) network and should be the primary communications means for Special C2, C2, and non-C2 users.

*d. User operated desktop VTC (DVTC).*

(1) All DVTC units must comply with Corporation for Open Systems VTC profile standards.

(2) Before acquiring communications services, users should determine with whom they need to VTC, and then obtain service from the same long-distance carrier. This is necessary, because not all long-distance digital services are interoperable.

(3) Along with the basic VTC standards described above, DVTC units should also comply with ITU standard T120 data protocols for multimedia conferencing.

*e. Getting connected to the DVS network.*

(1) Submit an RFS/telecommunications service request to start your transmission (instructions for completing an RFS may be found in DISA Circular 310–130–1 (.gov/mil restricted).

(2) Obtain DVS hub service and a site ID by contacting the appropriate Theater Video Operations Center (table 10–3).

**Table 10–3**  
**Theater video operations center contacts**

Location	Contact numbers
CONUS, DISA GS25	Phone: Commercial 703–681–1376; DSN, 312–761–1376 Fax: 703–882–3249; DSN 312–381–3249 E-mail: <a href="mailto:vtcops@ncr.disa.mil">vtcops@ncr.disa.mil</a>
EUROPE, DISA EU52	Phone: COM 011–49–711–68639–5840; DSN 314–434–5840 Fax: COM 011–49–711–68639–5312; DSN 314–434–5312 E-mail: <a href="mailto:vtcopseur@eur.disa.mil">vtcopseur@eur.disa.mil</a>
PACIFIC, DISA PC54	Phone: COM 808–656–3112; DSN 315–456–3112 Fax: COM 808–656–3838; DSN 315–456–3838 E-mail: <a href="mailto:vtcopspac@pac.disa.mil">vtcopspac@pac.disa.mil</a>

(3) For unclassified, complete a site registration form on-line. Download the "Authority to Connect Request." Download the "Connection Approval Process"

(4) For classified, complete a site registration form on-line. Download the "Access Approval Document." Download annex F.

(5) For tactical users, download the tactical site registration form

*f. Site identification.* After completion of the above documentation, DISA will assign a site ID code for record and billing purposes and direct the office that controls the crypto keying material to send it to you (when applicable). After review and approval of the site profile, the site contacts will receive an e-mail directing them to call the Joint Interoperability Test Command to begin certifying their equipment and confirm their profile configuration. Two days

after successful completion of this test, another e-mail is sent to the site contacts telling them to schedule a validation test with the service provider. The service provider gathers technical information about your facility and ensures your compatibility with the network.

## **10-9. Satellite systems and services**

*a. International Maritime Satellite (Inmarsat) Service.* The policy for Inmarsat is located in AR 25-1, paragraph 6-3a(1).

(1) The Inmarsat satellites network gives users a multiservice satellite capability. Inmarsat is no longer controlled by an international consortium, but the peaceful purpose clause requires users to agree to use the system only for peaceful, nonaggressive purposes.

(2) Several different mobile communication systems are offered that are designed to provide users at sea, on land, and in the air with Inmarsat services that range from maritime emergency beacons to broadcast-quality digital video telemetry. Devices require directional orientation toward one of several satellites because the satellites are 22,000 miles above the earth. Inmarsat, however, can be used to connect a much wider array of devices normally connected using terrestrial systems.

(3) Most terminals in use by the Army are type B, M, M4, C, Aero-C-Mini-M, Aero-H. The B terminal can operate up to 64 Kbps with the high-speed data option. The M terminal can be used for voice up at 4.8 Kbps, and fax and data at 2.4 Kbps. The Mini-M terminal is smaller and cheaper to operate but is limited to 2.4 Kbps for all functions. The M4 terminal is the most versatile and widely used by the Army and can operate at data rates of 64-128 Kbps.

(4) For the operational need statement (ONS), prepare and submit an ONS for approval per AR 71-9, paragraph 3-4 and appendix B, before attempting to purchase and commission Inmarsat terminals.

(a) The requester receives approval from the ODSC, G-3 to purchase and commission the specified number and type of Inmarsat terminals. Requesting organizations should also prepare a DISA Form 772 (Telecommunications Management System—for entry of their Inmarsat requirement into the satellite database (SDB).

(b) After obtaining the ONS approval memorandum from HQDA, per DODI 4640.14, the terminals must be purchased through DITCO using a terminal purchase RFS or telecommunication request (TR) for purchase, or organizations may obtain them on their own.

(c) After the owning organization obtains the ONS approval letter from HQDA, the terminals must be commissioned through NETCOM/9<sup>th</sup> ASC, the Army's Inmarsat commissioning authority. The commissioning process must be completed to receive the terminal's phone numbers (also known as Inmarsat mobile numbers terminal ID numbers, Inmarsat identification numbers, and Inmarsat commissioning identification numbers). Complete a commissioning application and registration for service activation application for each terminal and fax (DSN 879-0766) or mail it, along with the ONS approval memo from HQDA, to NETCOM/9<sup>th</sup> ASC, ATTN: NETC-EST-TC, Greely Hall, Building 61801, Suite 3560, 2133 Cushing Street, Fort Huachuca AZ 85613-7070.

(d) Once the terminal(s) are commissioned and the phone number(s) or IMN(s) are received from NETCOM/9<sup>th</sup> ASC, submit an RFS or TR to enroll the terminal(s) for use (this enrollment process can take up to 90 days). If your organization cannot afford to wait 90 days for DISA service, they may coordinate with NETCOM to obtain a temporary GSA commercial service contract that can be coordinated and established with a service provider of the organization's choice, not to exceed 90 days. Billing problems can result from use of the wrong land earth station and nonpayment for service. When possible, organizations must ensure that their terminals are enrolled through DISA before anyone is allowed to use the terminal. For more information on this step of the process, contact NETCOM/9<sup>TH</sup> ASC HQ.

(5) When an organization no longer needs Inmarsat service, that organization must terminate its financial and legal roles for the use of the terminal. This is a two-step process, and each step can be accomplished by one of two actions. The first step is to change commissioning information or decommission the terminal, and the second step is to submit a change RFS to change DITCO enrollment information or submit a discontinue RFS to stop all DITCO billing. The losing organization monitors any misuse of the transferred terminal and any charges for its use that accrue until either the commissioning information change memo or the decommissioning memo becomes effective, and until either the change RFS/TR or the discontinue RFS/TR becomes effective. For more information on this step of the process, contact NETCOM/9<sup>th</sup> ASC.

(6) Inmarsat can be contacted by telephone at 011-44-207-728-1777.

*b. Enhanced Mobile Satellite Service (EMSS) (Iridium).* For policy on the use and acquisition of Iridium, refer to AR 25-1, paragraph 10-9a.

(1) EMSS or Iridium provides users with a handheld satellite terminal. The terminal must be used outside, with the antenna pointing towards the sky. The terminal accesses one of 66 satellites. DISA administers the EMSS program. At present Iridium is the only DOD-approved handheld satellite system.

(2) The terminals are purchased through NETCOM/9<sup>th</sup> ASC. Iridium users must purchase the handset with the secure module/sleeve. Organizations requesting Iridium terminals should follow the ONS procedures outlined in

paragraph 10–9a. Requesting organizations should prepare a DISA Form 772 for entry of their EMSS requirement into the SDB.

*c. Equipment and services for other commercial satellite communications.* The requesting unit completes DISA Form 772 for their satellite communications (SATCOM) requirement. The unit may submit the requirement through the telecommunications management system classified SATCOM tool kit or via DISA Form 772. DISA Form 772 is validated by each submitting organization's internal process and then forwarded to DCS, G–8. DCA, G–8 submits the form to the Joint SATCOM panel (JSP) administrator who checks the form for completeness and enters the submission as a SDB requirement candidate. The JSP administrator then presents the requirement to the JSP for approval. In conjunction with the submission of the DISA Form 772, the requesting unit completes DISA commercial satellite team's CSS. The CSS is sent to the commercial satellite team and is analyzed for suitable provisioning (this is also the form DISA uses to provide a rough order of magnitude). After being approved for entry into the SDB, the requirement is submitted by RFS through proper channels. RFS should include the SDB tracking number for authentication or explanation about why the SDB tracking number could not be provided or when it will be provided. The voice number for a NETCOM POC is DSN 879–8024 or commercial (520) 538–8024.

*d. Global Positioning Service (GPS)/Precise Positioning Service (PPS).*

(1) The following procedures are to be followed by U.S. Army units that have candidate special requirements to acquire GPS/PPS special-application or common user equipment for which the using unit does not have authorization in an approved table of organization and equipment (TOE)/TDA. These procedures are necessary to satisfy the policies of AR 71–9, AR 70–1, and AR 25–1.

(2) The requesting unit prepares an ONS that is forwarded to the MACOM level for signature by a General Officer/Senior Executive Service (SES) civilian. The Office of the Deputy Chief of Staff for Programs (DAPR–FDC) should be consulted beforehand to confirm that an ONS is the most appropriate type of need statement to submit for the specific requirement and to obtain special guidance if the requirement is urgent. For additional assistance and product information to refine the requirement and develop the need statement, the requesting unit should contact the Army Product Manager for GPS (PM–GPS): U.S. Army PM–GPS, SMC/CZA, 2435 Vela Way, Suite 1613, Los Angeles AFB CA 90245–5500. The Army PM–GPS Web site is located at <http://army-gps.robins.af.mil/>.

(3) The MACOM forwards the ONS to DAPR–FDC.

(4) DAPR–FDC forwards the ONS to HQ, TRADOC DCSCD (ATCD–GC) for evaluation, allowing 45 days for review. As part of their review, TRADOC evaluates the appropriateness of the requested GPS/PPS equipment to satisfy the requirement.

(5) DAPR–FDC reviews the ONS and recommends approval (or disapproval) to the ODCSPRO–FD. DAPR–FDC may recommend that the ONS be approved for the requesting unit to acquire the needed equipment from a commercial source, through the Army PM–GPS, at the unit's/MACOM's own expense from its budgeted operations and maintenance funds. Otherwise, DAPR–FDC may recommend that the established Army PM–GPS managed GPS/PPS common user equipment acquisition program should meet the requirement and may also direct the requesting unit to apply for a TOE/TDA change under provisions of AR 71–32.

(6) Upon approval, DAPR–FDC sends a copy of the ONS back to the requesting unit and a copy to the Army PM–GPS.

(7) Upon receiving the approved ONS, the requesting unit arranges for acquisition of the needed equipment through the Army PM–GPS. The requesting unit must identify a valid fund cite and responsible billing addressee in order to initiate the acquisition process. The PM–GPS submits to the Army Acquisition Executive (AAE) any needed request for waiver for the use of Standard Positioning System equipment rather than PPS equipment, per AR 25–1, paragraph 6–4e.

*e. Equipment and Services for Other Commercial Satellite Communications.* The following procedures are provided for U.S. Army units that have candidate new requirements for commercial SATCOM services and/or user terminal equipment. These procedures are necessary to satisfy the policies of AR 71–9, AR 70–1, AR 5–12, and CJCSI 6250.01B.

(1) The requesting unit prepares an ONS, which is forwarded to the MACOM level for signature by a General Officer/SES civilian. Since commercial satellite communications is potentially a very expensive communications medium, the requesting unit should assess the cost versus benefit as part of their ONS development process. For assistance and information to accomplish this assessment, the requesting unit should contact the Project Manager for WIN–T (PM WIN–T) Commercial Satellite Terminals Program (CSTP) office, SFAE–C3T–WIN Building 744, Fort Monmouth, NJ 07703–5508.

(2) If a requirement is considered urgent, the requesting unit should directly contact DAPR–FDC for guidance.

(3) The MACOM forwards the ONS to DAPR–FDC.

(4) DAPR–FDC forwards the ONS to HQ TRADOC DCSCD (ATCD–GC) for evaluation, allowing 45 days for review. As part of their review, TRADOC evaluates the appropriateness of commercial satellite communications media to satisfy the requirement.

(5) DAPR–FDC reviews the ONS and recommends approval (or disapproval) to the ODCSPRO–FD. DAPR–FDC may recommend that an existing Army program that acquires SATCOM equipment and/or services should meet the

requirement. Otherwise, DAPR–FDC may recommend that the ONS be approved for the requesting unit to acquire or lease the requested commercial SATCOM equipment and/or services at the unit’s/MACOM’s own expense from budgeted operations and maintenance (O&M) funds.

(6) Upon approval, DAPR–FDC sends a copy of the ONS back to the requesting unit and a copy to the PM WIN–T CSTP office.

(7) Upon receiving the approved ONS, the requesting unit arranges acquisition or lease of the needed commercial SATCOM equipment and/or services through the PM WIN–T CSTP office. The requesting unit must identify fund cite(s) and responsible billing addressee(s) in order to initiate acquisition/lease of equipment and to lease or enroll for commercial satellite access resources.

(8) If commercial SATCOM terminals are procured to be owned and operated by an Army unit, the acquisition manager (PM WIN–T) submits DD Form 1494 (Application for Equipment Frequency Allocation) to the U.S. Army Communications-Electronics Services Office (address at paragraph 10–9d(1)), to obtain a certification of spectrum supportability of equipment. This certification is required before the using unit may operate the satellite terminal equipment. The PM WIN–T CSTP office facilitates the arrangement of host nation agreement support if the Army-owned commercial satellite terminal equipment will be used in a foreign country. The using unit may incur additional expense if there are tariffs attached to the use of the equipment in a foreign country.

(9) Before the commercial SATCOM terminal equipment is operated to accomplish a required satellite communications mission, the using unit assures registration of a CJCS-approved SATCOM access requirement for the mission in the Integrated Communications Database (ICDB) under the provisions of CJCSI 6250.01B. Upon receiving the approved ONS from DAPR–FDC, the unit may apply for ICDB registration by preparing and sending DISA Form 772 (TMS–C) SATCOM Requirement Request) through the MACOM level to the Joint Staff’s Joint MILSATCOM Panel Administrator for approval.

## **10–10. Land Mobile Radio Program**

*a.* Land mobile radio (LMR) systems provide wireless communications for missions and administrative operations at posts, camps, and stations. To carry out missions and operations, non-tactical wireless communications are needed for force protection, public safety, installation management, and homeland security. LMR solutions will be either trunked or conventional.

(1) Trunking technology automatically and dynamically assigns available radio frequencies on an LMR system among many users, thus allowing limited spectral resources to be used more efficiently.

(2) Conventional technology uses frequencies that are dedicated to specific channels. A single frequency, or duplex frequency pair, equates to one usable channel. When a channel is in use, other users who may want to transmit a signal on that channel must listen and wait for the current users to complete their conversation.

*b.* The DOIM—

(1) Plans and manages the LMR system, equipment and software on the local installation, and integrates any installation LMR resources into the overall installation, Army and DOD plans and standards.

(2) Provides assistance and recommendations to the user organization concerning procurement of LMR equipment to include hardware and software.

(3) Requests frequency assignments from the Interdepartmental Radio Advisory Committee and the Frequency Assignment Subcommittee and applies for Spectrum Planning Subcommittee trunking certification.

(4) Ensures installation POM justification language includes LMR system operations and maintenance requirements, including the need for a system administrator/manager.

(5) Coordinates, orders, and manages connectivity to repeater sites and dispatch consoles, as necessary.

*c.* If there is an existing requirements contract available, the LMR system or service should be obtained from that contract to the maximum extent practicable. If a requirements contract is not available, the DOIM must make every effort to furnish data to support a competitive procurement.

*d.* The assistant project manager, LMR, is the Army program office who monitors Army acquisition of non-tactical LMR systems. The assistant project manager, LMR also manages the Base Radio System (BRS) contracts. The BRS contracts provide a vehicle for Government agencies and organizations to purchase turnkey LMR infrastructure, mobile and portable subscriber units, and technical support services. This equipment includes both trunking and conventional technologies in addition to encryption (for example, advanced encryption standard capabilities). The BRS contract is an indefinite delivery/indefinite quantity contract. Information on ordering, services, and equipment from the BRS contract may be found at [www.eis.army.mil/brs](http://www.eis.army.mil/brs).

## **10–11. Other Army radio systems**

*a.* Coordination with the installation DOIM is required for radios to connect to existing networks. Installation radio support consists of non-tactical, user-operated, radio-networks systems, and facilities, equipment and information services required to support host and tenant activities at the installation level.

*b.* 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.

(1) Requirements for installation radio systems support services are justified based upon operational necessities and on an economic analysis.

(2) COTS equipment available on contracts negotiated by the Base Support Trunked Radio System project is used unless other equipment is justified.

(3) To preclude unnecessary cost to the installation because of costly modification or replacement of equipment because frequency assignments cannot be obtained, availability of radio frequency assignment should be assured before procurement action is started per AR 5–12 and this paragraph.

(4) Written waiver requests for procurement of new or expansion of existing radio systems should be submitted to the office of the PM, Joint Tactical Radio System. For further information on the waiver request format, see [http://jtrs.army.mil/sections/programinfo/fset\\_programinfo.html](http://jtrs.army.mil/sections/programinfo/fset_programinfo.html).

*c.* All U.S. Army installations within CONUS have high frequency (HF) radio systems provided specifically by the Army CONUS HF Radio Program. This HF system is capable of providing voice, secure data, and radio wire integration. The system also has automatic frequency link capability. It is designed for interoperability, transportability, and ready adaptation to emergencies and contingency operations. The DOIM supervises—

(1) Operation and maintenance of the system.

(2) Communications security support for the installation Army CONUS HF radio station and equipment.

*d.* The Army Military Affiliate Radio System (MARS), addressed in AR 25–6, is part of an overall communications service involving the military services and civilian amateur radio operators.

(1) A military installation or base MARS station is a facility installed, operated, and maintained by U.S. military or DA civilian personnel.

(2) Military installation, military units/clubs, and volunteer licensed U.S. amateur radio stations and operators may participate in the MARS program.

(3) MARS provides DOD-sponsored emergency communications on a local, national, or international basis as an adjunct to normal communications.

(4) Commanders and agency heads should support and encourage MARS and amateur radio activities, and avoid, within the limitations imposed by military agencies, any action that would tend to jeopardize the independent prerogatives of the individual amateur radio operator.

## **10–12. Army radio frequency spectrum management**

*a.* AR 5–12 governs Army-wide spectrum management.

*b.* CONUS-based spectrum management activities are carried out under the National Telecommunications and Information Administration's policies and guidelines for use of the spectrum by all Federal Government agencies and by provisions of DODD 4650.1. The Army is obligated to comply with these policies unless waived by the Army Spectrum Manager.

*c.* OCONUS-based spectrum management activities. The frequency spectrum is a natural resource within any sovereign nation's boundaries and can only be used with that nation's consent. Spectrum use in OCONUS locations is subject to Status of Forces Agreements made with host nations and is determined by appropriate theater policies and procedures.

*d.* Installation commanders coordinate, plan, program, and fund adequate management and supervision of the spectrum. Installation commanders monitor all devices that emit electromagnetic emissions from their installation. The installation DOIM or other designated individual in the area or region provides spectrum management support. Areas of spectrum management that require command emphasis are:

(1) Certification of spectrum-dependent equipment per AR 5–12, chapter 4.

(2) Frequency assignment in CONUS and host nation approval in OCONUS locations per AR 5–12, chapter 5 (see Military Communications-Electronics Board (MCEB) Pub 7).

(3) Ongoing review of frequency assignments for deletion or amendment. In CONUS, U.S. Government policy requires Army users to revalidate each permanent frequency assignment to delete or modify the record, normally every 5 years. OCONUS, Army records require a similar review under Allied Communications Publication (ACP) 190(B) (US SUPP–1) or per COCOM directives.

(4) Clearance for electronic attack operations per AR 5–12, paragraph 5–9.

(5) Radio station identification, international call signs, and other nontactical call signs per AR 5–12, chapter 6.

(6) Coordination with other installation directorates and tenant activities concerning spectrum-dependent equipment per AR 5–12, chapters 4 and 5.

(7) Assistance in resolving incidents of harmful radio interference per AR 5–12, appendix C.

(8) Appropriate classification markings, classification authority, and downgrading instruction for classified frequency certification and frequency assignment records per AR 380–5.

(9) Awareness of the operating parameters (power level, antenna type, height, gain, authorized operational use, area of operation, and so on) of assigned frequencies.

(10) Coordinate with installation directorates and tenant activities to ensure that spectrum-dependent equipment (for example, fire alarms, paging systems, handheld radios, barcode readers) being developed or procured by or for use on the installation is fully supportable (see AR 5–12, chaps 4 and 5).

(11) Ensure that the installation frequency coordinator is trained. Frequency coordination constitutes dealing with international and national laws on a regular basis in addition to safety of life issues. Assigning this function as an additional duty or temporary assignment to untrained personnel could have severe repercussions.

(12) Establish a program in which each tenant/supported organization that use spectrum-dependent emitters performs positive radio control duties such as—

(a) Using radiation-suppression devices (dummy loads) as much as possible when tuning, testing, or experimenting.

(b) Ensuring that proper radio procedures are used when transmitting. Refer to appropriate Allied Communications Publications.

(c) Providing to the installation frequency coordinator, the name and phone number of a point of contact for frequency matters.

(d) Ensuring that electromagnetic radiating equipment operations comply with authorized parameters, for example, power, location, frequency.

(e) Informing the installation frequency coordinator of any changes in location, operations, or technical parameters (for example, power operating bandwidth, change of antenna type, height, or location) for operation of electromagnetic radiating equipment.

(f) Advising the installation frequency coordinator when frequencies are no longer needed.

(g) Obtaining a frequency assignment before using devices that intentionally emit radio frequency (RF) energy or require protection of receive-only frequencies from interference.

(h) Coordinating frequency actions with the installation frequency coordinator.

(i) Requesting the minimum number of frequencies necessary to accomplish the mission.

(j) Requesting the minimum transmitter power an antenna height and gain necessary to ensure adequate coverage.

(k) Ensuring that transmissions on all RF emitters are for official Government use.

## **Chapter 11**

### **Delivery and Support of IT Systems and Services**

#### **11–1. General**

a. This chapter offers guidelines on acquiring and delivering IT systems, services, and equipment (see AR 70–1 and DA Pam 70–3 for more information on Army’s acquisition policy and procedures).

b. Acquisition is obtaining supplies or services by contract with proper funds. These supplies or services—

(1) May be used by the Federal Government.

(2) May be acquired through purchase or lease.

(3) May already exist.

(4) May need to be designed, developed, demonstrated, and evaluated.

c. Acquisition begins when the organization’s needs are established. The process includes—

(1) A description of requirements to satisfy organizational needs.

(2) Solicitation and selection of sources.

(3) Contract award.

(4) Contract financing.

(5) Contracting performance.

(6) Contract administration.

(7) Technical and management roles related to the process of meeting installation/activity needs by contract.

(8) Sharing, reusing, and contracting for items by lease, purchase, or any legal methods.

d. Under acquisition reform, procurements require performance specifications but not mandatory standards. Performance and results are the objectives. This change in philosophy emphasizes organizational needs rather than the mechanics of the contracting process. Changes in Federal contracting statutes institutionalized the preference for the use of commercial products and commercial practices in contracting. Customers can now make selections based on best value, similar to the way private industry buys supplies and services.

e. The ASCP is the primary source for commercial IT purchases. ASCP makes purchasing more efficient and decreases the total costs of IT procurements. The inventory includes IT products and services that are in compliance with DOD, Army, and NETCOM policies and standards to ease the Army transformation to a net-centric architecture.

Army customers must look to meet their requirements using ASCP contracts before making commercial IT purchases from other sources. A complete list of contracts is available at <https://ascp.monmouth.army.mil>.

## 11–2. Acquisition and delivery strategies

*a. Procurement strategies.* Customers and providers of information systems must be aware of the various procurement approaches available for acquiring IT systems and services. If there is an existing ASCP indefinite delivery, indefinite quantity contract or blanket purchase agreement (BPA) available, the system or service is obtained from that contract or agreement to the maximum extent practical or a waiver obtained. If there is an existing DOD ELA, that vehicle must be used or a waiver obtained. If a contract vehicle is not available on an ASCP contract, DOD ESI or the Federal Supply Schedule (FSS), and the requirement is greater than \$500K, the customer should contact the Army Contracting Agency/Information Technology E–Commerce and Commercial Contracting Center and provide data to support a competitive procurement. The scope and cost factors (program and life cycle) determine if the IT acquisition should be managed at the MACOM or Army level. See DA Pamphlet 70–3 for the definitions and thresholds of acquisition categories.

*b. Methods of acquiring IT supplies and services.* IM/IT managers should be aware that the Information Technology E–Commerce and Commercial Contracting Center is the Army-wide Army Contracting Agency central contracting office for all installation computer services. It has established contracts and other business arrangements that offer economical solutions to most common-use service requirements. IM/IT managers must send requirements for computing-related services over \$500K to the Information Technology E–Commerce and Commercial Contracting Center for disposition by the local director of procurement. This includes all requirements that are contemplated as outsourcing opportunities through another agency, such as the GSA or Department of the Interior. IM/IT managers must consider the merits of all available procurement methods before selecting a procurement approach. Methods include sharing or reuse and procurement from various procurement lists and the FSS. See FAR and DFARS for information on the contracting processes (for example, invitation for bids and request for proposals).

(1) IM/IT offices may select from various contract vehicles and techniques to meet their requirements. Multiple approaches may need consideration to meet both short- and long-term requirements.

(2) There is no single acquisition strategy that is ideal for every situation. The best acquisition approach for a particular project or program is only determined after examining each requirement's many objectives and environments. The customer must be aware that contract offices may vary in the quality of service and the amount of industrial funding fees charged for clerical costs. Another issue is the variation in the timelines of service in different vehicles. Managers must build a business case for each option and then decide, based on cost, performance and risk management factors.

*c. Purchase.* The Army gains title for purchases at the time of successful final test and acceptance. Purchase contracts may have warranty periods in which the contractor gives parts, training, and maintenance at no charge. Customers must ensure that the effective date for providing contract maintenance and parts matches the expiration date of the guarantee period. The practice of designating a preferred source for a specific order is prohibited under the FAR. This practice robs the Government of the benefits of continuous, streamlined, commercial-style competition gained from the fair opportunity process.

### *d. Micropurchases.*

(1) Before purchase, the DOIM must approve all IT procured using the micropurchase process.

(2) A micropurchase is a simplified acquisition procedure for purchases under \$2,500. Putting a lot of effort into purchases under \$2,500 would not yield enough savings to justify it. Micropurchases need not be set aside for small business and, if the price is considered reasonable, may be awarded without soliciting competitive quotations.

(3) A micropurchase is a procedure rather than a source and involves the placement of an order against an existing contract. Micropurchases may be made by means such as purchase orders, orders against FSS contracts, calls against BPAs, Government purchase card purchases at local retailers or catalog companies, and so on. A micropurchase requires only going to a local store or ordering from a supply catalog. Micropurchasing authority is increasingly delegated to the requesting activity. The majority of micropurchases are now made via purchase card (see para 11–4).

(4) One of the disadvantages is that the procedure can be abused. With delegation of authority there may be a greater risk of fraud, waste, and abuse. Activities may not split requirements to stay below micropurchase threshold.

*e. Lease.* Under this method, IT systems and equipment are acquired under a periodic charge arrangement. The lease may lead to direct ownership. Lease contracts might include added charges for extra use of equipment. Maintenance, training, and other contract support could be priced separately or be included in the lease cost. General purpose IT equipment can be leased under the GSA Schedule (or through multiple BPAs). Lease terms vary. Lease type must be coordinated with resource management to ensure proper funding for the lease.

(1) Three common lease arrangements are—

(a) Straight lease. The Government leases resources for a base period and may have an option for more periods.

(b) Lease-to-ownership plan. The Government leases items for a period, after which lease payments end and the Government takes title.

(c) Lease with option to purchase. The Government leases items for a period with an option to purchase at a later

date. The Government may acquire ownership of resources by invoking the contract option(s). All proposed lease acquisitions include a lease/purchase analysis that is prepared by the requiring activity and reviewed by the contracting office before completing the acquisition plan.

(2) Leasing hardware desktop resources is cost beneficial to many private sector firms that must maintain a competitive edge. When equipment is traded up every two years or so, a lease arrangement may give the firm a total cost of use (ownership) lower than purchasing, particularly with regard to replacing obsolete purchased IT equipment that will have little or no resale value. Leases on software (COTS common use) are not practical, since they may be obsolete in months.

(3) Computer leasing is usually not a good option to meet the needs of the average customer since the costs of leasing versus purchase are usually higher. But organizations with a need for state-of-the-art equipment may consider leasing. Organizations should do a benefit/cost comparison before deciding to lease.

*f. Standard contract vehicles.* Under the GSA FSS contracts program, the FSS administers the award and oversight of schedule contracts, including IT schedules. This is the most well-known program for Federal contracts. The program is a nonmandatory source of supply and services. Also known as multiple award schedule, FSS is a listing of vendors that have been awarded a contract by GSA that can be used by all Federal agencies. GSA awards competitive contracts to those companies, which give the same or better discounts as compared to those given to the contractors' best customers. GSA has determined prices to be fair and reasonable.

(1) A multiple award schedule is an indefinite delivery, indefinite quantity contract available to Federal agencies. These contracts are compliant with applicable laws and regulations. Administrative time is reduced, an array of commercial items is available, and agencies order directly from the contractor.

(2) BPAs are accounts that can be set up with schedule contractors to meet recurring needs for services and products. FSS BPAs may be considered to cover short-term startup requirements, such as installing cable, until a longer-term, more appropriate vehicle is awarded. Contractors may offer the best quantity/volume discounts available under their contract based on the potential volume of business that may be generated by the BPA. BPAs provide discounts while eliminating the need for writing numerous task/delivery orders. BPAs are determined on best-value per FAR 8.404. BPAs should be reviewed yearly to ensure it remains the best value for an agency.

(3) Government-wide award contracts. These are contracts for IT resources owned by one Federal agency that all other Federal agencies may use on a limited basis. The owning (host) agency establishes the maximum value of the contract based on their requirements plus an additional 20 percent for other agencies. Other agencies' indefinite delivery, indefinite quantity contracts are primarily for use by the host agency. Access is limited to other agencies and limited sources are available. In some cases, ordering must go through the host agency. Some require approval letters, documentation for best value selection, price determinations, etc.

*g. Other IT acquisition and delivery options.* The ASCP is the primary source for purchases of COTS software, desktops, and notebook computers, regardless of dollar value, and for all other IT purchases greater than \$25K. ASCP has an array of fully competed contract vehicles to meet Army requirements. These contract vehicles must be considered before buying from contract vehicles from other sources. If an Army customer chooses other than an ASCP contract vehicle, ASCP must first grant a waiver. If an Army customer chooses other than a DOD ELA for a software purchase, ASCP must first grant a waiver. A complete list of ASCP contracts, DOD ELAs, and the online waiver process is available at <https://ascp.monmouth.army.mil>.

(1) *Outsourcing.* Outsourcing IT support is becoming an alternative or adjunct to an in-house workforce due to the reduced costs associated with personnel and maintenance

(2) *Consolidation, restructuring, and regionalization.* Under OMB Circular A-76 and other mandates, installations are assessing consolidation or restructuring alternatives to make operations and services more efficient. It is more expensive to operate and maintain many small facilities than a fewer number of larger ones.

(3) *Seat management.* The seat management (desktop outsourcing) concept calls for organizations to transfer the procurement and management of their desktop environment to an outside contractor. It is based on the telecommunications industry, with the computer treated as a utility and the service behind being transparent. Many firms in private industry have outsourced PCs and their support. A service provider is given a set of equipment and maintenance requirements and agrees to meet the requirements for a charge-per-seat-per-month fee. The package includes hardware and software maintenance, configuration management, and upgrades. This method is designed to capture the total cost of ownership.

(4) *Defense enterprise computing centers.* The DOD-wide consolidation of data centers is an example of a consolidation effort that reduced IT costs. Cost-saving measures prompted DOD agencies to transfer their information processing to enterprise computing centers in support of joint and DOD standard application systems.

(a) The computing services business area is operated as a Defense Working Capital Fund activity and includes mainframes, client server technology, network management and systems engineering that offer secure processing of classified and unclassified information, global interoperability from the sustaining base to deployed forces, surge capability, and operational sensitivity to rapidly changing priorities.

(b) Advantages of this outsourcing option include wartime survivability; migration to latest technology; reduced

hardware, executive software, system administration, personnel, and facility costs; increased standardization and interoperability; and enhanced security.

(c) Mainframe information processing is available to the military services and Defense agencies at five Defense enterprise computing centers: St. Louis, MO; Mechanicsburg, PA; Columbus, OH; Ogden, UT; and Oklahoma City, OK. Most Army mainframe processing is supported by Defense Enterprise Computing Center –St. Louis. Non-mainframe information services are provided at various DISA regional support activities throughout CONUS.

(d) Additional information on Defense enterprise computing centers services may be obtained from the CIO/G-6, SAIS-AON.

(5) *CECOM/Software Engineering Center*. The Software Engineering Center provides software support and software engineering products and services throughout the Army and DOD and may be contacted at U.S. Army CECOM, Software Engineering Center, Fort Monmouth, NJ 07703. Their services include: Integration of battlespace and sustaining base systems, C4I–electronic warfare and sensors, avionics, sustaining base and business systems software architecture and technology, consulting software acquisition, postproduction software support, software development and prototyping software, contract administration, and interoperability engineering

### **11–3. Redistribution and disposal of information technology assets**

a. The screening, redistribution, and disposal of IT equipment are completed through the DRMS. DRMS is the DOD-wide program for asset visibility, resource sharing, and asset redistribution. The Defense Logistics Agency is the executive agent of DRMS for DOD.

b. The process for disposal of IT equipment is consistent with the process used for all other excess property. For further guidance and clarification on the processes and communications flow for the disposal of excess IT equipment, installation DOIMs should contact their installation property book officer for guidance on reutilization, transfer, and donation programs for excess IT equipment or visit the DRMS Web site at [www.drms.dla.mil](http://www.drms.dla.mil).

c. Per DOD policy, all hard drives of unclassified computer equipment leaving the custody of DOD must be overwritten, degaussed, or destroyed in accordance with the associated security risk of the information contained within the drive. DOIMs and/or property book officers will ensure that hard drives are disposed of using the methods and procedures prescribed in the DOD Memorandum, "Disposition of Unclassified DOD Computer Hard Drives," dated 4 June 2001.

d. It is very important to check all computer equipment and property prior to turn-in to the DRMS for any Secret, Classified, Confidential, Tempest, or Hazardous indicators. A DD Form 1348–1A (Issue Release/Receipt Document) or 1348–2 (Issue Release/Receipt Document with Address Label) must accompany all property.

e. Turn-in procedures for CPUs without hard drives require the following:

- (1) A DD Form 1348–1A or 1348–2 (filled out completely).
- (2) The CPU chassis serial number in block 26 (optional).
- (3) One required statement either on/or with DD Form 1348–1A or 1348–2 and two optional statements.
- (4) Label chassis serial number when hard drive is removed using (Defense Logistics Information Service) DLIS Form 1867 (Certification of Hard Drive Disposition) or equivalent.
- (5) Name, rank/grade, and signature of individual certifying the information.
- (6) Removal of memory sticks from other forms of computer equipment, such as handheld computers (palm pilots, organizers, and so on).
- (7) Internal devices such as sound, network or controller cards may stay in the CPU.
- (8) Removal of the following computer media and cards from all turn-in computer equipment: compact flash cards, secure data cards, CD–ROM media, smart card media, microdrives, multimedia cards, memory sticks, Personal Computer Memory Card International Association (PCMCIA) cards, backup tapes, floppy diskettes, and zip media.

f. Turn-in procedures for CPU with hard drives require the following:

- (1) Ensuring that the hard drive (notebooks, desktops, laptops, and docking stations) has been degaussed or overwritten in accordance with DOD Memo dated 4 June 2001.
- (2) Completing DD Form 1348–1A or 1348–2 (filled out completely).
- (3) Labelling the CPU chassis/housing serial number in block 26 (optional).
- (4) One required statement either on/or with DD Form 1348–1A or 1348–2 and two optional statements.
- (5) Labelling the hard drive using DLIS Form 1867 or equivalent.
- (6) Ensure the following computer medias and cards are removed from all turn-in computer equipment (internal devices such as graphic, sound, networks or controller cards may stay in the CPU):
  - (a) Compact flash cards, secure data cards, CD–ROM.
  - (b) Media, smart card media, microdrives, multimedia.
  - (c) Cards, memory sticks, PCMCIA cards, backup.
  - (d) Tapes, floppy diskettes, and zip media.
- (7) A label on chassis using DLIS Form 1867 or equivalent.
- (8) Name, rank/grade, and signature of individual certifying the information.

(9) Removal of memory sticks from other forms of computer equipment such as handheld computers (palm pilots, organizers, and so on).

g. Turn-in procedures for hard drives require the following (no labeling or certification requirements exist for unused hard drives (not in original packaging):

- (1) A completed DLIS Form 1867 or equivalent for all hard drives.
- (2) The hard drive serial number(s).
- (3) A signed certification on the disposal turn-in document (DTID) that must contain a statement such as “Hard drive (s) has/have not been used.”

h. Turn-in procedures for all other computer-related devices require the following:

(1) A DTID (DD Form 1348–1A or 1348–2) for each national stock number and Federal Supply Group/Federal Supply Classification/FSC, type property (a label is not required if the hard drive is destroyed and turned in as scrap).

(2) Unless required by organization supply personnel, no serial numbers required.

(3) Statement on/or with the DTID if the generator requires verification that the hard drives were turned in to the DRMO as scrap.

(4) Removal of monitors, printer (toner must be removed), keyboards, speaker, modems, mouse/mice, plotter (toner must be removed), and external devices.

(5) All others that do not fall under the category of classified, secret, tempest or hazardous waste.

i. DOIM turn-in procedures include the following:

(1) Hand-receipt holders will—

(a) Turn-in to the unit PBO all IT equipment that is determined excess and/or replaced because of nonuse, unserviceability, upgrade, or system change.

(b) Maintain accountability of the equipment throughout the turn-in process.

(c) Ensure the hand receipt and any subhand receipt are updated to reflect turn-in.

(2) The unit property book office will prepare documentation (DA Form 3161 (Request for Issue or Turn-In) ) required for disposal or redistribution.

(3) The DOIM, with assistance from user(s)—

(a) Coordinates the redistribution/disposition of IT equipment.

(b) Reviews documents identifying IT equipment due for redistribution/disposition.

(c) Turns in all IT equipment and provide written results on DA Form 2407 (Maintenance Request) to the appropriate hand receipt holder.

(d) Manages all IT equipment assets and their related systems for activities.

(e) Renders technical inspection IT equipment identified by hand receipt holder for turn-in.

(f) Receives IT equipment that has been processed thru the installation Property Book Office.

(g) Removes hard drive from computers and affix required label.

(h) Disposes of equipment through the local support supply activity.

j. Procedures for IT turn-in include the following:

(1) The hand-receipt holder—

(a) Completes a DA Form 2407 for each item requiring turn in and submits DA Form 2407 to DOIM.

(b) Once the DOIM returns an annotated DA Form 2407, provides the form along with a request for turn-in to the technical inspector of the PBO and retains one copy until item is cleared from hand receipt.

(2) The installation PBO—

(a) Submits a memorandum requesting turn-in of IT equipment coded as serviceable and applicable DA Form(s) 2407 to the DOIM.

(b) Prepares documentation (turn-in and/or lateral transfer, DA Form 3161) required for disposition or redistribution instructions as determined by the DOIM and forward to the DOIM.

(3) The DOIM—

(a) Receives documentation from the installation property book office and schedules appointment with hand-receipt holder for turn in of equipment.

(b) Removes hard drives from computers and affixes required label.

(c) Disposes of equipment through the local support supply activity.

#### **11–4. Use of Government purchase cards for purchase of information technology assets**

a. *Use of the Government purchase card.* The Government purchase card (more formally referred to as the Government-wide commercial purchase card) can be used to procure and pay for purchases of COTS IT equipment, supplies, or services. While not an acquisition technique itself, the purchase card can be used with other acquisition methods. Government-wide commercial purchase cards may be used to—

(1) Order from ASCP contract vehicles.

(2) Order from DOD ELAs.

- (3) Order online from the ASCP e-commerce site, IT e-mart.
- (4) Order from GSA FSS contracts.
- (5) Place a task or delivery order (if authorized in the basic contract, basic ordering agreement, or blanket purchase agreement).

(6) Make payments, when the contractor agrees to accept payment by the card.

*b. Government purchase card benefits.* The use of the Government purchase card offers ease and flexibility of use, streamlining of the procurement process, and reduction of administrative costs. When the monthly invoice is paid on time, there is usually a rebate issued by the card company.

*c. Making purchases.* All applicable acquisition regulations, supplements, and local procedures apply when making purchases paid for with the purchase card. The cardholder has the authority to purchase and ensures that funds are available to pay for the purchase. The ordering office should check mandatory sources before purchase and ensure the price is reasonable. See paragraph 11–2*d* for information on micropurchases. Most ASCP contract vehicles allow for credit card purchases. The ASCP IT e-mart allows for online credit card ordering. For FSS items, follow the online directions for competitive procedures. For open market items, the orderer should verify and document price reasonableness when—

- (1) The cardholder suspects or has information to indicate the price may not be reasonable.
- (2) When purchasing items for which comparable pricing information is unavailable.
- (3) In (1) or (2) above, the buyer should document the purchase in writing with a brief explanation of how price reasonableness was determined. There are various ways to demonstrate price reasonableness. Obtaining competition is one of the best ways to demonstrate price reasonableness. Competition is achieved by documenting prices from three or more vendors. Cardholders may also document price reasonableness by a comparison of current prices with catalog prices or historical pricing information.

*d. Used as a method of payment.* The purchase card may be used as a method of payment for purchases and orders not over the simplified acquisition threshold (currently \$25,000) under existing IDIQ contracts, or for other established contracts when the contract authorizes its use as a payment method.

*e. Local purchases.* The card provides the flexibility of making local purchases under \$25,000 when they need items that are not available through the supply system in a timely manner. The authorized spending limit may differ for each cardholder. IM/IT officials should use charge cards per the local contracting SOP.

*f. Micropurchases.* Purchase cards are used for all micropurchases (purchases under \$2,500) unless an exception has been granted.

*g. Single purchase limit.* Single purchase limits are established through the cardholder/approving official's chain of command with the servicing resources management officer, up to \$25,000. The delegation of authority memorandum appoints the cardholder and designates the single purchase limit for each purchase card. This authorization has been established to ensure procurement laws and acquisition regulations are followed. Buyers may not split a requirement into several purchases to stay under the \$25,000 limit.

*h. Record of transactions.* For each purchase there must be a dated, written request which identifies the requirement. Purchase information may be entered on a monthly purchase log. Cardholders must keep a log of charges, preferably on magnetic media, and backed-up to prevent loss of the data. The log is to be used to assist in keeping track of charges, to ensure cardholders do not spend more than the amount committed by the resource management office to the account, and to provide documentation (in conjunction with actual charge slips) to make the reconciliation process easier and faster.

- (1) The monthly log should be retained at the approving official level with all other documentation for 36 months.
- (2) For OCONUS installations, when recording purchases made on the local economy in the log, the cardholder will have to use an estimated rate of exchange. The actual rate will be the market rate for purchase cards at the time the transaction moves from the country of origin's financial system to the U.S. financial system. At the time of transaction there is no way to know what that rate will be. Cardholders can get rates from local banks, local English language newspapers, or banks on post. This rate will be used to estimate the dollar amount of the transaction. Cardholders are reminded to allow for some exchange rate variation and should be careful of making purchases that calculate exactly to their single purchase limit. This method will lead to some difference between the purchase log and the account statement that will be received at the end of the billing cycle.

(3) A Government purchase card purchase record must be completed and processed for each purchase over \$2,500.

*i. Approval and oversight of IT purchases.* Purchases are approved through IMO channels and finally at the installation DOIM office before purchase. Written approval must be obtained from the appropriate command authority before purchase. Consumable items such as diskettes, ribbons, toner cartridges, and so on are authorized for purchase using purchase card without IMO or DOIM approval.

## **11–5. Administering information technology contracts performance**

*a. Technical administration.* The technical administration of Government contracts is an essential activity. It is essential that those entrusted with the duty to ensure that the Government gets all that it has bargained for must be

competent in the practices of contract administration and aware of the contents and limits of their delegation of authority from the contracting officer.

(1) The contracting officer's technical representative (COTR) is the eyes and ears of the contracting officer, monitoring technical performance and reporting potential or actual problems to the contracting officer. It is imperative that the COTR be in close communication with the contracting officer, relaying any information that may affect contractual commitments and requirements.

(2) In an effort to ease the contracting process, the COTR should ensure that the contracting officer understands the program mission. In some cases, the COTR may invite the contracting officer to meetings, conferences, and inspections so that they can become familiar with program requirements. This also offers other field program personnel an opportunity to meet the contracting officer.

(3) The COTR's role and list of specific duties and tasks, including tasks that should not be performed, must be clearly identified in writing. Duties may be tailored specifically for each contract by listing specific duties and tasks relevant to that contract. The COTR's supervisor, contractor, and other individuals involved should also understand clearly the COTR's roles and functions.

*b. Partnering with IT suppliers.* Where appropriate and when approved by the contracting officer, partnering may be used in IT services contracts to help avoid future contract administration problems. Partnering is used to prevent disputes from occurring. It involves Government and contractor management mutually developing a "plan for success," usually with the aid of a neutral facilitator. The facilitator helps the parties create a positive relationship, define goals and identify the major obstacles to project success. The process results in the parties developing a partnership charter that serves as a roadmap for contract success.

*c. Performance-based contracting.* Performance-based contracting structures all aspects of an acquisition around the purpose of the work to be performed as opposed to either the manner by which the work is to be performed or broad and imprecise statements of work. IT service contracts must include the specific requirements of contractor performance to ensure that the Government's objectives are met. This arrangement aligns the vendor's financial incentives with the organization's goals.

*d. On-line assistance for acquisition problems.* Information on acquisition policies and issues is available from various Federal and DOD sources. The list below represents a few of those sites.

(1) The Acquisition, Technology, and Logistic Sharing System has the latest information on acquisition news and policy and helpful links. It features an online option, "Ask a Professor Keyword Search" for users to submit inquiries about specific acquisition issues (<http://akss.dau.mil/jsp/default.jsp>).

(2) In addition to schedule information, the FSS Web site includes a legal corner, a newsletter, and free online training at "UMAS Virtual Campus," on a wide range of acquisition topics ([www.fss.gsa.gov](http://www.fss.gsa.gov)).

(3) The Acquisition Reform Network (Federal) includes a virtual library and professional development opportunities ([www.arnet.gov](http://www.arnet.gov)).

## **11-6. Electronic purchases**

The ASCP IT e-mart is a Web-based catalog and electronic procurement software system that enables streamlined procurement operations. ASCP IT e-mart provides interactive agency-vendor processing for configuration checks and Requests for Quotes, single-point access to multiple contracts, quick ordering, and shopping cart functionality. The URL is <https://ascp.monmouth.army.mil>.

*a.* Anyone may search or browse the Web site. Users wishing to request a quote or execute a shopping cart must be logged in. Army users who are registered with AKO are automatically registered to use the site.

*b.* Business-to-business capabilities allow customers to order contract-compliant, custom-configured solutions direct from ASCP contract/BPA holder sites. Customers are transferred to partnering vendor sites where they can configure solutions, and bring these solutions back to IT e-mart for order processing.

*c.* Shopping carts may be sent through a user-defined approval/workflow process. This module assists customers in handling order approvals by providing cart information.

*d.* Customers may issue requests for quotes to one or more ASCP contract/BPA holders simultaneously using IT e-mart

*e.* IT e-mart provides backup documentation for IT orders. Contract-specific instructions and information is provided for Standard Form SF1449 (Solicitation/Contract/Order for Commercial Items) to aid customers in completing paper-based order requisitions.

*f.* The ASCP IT e-mart URL is <https://ascp.monmouth.army.mil>. If additional assistance is needed, the ASCP helpline is available at 888-232-4405 for CONUS and 732-532-7950 for OCONUS.

## **Appendix A References**

### **Section I**

#### **Required Publications**

The following publications are available on the APD Web site (<http://www.apd.army.mil>) unless otherwise stated. Department of Defense publications are available from <http://www.dtic.mil/whs/directives>. United States Code is available at <http://www.gpoaccess.gov/uscode>.)

#### **AR 25-1**

Army Knowledge Management/Information Technology. (Cited in paras title page summary, 1-1, 1-4, chap 2, 2-3, 2-4b, 2-4j(6), 3-1, 3-9f(1), 3-9f(2), 4-1a, 5-1a, 5-2a, 5-2c(1), 5-2f(1), 5-3, 5-3e, 5-3h(1), 6-3c, 6-4c, 7-1b(2), 7-1b(3), 7-1c(3), 7-1e, 7-2b, 7-2c, 7-2e, 7-3b(4), 7-4a, 7-5a, 7-6b, 7-6f, 7-7a, 8-1a, 8-1k(2), 8-1k(3), 8-2b(3), 8-2h, 8-2i, 8-3a, 8-4a, 8-6a, 8-7a(1), 8-7b(16), 9-1d, 9-1e(2)(c), 9-1f, 9-1g(4), 10-1a(1), 10-2k, 10-3f(3)(i)2, 10-4c, 10-9a, 10-9b, 10-9d(1), 10-9d(7).)

#### **AR 25-2**

Information Assurance. (Cited in paras 3-4e(1)(e), 3-4e(2), 3-4h(1)(a)1, 3-4h(2), 3-4h(2)(c), 3-4h(5), 6-4c(6), 7-1d, 7-8a(4), 8-7a(1), 8-7d(4)(e)2.)

#### **AR 70-1**

Army Acquisition Policy. (Cited in paras 10-9d(1), 10-9e, 11-1.)

#### **AR 71-9**

Materiel Requirements. (Cited in paras 6-5b(2)(j), 10-9a(4), 10-9d(1), 10-9e.)

### **Section II**

#### **Related Publications**

A related publication is a source of additional information. The user does not have to read a related publication to understand this publication.

#### **AR 25-6**

Military Affiliate Radio System (MARS)

#### **AR 5-12**

Army Management of the Electromagnetic Spectrum

#### **AR 25-11**

Record Communications and The Privacy Communications System

#### **AR 25-30**

The Army Publishing Program

#### **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

#### **AR 25-400-2**

The Army Records Information Management System (ARIMS)

#### **AR 71-32**

Force Development and Documentation—Consolidated Policies

#### **AR 210-7**

Commercial Solicitation on Army Installations

**AR 215-1**

Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities

**AR 340-21**

The Army Privacy Program

**AR 360-1**

The Army Public Affairs Program

**AR 380-5**

Department of the Army Information Security Program

**AR 380-53**

Information Systems Security Monitoring

**AR 500-3**

Army Continuity of Operations (COOP) Program. (Available only from Army Knowledge On-Line.)

**AR 500-60**

Disaster Relief

**AR 600-20**

Army Command Policy

**AR 608-1**

Army Community Service Center

**AR 710-2**

Supply Policy Below the National Level

**AR 735-5**

Policies and Procedures for Property Accountability

**DA Pam 25-5**

Preparing and Processing Requests for Long-Haul Information Transfer Services

**DA Pam 25-40**

Army Publishing: Action Officers Guide

**DA Pam 25-91**

Visual Information Procedures

**DA Pam 70-3**

Army Acquisition Procedures

**TRADOC Pam 71-9**

Requirements Determination

**Headquarters, Department of the Army**

The Army Resource Formulation Guide. (Available at [www.daqs.army.mil](http://www.daqs.army.mil) (subscription and login required).)

**DFAS-IN Manual 37-100-FY**

Army Management Structure (AMS). (Available at <https://dfas4dod.dfas.mil>.)

**DFAS-IN Regulation 37-1**

Finance and Accounting Policy Implementation. (Available at <https://dfas4dod.dfas.mil>.)

**United States Army**

Army Strategic Planning Guidance. (Available at [www.army.mil](http://www.army.mil).)

**ACP 190(B)**

Guide to Spectrum Management in Military Operations. (Available at [www.jcs.mil](http://www.jcs.mil).)

**CJCSI 3170.01E**

Joint Capabilities Integration and Development System. (Available at [www.dtic.mil](http://www.dtic.mil).)

**CJCSI 6211.02A**

Defense Information System Network (DISN): Policy, Responsibilities and Processes. (Available at [www.dtic.mil](http://www.dtic.mil).)

**CJCSI 6215.01B**

Policy for Department of Defense Voice Networks. (Available at [www.dtic.mil](http://www.dtic.mil).)

**CJCSI 6250.01B**

Satellite Communications. (Available at [www.dtic.mil](http://www.dtic.mil).)

**Department of Defense**

Defense Discovery Metadata Standard. (Available at <http://diides.ncr.disa.mil>.)

**Deputy Secretary of Defense Memorandum**

Information Technology Portfolio Management Policy, 22 March 2004. (Available at [www.dtic.mil/whs/directives](http://www.dtic.mil/whs/directives).)

**DFARS**

Defense Federal Acquisition Regulation Supplement. (Available at [www.acq.osd.mil](http://www.acq.osd.mil).)

**DISA Circular 310-130-1**

Submission of Telecommunications Service Requests. (Available at [www.disa.mil](http://www.disa.mil).)

**DISA Circular 310-D70-67**

Defense Information Infrastructure (DII) Defense Message System Transition Hub (DTH) Routing Doctrine for the General Service (GENSER) Community. (Available at [www.disa.mil](http://www.disa.mil).)

**DOD Memorandum, 4 June 2001**

Disposition of Unclassified DOD Computer Hard Drives. (Available at [www.drms.dla.mil](http://www.drms.dla.mil).)

**DOD Net-Centric Data Strategy**

Memorandum, Chief Information Officer, May 9 2003. (Available from [www.defenselink.mil/nii/doc/docArchive.html](http://www.defenselink.mil/nii/doc/docArchive.html).)

**DOD 5200.1-R**

Information Security Program.

**DOD 5120.20-R**

Management and Operation of Armed Forces Radio And Television Service (AFRTS)

**DOD 7000.14-R**

Department of Defense Financial Management Regulations (FMRs)

**DODD 1035.1**

Telework Policy for Department Of Defense

**DODD 3020.26**

Continuity of Operations (COOP) Policy and Planning

**DODD 4640.7**

DOD Telecommunication System (DTS) in the National Capital Region (NCR)

**DODD 4650.1**

Policy for Management and Use of the Radio Frequency Spectrum

**DODD 5240**

DOD Intelligence Activities

**DODD 8500.1**

Information Assurance (IA)

**DODD 8000.1**

Management of DOD Information Resources and Information Technology

**DODD 8320.2**

DOD Data Administration.

**DODD 8500.1**

Information Assurance

**DODI 1015.12, Enclosure 4**

Lodging Program Resource Management

**DODI 1100.21**

Voluntary Services in the Department of Defense

**DODI 3020.37**

Continuation of Essential DOD Contractor Services During Crisis

**DODI 4000.19**

Interservice and Intragovernmental Support

**DODI 4640.14**

Base and Long-Haul Telecommunications Equipment and Services

**DODI 5200.40**

DOD Information Technology Security Certification and Accreditation Process (DITSCAP)

**DODI 5335.1**

Telecommunications Services in the National Capital Region (NCR)

**DODI 8100.3**

Department of Defense (DOD) Voice Networks

**MCEB Pub 7**

Standard Frequency Action Format (SFAF), version 7—Final. (Available at [www.jsc.mil](http://www.jsc.mil).)

**MIL—STD—6040**

United States Message Text Formatting Program. (Available at <http://assist.daps.dla.mil>.)

**36 CFR Part 1194**

Title 36—Parks, Forests, And Public Property, Electronic and Information Technology Accessibility Standards. (Available at <http://ecfr.gpoaccess.gov>.)

**Executive Order 13011**

Federal Information Technology. (Available at [www.archives.gov/federal-register/executive-orders](http://www.archives.gov/federal-register/executive-orders).)

**FIPS 140-2**

Security Requirements for Cryptographic Modules. (Available at [www.itl.nist.gov/fipspubs](http://www.itl.nist.gov/fipspubs).)

**OMB Circular A-11**

Preparation, Submission and Execution of the Budget. (Available at [www.whitehouse.gov/omb/circulars](http://www.whitehouse.gov/omb/circulars).)

**OMB Circular A-76**

Performance of Commercial Activities. (Available at [www.whitehouse.gov/omb/circulars](http://www.whitehouse.gov/omb/circulars).)

**OMB Circular A-130**

Management of Federal Information Resources. (Available at [www.whitehouse.gov/omb/circulars](http://www.whitehouse.gov/omb/circulars).)

**OMB Memorandum, 26 September 2003**

Guidance for Implementing the Privacy Provision of the E-Government Act of 2002. (Available at [www.whitehouse.gov/omb/memoranda](http://www.whitehouse.gov/omb/memoranda).)

**Public Law 104–106**

National Defense Authorization Act for Fiscal Year 1996. (Available at [www.gpoaccess.gov/uscode](http://www.gpoaccess.gov/uscode).)

**5 USC 552**

Freedom of Information Act

**5 USC 552a**

The Privacy Act

**10 USC 1588(f)**

Authority to accept certain voluntary services: Authority To Install Equipment

**17 USC Chapters 1 and 2**

Software copyrights

**29 USC 794d**

“Section 508”—Nondiscrimination under Federal grants and programs: Standards used in determining violation of section

**40 USC Subtitle III**

Information Technology Management

**40 USC Section 11103**

“National security system\”” defined

**44 USC Chapter 35**

Coordination of Federal Information Policy

**47 USC 153**

Wire or Radio Communication

**47 USC 255**

Access by persons with disabilities

**FTR 1080B–2002**

Video Teleconferencing Services. (Available at [www.ncs.gov/library.html](http://www.ncs.gov/library.html).)

**IEEE 802**

LAN/MAN Standards. (Available at no cost to DOD personnel; contact Defense Automation and Production Service, 700 Robbins Ave., Bldg. 4, Philadelphia, PA 19111–5094.)

**IEEE/EIA 12207.0–1996**

Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software Life-Cycle Processes. (Available at no cost to DOD personnel from Defense Automation and Production Service, 700 Robbins Ave., Bldg. 4, Philadelphia, PA 19111–5094.)

**ISO/IEC 11179**

Information Technology—Metadata Registries. (Available at <http://metadata-standards.org>.)

**NIST Special Publication 800–44**

Guidelines on Securing Public Web Servers Recommendations. (Available at <http://csrc.nist.gov>.)

**Section III**

**Prescribed Forms**

This section contains no entries.

## **Section IV**

### **Referenced Forms**

The following forms are available on the Army Electronic Library CD–Rom and the APD Web site ([www.apd.army.mil](http://www.apd.army.mil)) unless otherwise stated. DD forms are available from the Office of the Secretary of Defense Web site ([www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm](http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm)).

#### **DA Form 12–R**

Request for Establishment of a Publications Account

#### **DA Form 2407**

Maintenance Request

#### **DA Form 3161**

Request for Issue or Turn-In

#### **DD Form 1144**

Support Agreement

#### **DD Form 1348–1A**

Issue Release/Receipt Document

#### **DD Form 1348–2**

Issue Release/Receipt Document with Address Label

#### **DD Form 1391**

FY\_\_ Military Construction Project Data

#### **DD Form 1494**

Application for Equipment Frequency Allocation

#### **DISA Form 772**

Telecommunications Management System—Classified. (Available from [www.disa.mil](http://www.disa.mil), then click the “Contact us” button to request form.)

#### **DLIS Form 1867**

Certification of Hard Drive Disposition. (Available from [www.drms.dla.mil/turn-in](http://www.drms.dla.mil/turn-in).)

#### **Standard Form 1449**

Solicitation/Contract/Order for Commercial Items. (Available from [www.dtic.mil/whs/directives](http://www.dtic.mil/whs/directives).)

## **Appendix B**

### **Sample Telework Application and Agreement**

Telecommuting is designed to benefit employees, managers and the community by decreasing work trip vehicle miles, traffic/parking congestion, energy consumption, and air pollution; improving the quality of work life and performance; and improving morale by assisting employees in balancing work and family demands. The information in this appendix is designed to assist an organization to develop the necessary documents to implement a successful telework program.

#### **B–1. Sample telework application and agreement**

*a. Section I (to be completed by the employee).*

- (1) Employee name.
- (2) Organization.
- (3) Telephone.
- (4) Supervisor name and title.
- (5) Telephone.
- (6) Address and description of alternate work site.
- (7) Telephone.
- (8) Description of work to be performed at the alternate workplace.
- (9) Equipment needed to perform work at the alternate workplace is furnished—

- (a) By the employee.
  - (b) By the agency.
- (10) Telework schedule and tour of duty:
- (a) Regularly scheduled.
  - (b) Intermittent.
- (11) Work schedule hours.
- (12) Alternative work schedule day off (if applicable).
- (13) Telework days.
- (14) Voluntary participation. The applicant voluntarily agrees to work at the approved alternate workplace indicated above and to follow all applicable policies and procedures. The applicant recognizes that the telework arrangement is a privilege, not a right.
- (15) Salary and benefits. The supervisor and applicant agree that a telework arrangement is not a basis for changing the applicant's salary or benefits.
- (16) Official duties. The applicant agrees not to conduct personal business while in an official duty status at the alternate work place (for example, caring for dependents or making home repairs). Furthermore, the applicant agrees that telework is not a substitute for childcare, and that he or she will make appropriate arrangements for childcare as necessary to provide for a minimum of interruptions during the workday.
- (17) Time and attendance. The supervisor agrees to certify biweekly the time and attendance for hours worked at the regular office and the alternate workplace and to make sure that the applicant's timekeeper has a copy of the applicant's work schedule. The employee will be required to complete a time and attendance worksheet to document hours worked.
- (18) Leave. The applicant agrees to follow established office procedures for requesting and obtaining approval for leave.
- (19) Overtime. The applicant agrees to work overtime only when approved in writing and in advance by the supervisor and understands that claimed overtime work without such approval may result in termination of the telework privilege.
- (20) Alternate workplace costs. The employee understands that the Government is not obligated for any operating costs that are associated with the use of the employee's home as an alternate work site, for example, home maintenance, insurance or utilities. The employee also understands that any entitlement to reimbursement for authorized expenses incurred while conducting business for the Government, as provided for by statute or regulation, is not relinquished by this agreement.
- (21) Equipment/supplies. The employee agrees to protect any Government-owned equipment and to use the equipment only for official purposes. The agency agrees to issue service and maintain any Government-owned equipment issued to the employee (see para 9-1g). The employee agrees to service and maintain any employee-owned equipment used. The agency agrees to provide the employee with all necessary office supplies, such as a Government calling card for business-related long-distance calls.
- (22) Security. The applicant agrees to follow all existing security policies and procedures. Privacy Act data, and other sensitive or classified data may not be accessed or used from the alternate workplace. Remote access to the network will be granted, as needed.
- (23) Information assurance. The applicant agrees to follow all information assurance requirements identified by the designated approving authority. The applicant agrees to complete user security awareness training, participate in all required training program, and protect information at all times.
- (24) Liability. The applicant understands that the Government will not be held liable for damages to his/her personal or real property while (s)he is working at the approved alternate workplace, except to the extent the Government is held liable under the Military Personnel and Civilian Employees Claims Act and the Federal Tort Claims Act.
- (25) Alternate work site inspection. The employee agrees to permit the Government to inspect the alternate work site during the employee's normal working hours to ensure proper maintenance of Government-owned property and conformance with safety standards. This is in addition to the self-certification that the employee must complete.
- (26) Work area. An applicant working at home agrees to provide a designated work area adequate for performance of official duties.
- (27) Injury compensation. The applicant understands that (s)he is covered under the Federal Employees Compensation Act if injured in the course of actually performing official duties at the alternate workplace. The applicant agrees to notify his/her supervisor immediately of any accident or injury that occurs at the alternate workplace and to complete any required forms. The supervisor agrees to investigate such a report as soon as possible.
- (28) Work assignments/performance. The employee agrees to complete all assigned work according to guidelines and standards in the employee performance plan. The applicant and supervisor agree to exercise good communication skills and work cooperatively to obtain a common understanding of expectations and desired results, and set reasonable and measurable objectives for work to be accomplished. The employee agrees to provide regular reports if required by

the supervisor to help judge performance. The employee understands that a decline in performance may be grounds for terminating or modifying the telework arrangement.

(29) Disclosure. The applicant agrees to protect Government records from unauthorized disclosure or damage and will comply with requirements of the Privacy Act of 1974, 5 USC 552(a).

(30) Standards of conduct. The applicant agrees that (s)he is bound by official standards of conduct while working at the alternate workplace.

(31) Cancellation. The applicant understands that the organization may cancel the telework arrangement and instruct him/her to resume working at the office. If the applicant elects to voluntarily withdraw from the program, (s)he is expected to give sufficient notice so that arrangements can be made to accommodate his/her return to a regular work schedule and (s)he must complete the Telework Termination Form.

(32) Compliance with this agreement. The employee's failure to comply with the terms of this agreement may result in the termination of this agreement and the telework arrangement. Failure to comply also may result in disciplinary action against the employee if just cause exists to warrant such action.

(33) Term. Unless canceled or terminated earlier by either the employee or the employer, this agreement shall expire on            (enter date), unless renewed by agreement of the employee and the employer.

(34) Certification. By signing this agreement, the applicant certifies that (s)he has read the terms of this agreement and agrees to follow the policies and procedures outlined in them as well as all other applicable policies and procedures.

(35) Applicant's signature.

(36) Date.

*b. Section II (to be completed by the supervisor and approving official).*

(1) Supervisor's recommendation. I recommend that the application and agreement be—

(a) Approved as written.

(b) Approved with the following modification.

(c) Disapproved for the following reason(s):

1. Work not suited to telework.

2. Need for office coverage.

3. Employee is in a developmental assignment or position.

4. Alternate work site does not conform with safety requirements.

5. Employee failed to attend required training on telework.

6. Other (please specify).

(2) Approving official's decision:

(a) I concur with the above recommendation.

(b) I disagree with the above recommendation for the following reason(s):

1. Work not suited to telework.

2. Need for office coverage.

3. Employee is in a developmental assignment or position.

4. Alternate work site does not conform with safety requirements.

5. Employee failed to attend required training on telework.

6. Other (please specify).

(3) Approving official's signature.

(4) Date.

## **B-2. Telework safety assessment**

*a.* This assessment is to be completed only if the proposed alternate workplace is located in a private residence. This checklist is designed to assess the overall safety of the designated work area of the alternate workplace. Each applicant should read and complete the self-certification safety checklist. Upon completion, the checklist should be signed and dated by the applicant.

*b.* Applicant.

*c.* Telephone.

*d.* Location of alternate workplace.

*e.* Telephone.

*f.* Describe the designated work area.

*g.* Within the designated work area—

(1) Are all stairs with four or more steps equipped with handrails?

(a) Yes

(b) No

(c) N/A

- (2) Are all circuit breakers and/or fuses in the electrical panel labeled as to intended service?  
(a) Yes  
(b) No  
(c) N/A
- (3) Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through the walls, exposed wires fixed to the ceiling)?  
(a) Yes  
(b) No  
(c) N/A
- (4) Will the building's electrical system permit the grounding of electrical equipment?  
(a) Yes  
(b) No  
(c) N/A
- (5) Are aisles, doorways, and corners free of obstructions to permit visibility and movement?  
(a) Yes  
(b) No  
(c) N/A
- (6) Are file cabinets and storage closets arranged so drawers and doors do not open into walkways?  
(a) Yes  
(b) No  
(c) N/A
- (7) Are the chair casters (wheels) secure and the rungs and legs of the chair sturdy?  
(a) Yes  
(b) No  
(c) N/A
- (8) Are the phone lines, electrical cords, and extension wires secured under a desk or alongside a baseboard?  
(a) Yes  
(b) No  
(c) N/A
- (9) Is the office space neat, clean, and free of excessive amounts of combustibles?  
(a) Yes  
(b) No  
(c) N/A
- (10) Are floor surfaces clean, dry, and level?  
(a) Yes  
(b) No  
(c) N/A
- (11) Are carpets well-secured to the floor and free of frayed or worn seams?  
(a) Yes  
(b) No  
(c) N/A
- (12) Is there sufficient light for reading?  
(a) Yes  
(b) No  
(c) N/A
- (13) Computer workstation (if applicable):
- (14) Is your chair adjustable?  
(a) Yes  
(b) No
- (15) Do you know how to adjust your chair?  
(a) Yes  
(b) No
- (16) Is your back adequately supported by a backrest?  
(a) Yes  
(b) No
- (17) Are your feet on the floor or fully supported by a footrest?

- (a) Yes
- (b) No
- (18) Are you satisfied with the placement of your monitor and keyboard?
- (a) Yes
- (b) No
- (19) Is it easy to read the text on your screen?
- (a) Yes
- (b) No
- (20) Do you need a document holder?
- (a) Yes
- (b) No
- (21) Do you have enough leg room?
- (a) Yes
- (b) No
- (22) Is the screen free from noticeable glare?
- (a) Yes
- (b) No
- (23) Is the top of the screen at eye level?
- (a) Yes
- (b) No
- (24) Is there space to rest your arms while not keying?
- (a) Yes
- (b) No
- (25) When keying, are your forearms close to parallel with the floor?
- (a) Yes
- (b) No
- (26) Are your wrists fairly straight when keying?
- (a) Yes
- (b) No

*h.* By signing this document, the applicant certifies that all of the above applicable questions were answered in the affirmative or, if answered in the negative, that the applicant will take all necessary corrective actions to eliminate any hazard (as revealed by a negative response) before he/she begins to telework:

- (1) Applicant's signature.
- (2) Date.

### **B-3. Supervisory-employee policies and procedures list**

The following list is designed to ensure that the teleworker and supervisor are properly oriented to the policies and procedures of the telework program (h, i, and j may not be applicable to the telework employee. If this is the case, state nonapplicable or NA. The following information is entered:

- a.* Employee name.
- b.* Supervisor's name.
- c.* Employee/supervisor has read AR 25-1, paragraph 6-10 and paragraph 7-6 of this document and reviewed DOD telework policy located at [www.cpms.osd.mil/fas/telework/dod-telework-policy.htm](http://www.cpms.osd.mil/fas/telework/dod-telework-policy.htm). Enter date.
- d.* Employee has been provided with a schedule of work hours. Enter date.
- e.* Employee has been issued/has not been issued Government furnished equipment. (If no equipment has been issued please mark N.A. on the date line.) Enter date.
- f.* Army-issued equipment is documented and properly receipted. Check as applicable:
  - (1) Computer
    - (a) Yes
    - (b) No
  - (2) Modem
    - (a) Yes
    - (b) No
  - (3) Fax machine
    - (a) Yes
    - (b) No
  - (4) Telephone

- (a) Yes
- (b) No
- (5) Other
- (a) Yes
- (b) No

g. Policies and procedures for care of equipment issued by the agency have been explained and are clearly understood. Enter date.

h. Policies and procedures covering classified, secure, or Privacy Act data have been discussed and are clearly understood. Enter date.

i. Policies and procedures covering information assurance operations of the equipment and IA functions have been discussed and clearly understood. Enter date.

j. Requirements for an adequate and safe office space and/or area have been discussed, and the employee certifies those requirements are met. Enter date.

k. Performance and conduct expectations have been discussed and are clearly understood. Enter date.

l. Employee understands that the supervisor may terminate employee participation in accordance with established administrative procedures and union-negotiated agreements. Enter date.

m. Employee has participated in training. Enter date.

n. Supervisor has participated in training. Enter date.

o. Telework Agreement has been completed and signed. Enter date.

p. Enter employee's signature and date.

q. Supervisor's signature and date.

#### **B-4. Telework termination form**

a. The telework option is not an employee right but falls rather under the supervisor's discretion to determine how work should be accomplished with the organization. Termination from the telework agreement can be either voluntary or involuntary. This is notification that the telework agreement signed on \_\_\_ (enter date) is no longer in effect and is hereby terminated. Enter the following information:

b. Employee's name.

c. Organization.

d. Termination is based on (please check one)—

(1) Voluntary withdrawal.

(2) Involuntary withdrawal.

e. If involuntarily terminated, this decision was based on—

(1) Requirements of the current work assignment.

(2) Reassignment or change in duties.

(3) Lack of office coverage.

(4) Failure to maintain eligibility standards (please specify).

(5) Other (please specify).

f. Employee's signature and date.

g. Supervisor's signature and date.

h. Approving official's signature and date.

## **Appendix C Funding, Billing, and Accounting for Information Resources**

### **C-1. Billing and accounting for official phone services**

Policy regarding official phone service (Classes A, C and D) is found in AR 25-1, paragraph 6-1d.

a. Installations may control commercial communications costs by creating certification procedures that ensure payment occurs only when services are needed and received. Activities and organizations appoint TCOs to review their parts of commercial and Defense Working Capital Fund bills. This list of bills must be provided to the TCO when they are appointed so they understand their roles.

b. Installation DOIM or Deputy Chief of Staff for Information Management (DCSIM) offices publish written policy detailing firm guidelines for using official Government phone service, recovery procedures where individuals use official services for personal use, and penalties, if applicable. Such policies are staffed with the supporting staff Judge Advocate prior to being circulated.

c. The DOIM receives communications bills from service providers, sorts them by activity or unit, and distributes

them to appropriate TCO(s). Bills must be paid promptly to avoid late payment charges. TCOs should review commercial billings carefully and certify that all charges appearing on bills are for official Government business only.

*d.* Where use is found outside what is permitted by AR 25-1, paragraph 6-1*d*, immediate action is taken to recover the cost of unauthorized calls. The phone customer service office and DFAS process cash collection vouchers. If organizations deem disciplinary action appropriate for abuse of Government phone service, the Civilian Personnel Administration Center (CPAC) or Civilian Personnel Operations Center (CPOC) should be consulted in the case of U.S. Government civilian employees; military commanders in the case of military personnel; and contracting officers in the case of contractors or their employees (see fig C-1 for information regarding telecommunication bill certification actions).

- 
1. Review and understand each component of the bill. This knowledge is essential to an understanding of what monthly recurring cost should be paid. TCOs need to understand these components of the bill certification process: How adjustments are applied. Where late charges appear. How late charges are calculated. How taxes are calculated. What comprises the monthly recurring cost. How late charges are calculated.
  2. Consolidate vendor bills into a summary account bill, aiming to receive just one monthly bill from each telecommunications vendor.
  3. Ensure the bills conform to both services rendered and to contract terms.
  4. Request a customer service request from the vendor that itemizes the services on the bills. Become familiar with the format of these and DSN call detail reports.
  5. Reconcile monthly billings with applicable tariffs, communications service authorizations, and customer service requests to make sure bills for services rendered match the contract amount and tariffs.
  6. Ensure that services received are covered by communications service authorizations.
  7. Investigate any differences in bills, customer service requests, communications service authorizations, and tariffs.
  8. Initiate procedures to resolve disparities between billings, services rendered, contracts, and tariffs.
  9. Monitor bills until full compliance is achieved. This procedure is essential if trend analysis is to be a useful tool.
  10. Monitor services to determine if they are used; if not, notify the contracting officer's representative or request for service submission POC so they can terminate unnecessary services and modify the CSA.
  11. Request credits for overpayments when identified. A refund check is sent to the U.S. Treasury.
  12. Review tariffs quarterly to ensure rates have not changed and that untariffed services have been changed to tariffed services. The contracting officer's representative should keep a file of applicable tariffs and proposed tariff adjustments sufficient to explain monthly recurring costs.
  13. Maintain a trend analysis. Compare monthly recurring cost, long-distance charges, and total bill for each account with the previous month's to see if any major changes occurred. Investigate unusual changes and take proper action.
  14. Discuss disputes immediately with vendors' customer service representatives or your Resource Management POC at the ATD, and follow up to resolve questionable charges as soon as possible. Adjust payments accordingly, and ensure any agreed-upon adjustments are reflected in the next bill.
  15. Streamline the voucher payment process.
  16. Date-stamp bills when received to document the date it arrived and start the late-payment clock.
  17. Automate the Vendor Payment Journal and expand its use to help reconcile vendor accounts, so the Phone Control Coordinator will know the exact status of each account at all times.
  18. Obtain and use the automated version of Standard Form 1034 (Public Voucher for Purchases and Services Other Than Personal).
  19. Process bills in a timely manner. Prioritize workload to allow time to prepare Standard Forms 1034 for phone bills upon receipt. Accelerate internal routing by hand-carrying the payment packages to the Funds Control Officer, particularly when tariff provisions allow late charges.
  20. Investigate questionable long-distance charges after the bill is paid. If they are invalid billing items, request a credit from the phone company. If they are unofficial calls, request payment from the party making the call.
  21. Request "read-only" access to DFAS databases to—
    - a. Review the status and amounts of telecommunications vendor payments processed by the DFAS.
    - b. Aid in resolving payment questions from vendors.
  22. Ask the Director of Resource Management to provide the TCO with a copy of the paid-voucher packages when the DFAS sends the packages to the installation.

Figure C-1. List of telecommunications bill certification actions

---

e. AR 25-1, paragraph 6-4d(6) says that the installation commander establishes local policy for handling incoming official collect calls. Installation DOIMs assist installation commanders in developing written policy specifying who can authorize incoming collect calls, procedures for documenting receipt of collect calls, and guidance for certifying collect calls on phone bills. TCOs, IMOs, or other designated individuals who verify commercial billings before payment certify that collect calls were for official use and authorized for payment.

f. AR 25-1, paragraph 6-4f governs the ordering and use of phone calling cards. It states that phone calling cards are only used for official business, when the cardholder is away from the normal duty station (and outside the local calling area), and in a location where no Government service is available. Prepaid calling cards may be used instead of cards issued by the phone service provider if they meet user requirements.

(1) Phone calling cards require special security precautions to prevent unauthorized use. Cards are canceled when the card holder separates from the organization, no longer requires a calling card, or when it is believed a calling card number has been compromised.

(2) The TCO should cancel the calling card by notifying the DOIM in writing. Replacement cards may be issued if necessary. Unissued or returned cards must be kept in a locked/secure area. When issuing correspondence regarding calling cards, leave off or cross out the personal identification number (PIN). The PIN is the last four numbers on the calling card (for example, 123-456-7890-XXXX). This makes it more difficult to use the card number should it be compromised. Individuals who misuse calling cards may face administrative actions or judicial penalties.

g. The TCO must exercise continual management over cellular phone bills as the potential for fraud, waste, or abuse in the use of the phone as well as inaccurate billing is more for cellular phones than most other phone equipment. The TCO must establish internal controls so that every cellular phone is assigned to an individual who uses it. Stolen/or missing cellular phones must be reported to the DOIM office immediately so service can be canceled to prevent illegal use/charges. Cellular phones must not be used when other less costly phone service is available (see AR 25-1, para 6-4w for Army policy on the issuance and use of mobile, portable, and cellular phones).

h. The ATD, NETCOM/9th ASC provides aid to installations on measures to reduce telecommunications costs. The major monthly cost of an installation's telecommunications bill is from long distance calls, either FTS (commercial) or DSN. Installations and separate reporting activities may institute the measures identified in figure C-2 to reduce telecommunications costs without degrading service.

- 
1. Use Personal Identification Numbers (PIN) on local long distance, FTS, and DSN services. This has proven to largely reduce phone system abuse. Review all long distance, FTS, and DSN calls monthly and have the PIN holders certify that all calls are government business.
  2. Issue an order to the commercial carriers to block third party calls and collect calls on all government switches and business lines as well as official business lines not on government premises. Issue calling cards to personnel on temporary duty to make required calls. Card holders should use cards when access to FTS, DSN, or other government local long distance service is unavailable.
  3. Use official calling cards through commercial phone services instead of cellular phone service to call long distance.
  4. When possible, make FTS2001 the long distance carrier on government switches and business lines, as well as official business lines not on government premises. For example, using FTS for all ROTC phone services provides a low-cost carrier service for an office that must conduct business mainly through commercial and not DSN phone service.
  5. Issue orders to commercial carriers to block directory assistance on government switches and business lines as well as official business lines not on government premises.
  6. Review the need and use of DSN precedence lines. Use of these lines results in additional charges over the usage charges to have the capability.
  7. Analyze monthly DSN and FTS service bills for duplicate bills, calls of excessive duration, numbers called excessively, use of DOD operators to place local and long distance calls, and calls to other installations off-netted to make calls to home or connect to local phone systems. Become familiar with automated operator numbers such as XXX-4663 (HOME). These numbers allow users to transfer calls off post without coordinating through human operators. Identify and report abuse of Government telecommunications systems.
  8. Establish local policy to prohibit the use of 1-800 calls from within the local area vice calling the local numbers. The most common misuse is using the TSACS National Phone Number or the Installation TSACS Number when access to TSACS is available through a local installation number.
  9. Ask that the local phone company block all collect and third-party calls.
  10. To avoid incurring late charges, date/time stamp bills upon receipt to restart the payment period on commercial phone bills. Payment of phone bills by use of a government credit card expedites bill paying and avoids late charges.
  11. Check the requirement for paying state or local taxes. The Federal government is not required to pay state or local taxes in some states.
  12. Check tariffs to ensure that the rate being charged is the most economical tariff rate or at least no greater than the established tariff. Rates paid to the local phone company are controlled by tariffs established by the State Public Utility Commission and the Federal Communications Commission.
  13. Inventory all phone services and combine them into one requirements package for open competition. This can result in lower prices due to a larger volume of services and a commitment to retain the services for a longer period of time rather than month-to-month service.
  14. Reconcile phone numbers billed against the phone numbers actually used. Request that customers inventory their accounts on regularly to ensure that bills correspond to the services required.

**Figure C-2. Optional measures to reduce telecommunications costs**

---

*i.* Policy regarding Class B service is found in AR 25-1 paragraph 6-3c. Policy and procedures regarding charges for Class B service and distribution of revenues are found in DFAS-IN Manual 37-1, paragraph 37-40.

(1) In some locations, the Government provides Class B service primarily for the use of occupants of Government housing and other unofficial subscribers. Class B service is provided on a pay-for-service or reimbursable basis. In addition to fixed monthly charges, Class B subscribers must pay for installations, moves, extensions, special equipment, and tolls. Appropriated funds are not used to pay for Class B service. Where practical, individual subscribers pay for Class B service by payroll deduction. This is coordinated between the DOIM and DFAS.

(2) Rates for Class B service are established by DOD. Because rates normally change annually, DOIMs providing Class B service must be aware of Class B rates and update customer charges promptly when notified of rate changes. Distribution of Class B revenues is compliant with DFAS-IN Manual 37-1, paragraph 37-40e(2).

(3) Charges for Class B service relocations resulting from on-post Government quarters movements of personnel are paid by the subscriber, unless the move is directed by the Government or is for the convenience of the Government.

The subscriber may present a claim for reimbursement of reconnect charges to the supporting Finance and Accounting Office. Permanent change-of-station moves are excepted.

### **C-2. Billing for long-haul services**

*a.* Bills for Army long-haul communications services are processed through the ATD. Customers submit a military interdepartmental purchase request to the ATD quarterly or annually for services based on estimates received from the ATD.

*b.* Estimates are derived from the customer cost and obligations report and from new or changed telecommunications requests submitted through Defense Information Systems Agency's Web order entry system (see para 5-16*d*). The ATD produces monthly invoices for each customer account. These invoices, and other relevant billing information, are found on the ATD Web page. Individuals with a need to know can obtain access to this page or additional billing information by sending an e-mail to: ato\_automation@hqasc.army.mil.

### **C-3. Funding for cable television**

*a.* CATV is commercially owned and operated, and is primarily intended for the use and enjoyment of personnel occupying quarters on military installations (see AR 25-1, para 6-3*w*).

*b.* DOD installations are CATV franchising authorities for the purpose of applicable CATV laws. Installations may issue a franchise, which grants a CATV company access to the installation and designated rights of way to permit the company to serve its subscribers. The installation commander is the franchising authority. When appropriate, the installation commander may designate a NAF instrumentality to be the franchising authority. The MWR director may be chosen as the primary authority over the cable franchising or renewal process. The individual subscriber to the CATV service contracts directly with the cable company for service and the payment of subscription fees.

*c.* No appropriated funds are involved in paying for individual services. However, appropriated funds may be used to pay for CATV service when procured by contract for DOD components subscribing to CATV services for official DOD business per the FAR. If such services are procured by appropriated fund activities, they are procured from the franchise. When using appropriated funds, DOD activities obtain services through official contracting channels, and payment is made through the supporting finance and accounting service.

*d.* Neither the award of a CATV franchise agreement nor the decision to procure CATV services for appropriated fund activities requires the Government to pay for CATV services for nonappropriated fund activities or individual subscribers. Nonappropriated funds activities and individual subscribers enter into their own agreements. Appropriated funds properly available for morale and welfare purposes may be expended for user and connection fees for services to appropriated fund activities that serve the community, but not individuals. Examples of these activities are hospital patient lounges and barracks day rooms.

*e.* Appropriated funds are authorized for CATV (installation and service, including a premium channel) in Army lodging in accordance with DODI 1015.12, encl 4.

*f.* The installation DOIM provides procedural guidance regarding CATV services, payment, and required approvals for official use of CATV to subscribers within their areas of supervision. The DOIM provides technical assistance to the installation contracting officer in determining the technical capabilities of potential CATV providers, reviewing the providers' proposals for technical proficiency, and assessing the fair value of existing facilities. Specific policy guidance regarding CATV in OCONUS locations is found in DOD 5120.20-R, chapter 10. In OCONUS areas, the Armed Forces Information Service, though the Armed Forces Radio and Television Broadcasting Center is the only source authorized to negotiate for or procure and distribute commercial and public broadcasting service programming to U.S. forces overseas.

*g.* Requests for approval of non-Armed Forces Radio and Television Broadcasting Center cable systems and satellite receiver stations on Army installations overseas are processed through the MACOM and Unified Command public affairs offices through HQDA to Office of the Assistant Secretary of Defense (PA), Director, AFIS.

*h.* DA Pam 25-91 covers procedures on VI-operated command channels that are provided as part of a CATV franchise agreement.

## **Glossary**

### **Section I Abbreviations**

#### **AAFES**

Army and Air Force Exchange Service

#### **ACS**

Army Community Services

#### **ACSIM**

Assistant Chief of Staff for Installation Management

#### **ADAS**

Automated Directory Assistance System

#### **ADHI**

Army data harmonization and integration

#### **ADP**

Architecture development plan

#### **ADS**

Authorative data sources

#### **AEA**

Army Enterprise Architecture

#### **AITR**

Army Information Technology Registry

#### **AKM**

Army Knowledge Management

#### **AKM SP**

Army Knowledge Management Strategic plan

#### **AKO**

Army Knowledge Online

#### **AMC**

Army Materiel Command

#### **ANCDMP**

Army Net-Centric Data Management Program

#### **ANSI**

American National Standardization Institute

#### **AONS**

Architecture, operations, networks, and space

#### **AOR**

Army infostructure operational area

#### **AR**

Army regulation; Army Reserve

#### **ARM**

Asset and resource management

**ARNG**

Army National Guard

**ARM**

Asset and Resource Management

**ASA(ALT)**

Assistant Secretary of the Army for Acquisition Logistics and Technology

**ASB**

Army Signal Battalion

**ASCP**

Army Small Computer Program

**ASD(NII)**

Assistant Secretary of Defense (Networks and Information Integration)

**ASD(NII)**

Assistant Secretary of Defense (Networks and Information Integration)

**ATD**

Army Telecommunications Directorate

**ATMS**

Asynchronous transfer mode switches

**ATO**

Authority to operate

**AV**

All view

**AWRAC**

Army Web risk assessment cell

**BASECOM**

Base Communications

**BES**

Budget estimate submission

**BPA**

Blanket purchase agreement

**BRS**

Base radio system

**C4**

Command, control, communication, and computers

**CADM**

Core architect data model

**CAP**

Compter/Electronic Accommodations Program

**CATV**

Cable television

**CDAd**

Component data administrator

**CES**

Core enterprise services

**CFR**

Code of Federal Regulations

**CIO**

chief information officer

**CIO/G-6**

Chief Information Officer/G-6

**CIR**

Capital investment report

**CJCSI**

Chairman of the Joint Chiefs of Staff Instruction

**CM**

Configuration management

**COI**

Community of interest

**CONUS**

Continental United States

**COTR**

Contracting officer's technical representative

**COTS**

Commercial off the shelf

**CPIM**

Capital planning and investment management

**CPU**

Central processing unit

**CSA**

Chief of Staff, Army

**CSDS**

Circuit Switched Data Service

**CSS**

Circuit switched service; Commercial Satellite Survey

**CSTP**

Commercial Satellite Terminals Program

**CUITN**

Common user installation transport network

**DBMS**

Database Management System

**DCASS**

Defense Communications and Army Switched Systems

**DEERS**

Defense Enrollment Eligibility Reporting System

**DFARS**

Defense Federal Acquisition Regulations Supplement

**DFAS**

Defense Finance and Accounting Service

**DISA**

Defense Information Systems Agency

**DISN**

Defense Information Systems Network

**DISR**

DOD IT Standards Registry

**DITCO**

Defense Information Technology Contracting Office

**DITSCAP**

DOD information technology security certification and accreditation process

**DLAN**

Departmental LAN

**DMS**

Defense Message System

**DOD**

Department of Defense

**DODAF**

DOD architecture framework

**DODD**

Department of Defense directive

**DODI**

Department of Defense instruction

**DOIM**

Director of Information Management

**DPP**

Defense performance planning

**DPPS**

Data Performance Planning System

**DPW**

Director of public works

**DRMO**

Defense Reutilization Management Office

**DRMS**

Defense Reutilization and Marketing System

**DSN**

Defense switched network

**DTH**

DMS Transition Hub

**DTID**

Disposal turn-in document

**DTS**

Dedicated transmission service

**DVS**

Defense video services

**DVS-G**

Defense video services-global

**DVTC**

Desktop Video Teleconferencing Systems

**EB**

Executive board

**EID**

Enterprise identifiers

**EIE**

Enterprise information environment

**EIT**

Electronic and information technology

**ELA**

Enterprise license agreement

**EMSS**

Enhance mobile satellite service

**ES**

Enterprise services

**ESA**

Enterprise system agreement

**ESI**

Enterprise software initiative

**ESTA**

Enterprise system technology activity

**FAQs**

Frequently asked questions

**FAR**

Federal Acquisition Regulation

**FCC**  
Federal Telecommunications Commission

**FDED**  
Ft. Detrich Engineering Directorate

**FDEO**  
Ft. Detrich Engineering Office

**FMA**  
Family member account

**FOA**  
field operating agency

**FOIA**  
Freedom of Information Act

**FRS**  
Frame Relay Service

**FSS**  
Federal Supply Schedule

**FTR**  
Federal telecommunications recommendations

**FTS**  
Federal Telephone System

**FY**  
Fiscal year

**GIG**  
Global Information Grid

**GILS**  
Government Information Locator Service

**GPRA**  
Government Performance and Results Act

**GPS**  
Global Positioning Service

**GSA**  
General Services Administration

**HF**  
High frequency

**HMW**  
Health, morale, welfare

**HQ**  
Headquarters

**HTTP**  
Hypertext Transfer Protocol

**IA**

Information assurance

**IASO**

Information assurance security offices

**ICDB**

Integrated communications database

**IEEE/EIA**

Institute of Electrical and Electronic Engineers/Electrical Industries Association

**IESS**

Information exchange standard specifications

**IM**

information management

**IMA**

Installation Management Agency

**IMO**

Information management office/officer

**Inmarsat**

International maritime satellite

**IP**

Implementation plan; internet protocol

**IPS**

Internet protocol internetworking service

**IRM**

Information Resources Management

**ISCE**

Information systems cost estimate

**ISDN**

Integrated services digital network

**ISO**

International Organization for Standardization

**ISR**

Installation status reporting

**IT**

information technology

**ITAPDB**

Integrated Total Army Personnel Database

**ITM**

Information technology management

**ITU-T**

International Telecommunications Union—Telecommunications

**ITU-TSS**

International Telecommunications Union-Telecommunications Standard Sector

**JSPA**

Joint SATCOM Panel Administrator

**JWCA**

Joint Warfighting Capability Assessment

**JWRAC**

Joint Web Risk Assessment Cell

**KC**

Knowledge Center

**KCC**

Knowledge Center collaboration

**LAN**

Local area network

**LATA**

Local Access and Transport Area

**LCM**

life-cycle management

**LMR**

land mobile radio

**LWN**

LandWarNet

**MACOM**

major Army command

**MARS**

Military Affiliate Radio System

**MDEP**

Management Decision Package

**MILCON**

Military construction

**MWR**

Morale, welfare, and recreation

**NAF**

Nonappropriated fund

**NCES**

Net-centric Core Enterprise Services

**NETCOM**

Network Enterprise Technology Command

**NETCOP**

Network Common Operational Picture

**NETOPS**

network operations

**NII**

Networks and information integration

**NIPRNET**

Nonclassified internet protocol router network

**NIST**

National Institute of Standards and Technology

**NSS**

National Security Systems

**OCONUS**

Outside continental United States

**ODSC, G-3/5/7**

Office of the Deputy Chief of Staff, G-3/5/7

**OMA**

Operations & Maintenance, Army

**OMB**

Office of Management and Budget

**ONS**

Operational need statement

**OSD**

Office of the Secretary of Defense

**OV**

Operational view

**Pam**

pamphlet

**PBO**

Property book office; property book officer

**PCMCIA**

Personal Computer Memory Card International Association

**PEG**

Program evaluation group

**PEO**

Program executive officer

**PM**

Program manager

**POC**

Point of contact

**POM**

Program objective memorandum

**POP**

Point of presence

**PPBE**

Planning, programming, budgeting, and execution

**PPS**

Precise positioning service

**PRB**

Project review board

**PSS**

Packet switched service

**PUA**

Proxy user agents

**QI**

Quality of information

**R&R**

Review and Revalidation

**RCIO**

Regional chief information officer

**RD**

Regional director

**RFS**

Request for service

**RNOSC**

Regional network operations and security center

**ROI**

Return on investment

**ROTC**

Reserved Officers' Training Corps

**SAC**

Service access code

**SATCOM**

Satellite communications

**SBC**

Service-based costing

**SDP**

Service delivery point

**SDS**

Switched data service

**SES**

Senior Executive Service

**SIPRNET**

Secure internet protocol router network

**SLA**

Service-level agreement

**SLM**

Service-level management

**SMTP**

Simple mail transfer protocol

**SOAP**

Simple object access protocol

**SONET**

Synchronous optical network

**SP**

Strategic plan

**SQL**

Structured query language

**SRS**

Strategic Readiness System

**SV**

Systems view

**SVS**

Switched voice service

**TAP**

Total Army Plan

**TCO**

Telephone control officer

**TDA**

Table of distribution and allowances

**TNOSC**

Theater network operations and security center

**TOE**

Table of organization and equipment

**TR**

Telecommunications request

**TRADOC**

United States Army Training and Doctrine Command

**TSACS**

Terminal Server Access Control System

**TV**

Technical view

**UDDI**

Universal description, discovery, and integration

**USAAC**

U.S. Army Accessions Command

**USAISEC**

U.S. Army Information Systems Engineering Command

**VTC**

Video teleconferencing

**VTFs**

Video teleconferencing facilities

**WAN**

Wide area network

**WebOE**

Web Order Entry

**WLAN**

Wireless LAN

**WSDL**

Web services description language

**XML**

eXtensible markup language

**XTACACS**

Extended Terminal Access Controller Authentication Control System

**Section II****Terms****Accessible**

A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or Web services that expose the business or mission process that generates data in readily consumable forms.

**Access type**

The categorization of facilities used to provide access.

**Acquisition reform**

No mandatory standards are to be requested for inclusion in a contract.

**Acquisition support**

Acquisition policies are defined in AR 70-1 and DA Pamphlet 70-3.

**Activity based costing (ABC)**

A form of cost accounting focusing on the costs of performing specific functions (processes, activities, tasks, and so on), instead of on the costs of organizational units. ABC generates more accurate cost and performance information related to specific products and services than is available to managers through traditional cost accounting approaches.

**American Standard Code for Information Interchange (ASCII)**

The standard code used for information interchange among data processing systems, data communications systems, and associated equipment in the United States. The ASCII character set contains 128 characters. This includes upper and lower case alphabetic characters, numbers, and special characters, including a space and punctuation marks.

**Analog data**

(1) Data represented by a physical quantity that is considered continuously variable and whose magnitude is made directly proportional to the data or to a suitable function of the data. (2) The representation of digital data using analog signaling media such as analog tone modulation of a radio frequency carrier. (3) Data transmitted over an analog transmission medium (for example, voice grade channel using an analog modem).

**Army enterprise architecture (AEA)**

A disciplined, structured, comprehensive, and integrated methodology and framework encompassing 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 IT 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 Operational Data Repository**

A meta-data repository used for architectures of functional Army systems.

**Army Telecommunications Directorate (ATD)**

A subordinate element of the U.S. Army Networks, Engineering, and Telecommunications Directorate under the command of the CG, NETCOM/9th ASC, that provides centralized management of the Army's worldwide commercial-leased and Government-owned telecommunications; serves as the Army interface with the Defense Information Systems Agency, Defense Information Technology Contracting Office, and General Services Administration on telecommunications certification office related matters.

**Asynchronous services**

With asynchronous services, the client invokes the service but does not—or cannot—wait for the response. Often, with these services, the client does not want to wait for the response because it may take a significant amount of time for the service to process the request.

**Audio**

Relating to recording, production, reproduction, and distribution of sound.

**Authoritative data source**

A source of data or information that is recognized by members of a COI to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference (for example, the United States Postal Service is the official source of U.S. mailing ZIP codes).

**Automated Information system (AIS)**

An acquisition program that acquires IT, excluding IT involving equipment vital to a weapon system or weapons systems or is a tactical communication system. (DODD 5000.1)

**Automation**

Conversion of a procedure, a process, or equipment to automatic operation. When allied to telecommunications facilities, automation may include the conversion to automatic operations of the message processing at an exchange or remote terminal.

**Balanced scorecard**

An aid to organizational performance management. the balanced scorecard helps to focus not only on the financial targets but also on the internal processes, customers, and learning and growth issues.

**Baseline architecture**

A description of the current set of IT resources and capabilities.

**Basic rate interface (BRI)**

An ISDN multipurpose user's interface standard that denotes the capability of simultaneous voice and data services provided over 2B+D channels, two clear 64 kb/s channels and one clear 16 kb/s channel access arrangement to each subscriber's location as defined by ITU-TSS I.412.

**Broadcast**

The transmission of radio and television signals through the airwaves. The transmission of information, through any network medium, for simultaneous reception of the information by multiple receiving stations on the network.

**Browser**

Client software which moves documents from Web sites on the Web or intranets to a computer for viewing, processing, or storage.

**Business process reengineering**

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 a part of what is necessary in the radical change of processes; it refers specifically to the design of a new process (see DODD 8000.1).

**Business rule**

A statement or fact defining the constraints governing how data are processed (for example, referential integrity constraints for add, change, and delete transactions against records in a database). For example, referential integrity constraints may be derived from relationships defined in a data model. For this type of constraint, each business rule statement should be constructed so that the parent entity name is the subject, the relationship name is the verb phrase, and the child entity name is the object (see DOD 8320.1-M).

**Busy hour**

The 60-minute period during which the traffic load of a given 24-hour period is at maximum.

**C4/IT services list**

Customer focused services that support Army business processes and are a subset of the 95 Assistant Chief of Staff for Installation Management services. The list's service groups are communications and computers, automation, visual information, information assurance, and document management.

**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.

**Call**

A unit of traffic measurement that refers to any demand to set up a connection.

**Caller, calling party, call originator**

A person, program, or equipment that originates a call.

**Call detail report**

Telephone records containing various recorded data about each call and are part of the invoice.

**Call type**

Indication of the type of call transaction as identified on the call detail report. Examples of PSS call types include: 30 bits per second (b/s) dial-up data (DU3); 1,200 b/s dial-up data (DU12); or 9,600 b/s digital data (DI96).

**Centrex**

A service offered by the base operations centers, which provides, from the telephone company central office, functions and features comparable to those provided by a PBX or a Private Automatic Branch Exchange. As used in this document may refer to comparable service offered by non-Bell Local Exchange Companies (for example, GTE).

**Circuit**

The complete transmission path between two terminals over which one-way or two-way communication may be provided. A circuit may provide one or more channels.

**Classes of telephone service**

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. 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. 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. 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.

**Command, control, communications, and intelligence (C3I)**

One of four domains used to manage architecture configurations in the ASA. C3I includes all systems involved in 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.

**Commercial communications work order (CCWO)**

DD Form 1367, used to accomplish the modification, changing, or moving of any leased telecommunications service in accordance with the limitations specified by an ML-CSA.

**Commercial satellite communications initiative (CSCI)**

A reimbursable service administered by DISA to provide commercial satellite communications services and terminals to meet special requirements of DOD users.

**Commercial Satellite Communications Terminal Program (CSTP)**

A reimbursable service administered by U.S. Army Project Manager for Military Satellite Communications (PM-MIL-SATCOM) to provide commercial satellite communications terminals to meet DOD commercial satellite communications requirements.

**Common-user information services**

Official Army information services available to all authorized customers.

**Communications management monitoring**

Monitoring DOD dedicated and common user telephone systems of the Defense Communications System to determine the operational efficiency and proper utilization of the system. Telephone systems are subject to communications management monitoring at all times (see DODD 4640.1).

**Communications systems**

A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

**Communications service authorization (CSA)**

DD Form 428 prescribed for use in procuring leased communications services under the terms of general agreements with common carriers.

**Community of interest (COI)**

A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.

**Community of practice (COP)**

A group of people who have a common interest in some subject or problem, collaborate to share ideas, find solutions, and build innovations.

**Compliance**

A system that meets, or is implementing an approved plan to meet, all applicable Technical Architecture (TA) mandates.

**Concept**

A document or theory translating vision(s) 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 (that is, expected performance) and in physical terms (that is, appearance and composition).

**Connection**

A call, session, or virtual communications link provided via switched service types or the use of the fixed transmission media of dedicated facility-based service types.

**Context**

The interrelated conditions that compose the setting in which, the architectures exist. It includes environment, doctrine, and tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

**Contracting officers technical representative (COTR)**

Contracting officers/COTRs report to the contracting officer for those actions delegated by the contracting officer as specifically addressed in the letter of appointment.

**Conference call**

Call in which more than two access lines are connected.

**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.

**Customer/user**

The requester and recipient of information services.

**Data architecture**

The framework for organizing and defining the interrelationships of data in support of an organization's missions, functions, goals, objectives, and strategies. Data architectures provide the basis for the incremental, ordered design and development of databases based on successively more detailed levels of data modeling (see DOD 8320.1-M).

**Data architecture products**

The data-specific inputs required or outputs produced through the IM/IT life cycle activities, from Architecture definition through requirements specification, design, development, production, deployment, operations, and maintenance of database applications. These products provide the basis for the incremental, ordered design and development of databases based on successively more detailed levels of data specifications to "build out" the required data architecture product set.

**Data asset**

Any entity that comprises data. For example, a database is a data asset that comprise data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (for example, www.weather.com) would be a data asset. A human, system, or application may create a data asset.

**Data circuit terminating equipment**

In a data station, the equipment that provides signal conversion, coding, and other functions at the network end of the line between the data terminal equipment and the line, and that may be a separate or an integral part of the data terminal equipment or of the intermediate equipment.

**Data interoperability**

The exchange of information that preserves the meaning and relationships of the data exchanged.

**Data management services**

Data management services provide for the independent management of data shared by multiple applications. These services include data dictionary, directory services and DBMS services. DBMS services support the definition, storage, and retrieval of data elements from monolithic and distributed DBMSs.

**Data model**

A graphical and textual version 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 terminal equipment (DTE)**

Equipment that converts user information into data signals for transmission, or reconverts the received data signals into user information.

**Dedicated access**

A type of access in which a communications channel is assigned to specific users for an extended period of time. Dedicated access service is generally billed on a monthly basis.

**Dedicated service types**

The access and transport service types generally based on the use of fixed transmission media and generally billed on a monthly recurring basis.

**Dedicated transmission service (DTS)**

The service category covering provision of private-line transmission of voice or data using end-to-end transmission media.

**Dedicated data transmission service**

Equipment and circuitry specifically designated to transmit and/or receive digital data. The transmission path for this service may be a dedicated circuit, direct distance dial, or official commercial telephone.

**Dedicated telecommunications**

Those telecommunications services or circuits used by one or more special users authorized and used for specific purposes between predetermined and fixed locations (for example, point-to-point, data, command, and control). The service may or may not be switched.

**Delay**

The interval of time between transmission and reception of a signal.

**Digital integrated services network (DISN)**

An integrated digital network in which the same digital switches and digital paths are used to establish connections for different services; for example, voice, data, or video.

**Digital switching**

A process in which connections are established by operations on digital signals without converting them to analog signals.

**Defense Information Technology Management System (DITMS)**

Manages the reporting of automation resources inventory and excess including hardware and software.

**Defense Metropolitan Area Telephone System (DMATS)**

DMATS is a consolidation of telephone services and facilities within a specified geographical area, under a single manager, providing telephone services to DOD customers for the transaction of official Government business.

**Doctrine**

Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative, but requires judgment in application. Doctrine represents consensus on how the Army conducts operations today.

**DOD IT Standards Registry (DISR)**

The DISR is an online repository for a minimal set of primarily commercial IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. These standards are used as the “building codes” for all systems being procured in the Department of Defense. Use of these building codes facilitates interoperability among systems and integration of new systems into the GIG. In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver net-centric capabilities.

**Domain**

For purposes of IT architecture, domain is a distinct functional area that can be supported by a family of systems with similar requirements and capabilities. An area of common operational and functional requirements. On the Internet, a domain consists of a set of network addresses. This domain is organized in levels. The top level identifies geographic or purpose commonality (for example, the nation that the domain covers or a category such as “commercial.” The second level identifies a unique place within the top level domain and is, in fact, equivalent to a unique address on the

Internet (or Internet protocol). Lower levels of domain may also be used. For purposes of data sharing in DOD, domains are subsets of mission areas and represent a common collection of related, or highly dependent, information capabilities and services. Managing these related information capabilities and services within domains improves coordination, collaboration, integration, and consistency of processes and interfaces for information sharing.

### **Domain name system (DNS)**

A hierarchical distributed method of organizing the names of computers on the network. The DNS groups host into a hierarchy of authority allowing addressing and other information to be widely distributed and maintained. The principal top-level domains presently authorized in the United States are COM, EDU, ORG, GOV, NET, and MIL. The US domain is also in use in the United States. DISA manages the MIL domain.

### **Domestic**

Within the United States, Puerto Rico, the U.S. Virgin Islands, Guam, the Northern Marianas, and American Samoa.

### **DSN access line**

A circuit connecting an DSN subscriber (instrument or PBX/PABX) directly to an DSN switch.

### **DSN subscriber**

An individual, station, installation, or location having direct access into an DSN switch.

### **DSN sser**

An individual, station, installation, or location having access into the DSN indirectly, that is, either by dialing a designated access code or placing a call through a local private branch exchange or through a console.

### **Dual-tone multifrequency signaling**

A telephone signaling method using standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four relatively high frequencies.

### **Dual-use access line**

A subscriber access line normally used for voice communications but with special conditioning for use as digital transmission circuit.

### **Economic analysis**

A systematic approach to identify, analyze, and compare costs or benefits of alternative courses of action that will achieve a given set of objectives. This approach is taken to determine the most efficient and effective manner to employ resources. In the broad sense, the systematic approach called EA applies to new programs as well as to the analysis of ongoing actions (see the Department of the Army Economic Analysis Manual, July 1995).

### **Electronic access**

The ability to access information online (dedicated or dial-up), e-mail, and fax.

### **Electronic commerce**

Army EC is electronic techniques for accomplishing business transactions, including electronic mail or messaging, Web technology, electronic bulletin boards, purchase cards, electronic funds transfers, and electronic data interchange.

### **Electronic data interchange (EDI)**

The exchange of routine business transactions in a computer-processable format, covering such traditional applications as inquiries, planning, purchasing, acknowledgments, pricing, order status, scheduling, test results, shipping and receiving, invoices, payments, and financial reporting. A form and format of EDI is defined by the ANSI X12 family of standards. Third parties provide EDI services that allow organizations with different equipment to interoperate.

### **Electronic mail (e-mail)**

An information dissemination and retrieval service accessed through distributed user workstations normally provided through office automation initiative.

### **End-to-end**

Telecommunications service from the originating user's terminal to the destination user's terminal. As applied in this document, this term refers to SDP to SDP service.

**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.

**Facsimile transmission (fax)**

In communications, system for the electrical transmission of printed material, photographs, or drawings. Facsimile transmission is accomplished by radio, telephone, or undersea cable. The essential parts of a fax system are a transmitting device that translates the graphic matter of the copy into electrical impulses according to a set pattern, and a synchronized receiving device that retranslates these impulses and prints a facsimile copy.

**Features**

Features are separately priced integral capabilities of, or additional enhancements to, basic services.

**Federal relay service**

A Federal Government provided service acting as an intermediary between hearing individuals and individuals who have hearing or speech disabilities.

**Federal Technology Service (FTS)**

The Government organization that plans, develops, establishes, and manages the FTS program to meet Federal requirements for common-user local and long-distance telecommunications services Government-wide (Federal Telecommunications Service prior to October 1997).

**Federal Telephone System 2001 (FTS 2001)**

A combination of Federal telephone contract options for commercial long-distance telecommunications services available to Federal agencies. FTS 2001 is managed by the GSA.

**File transfer protocol (FTP)**

A TCP/IP service that supports bidirectional transfer of binary and ASCII files without loss of data between local and remote computers on the Internet. The FTP command set allows a user to log onto a remote server over the network, list file directories and copy files.

**Foreign carrier**

Any person, partnership, association, joint-stock company, trust, Governmental body, or corporation not subject to regulation by a U.S. Governmental regulatory body and not doing business as a citizen of the United States, which provides telecommunications services outside the territorial limits of the United States.

**Foreign exchange services**

A service connecting a customer/user to a distant telephone exchange and providing the equivalent of local service from that exchange. Rates are established by local tariffs.

**FORTEZZA**

FORTEZZA describes a family of security products that were developed to create user-friendly, low-cost security devices for the Defense Message System. The Defense Department also uses FORTEZZA to encrypt voice communications over its secure telephones. FORTEZZA cards (and other devices) are general-purpose, cryptographic "co-processors" that can be used to provide authentication, data integrity, and confidentiality. Authentication (and non-repudiation) is provided via digital signature algorithm, which is part of the digital signature standard). Data integrity is provided via secure hash algorithm. Confidentiality is provided via key exchange algorithm and the SKIPJACK encryption algorithm.

**Friendly name**

An easily used and natural language name for something that may have a more technical designation. For example, a modem on a network could be called \z2x/144 or a more friendly name like Modem2.

**Full duplex**

A mode of operation in which simultaneous communication in both directions may occur between two terminals. Contrast with half duplex or simplex operation in which communications occur in only one direction at a time.

**Functional requirements**

Drive and justify IT modernization.

**General purpose (common-user)**

Official Army telecommunications services available to all authorized users on a shared basis.

**Government-wide purchase card**

Provides a means to purchase items at a lower cost and gives unit commanders organic procurement capability.

**Governmental regulatory body**

The Federal Communications Commission, and statewide regulatory body, public utility commission, or any body with less than statewide jurisdiction when operating pursuant to State authority.

**Hardware reuse**

Excess hardware must be condition-coded as serviceable or unserviceable. All serviceable hardware, regardless of condition code, must be reported to DITMS.

**Human capital**

The accumulated training, education, experience, and competencies an individual soldier or civilian possesses and applies in support of accomplishing the Army's mission.

**Hypertext markup language (HTML)**

Authoring software language used on the Internet and for creating Web pages. HTML is essentially text with embedded HTML commands identified by angle brackets and known as HTML tags.

**Hypertext transfer protocol (HTTP)**

The communications protocol used by a Web browser to connect to Web servers on the Internet.

**Hypertext transfer protocol secure (HTTPS)**

The protocol for accessing a secure Web server. The use of HTTPS in the URL directs the message to a secure port address instead of the default Web port address of 80.

**Inbound**

A switched connection made from a non-domestic location to a domestic location.

**Information assurance (IA)**

IA ensures the availability, integrity, identification, authentication, confidentiality, and non-repudiation of friendly information and systems and forbids the access to the information and systems by hostile forces. As a subset of defensive information operations, IA includes provisions for protection, detection, and response capabilities. The protection capability is composed of devices that ensure emission security, communications security, computer security, and information security. Detection is the capability to determine abnormalities such as attacks, damages, and unauthorized modifications in the network via mechanisms such as intrusion detection systems. The response capability refers to the ability to restore normal operations as well as the ability to respond to a detected entity.

**Information capability**

The ability to consume and generate information in the form of data assets by performing a specific task using IT and/or NSS.

**Information consumers**

A person, group, organization, system, or process that accesses and receives information enabling the execution of authorized missions and functions.

**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 management officer (IMO)**

The information manager in an organization whose primary functions are to develop, manage, and maintain the organization's information resources.

**Information producers**

A person, group, organization, system, or process that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions.

**Information management support council (IMSC)**

An installation implementation work group organized under the direction of the DOIM. The group is comprised of host installation and tenant representatives used to plan and execute the management of the installation information resources.

**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 record-keeping systems, whether manual or automated.

**Information system**

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

**Information technology (IT)**

Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Army or DOD. This includes equipment that is used directly or is used by a contractor under a contract with the Army or DOD which requires either the use of such equipment or the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term 'information technology' also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. 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 (40 USC 11101).

**Information Technology Infrastructure Library**

A set of internationally recognized best business practices on the management and provision of operational IT Services.

**Infrastructure**

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 information infrastructure architecture (I3A)**

The I3A is a standard communications infrastructure architecture for the U.S. Army installations embracing the DISR for all technology implementations. The installation infrastructure objective architecture designs are "roadmaps" for installation managers to plan, manage, budget and migrate towards.

**Integrated communications data base (ICDB)**

A database, administered by DISA for the Joint Staff, containing all CJCS approved and authorized requirements for users within DOD to communicate in networks via satellite communications accesses. Operation of any military satellite communications terminals requires valid ICDB authorizations.

**Integrated data management**

Integrated data management ensures the provision of correct information to the right person(s) at the necessary time. As a subset of information management, it addresses awareness, access, and delivery of information. This management area includes the safeguarding, compilation, cataloguing, storage, distribution, and retrieval of data. The area deals with the management of information flow to users in accordance with the commander's information policy. Integrated data management separates information into two types: planning and survival. Planners and decision-makers use information taken from databases, Web pages, and files to determine future action. Survival information is more time sensitive and pushed over tactical networks and data links to warfighters and weapon systems.

**Integrated services digital network (ISDN)**

An integrated digital network in which the same digital switches and digital paths are used to establish connections for different services; for example, voice, data, or video.

**Interexchange carrier (IEC)**

A communications common carrier that provides telecommunications services between LATA or between exchanges within the same LATA.

**Internet**

A global interconnection of individual networks operated by Government, industry, academia, and private parties. The Internet originally served to connect laboratories engaged in Government research, and has been expanded to serve millions of users and a multitude of purposes.

**Internet protocol**

A DOD standard protocol designed for use in interconnected systems of packet-switched computer communication networks. Note: The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small packet networks.

**Internetworking**

The process of interconnecting a number of individual networks to provide a path from a terminal or a host on one network to a terminal or a host on another network. The networks involved may be of the same type, or they may be of different types. However, each network is distinct, with its own addresses, internal protocols, access methods, and administration.

**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 equipment used for DOD component cryptologic applications**

Equipment acquired that becomes excess shall be reported to the National Security Agency in accordance with its implementing circulars.

**IT requirements**

Clear definitions of the functional requirements, not just the technical or system requirements.

**Knowledge management**

The systematic process of finding, selecting, organizing, improving, sharing and benchmarking explicit and tacit information for mission results. It involves sharing all of an enterprise's information assets, including databases, documents, policies and procedures, as well as the previously unarticulated expertise and experience resident in individual workers.

**Lease**

Information systems or equipment is acquired under a periodic charge agreement.

**Lease with option to purchase**

Leasing of items for specified periods with an option to purchase at a later date.

**Lease to ownership plan**

A program under which items are leased for a specific period after which the lease ends and title is transferred to the Government.

**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.

**Local access and transport area**

Under the terms of the Modification of Final Judgment, the geographical area within which a divested base operation center is permitted to offer exchange telecommunications and exchange access services.

**Local area network (LAN)**

A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. Note 1: LANs are usually restricted to relatively small areas, such as rooms, building, ships, and aircraft. Note 2: An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network. An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network. Note 3: LANs are not subject to public telecommunications regulations.

**Local exchange carrier (LEC)**

A telecommunications service corporation authorized to provide local exchange telecommunications service within a defined service area by appropriate State and, as applicable, local Government authority - also known as the "local telephone company." The infusion of competition into the local exchange market has engendered the acronyms, Incumbent Local Exchange Carrier (ILEC) to represent the former monopoly-situated carrier, and Competitive or Certified Local Exchange Carrier to represent the newer carrier(s) authorized to compete for business with the ILEC in the ILEC's defined service area.

**Location**

A physical space, such as a building or a room. A physical point where the FTS2001 contractor delivers service to a user.

**Loop start**

A supervisory signal given by a telephone or other telecommunications device after the loop path to the central office or other switching system is completed.

**Mandatory**

Those services, features, or equipment which the offeror must propose. Any service, feature or equipment proposed must be priced.

**Mandatory feature**

A feature to be provided by the contractor at least in limited areas and extended to other geographic areas at the same time that the contractor makes them commercially available in those areas.

**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 roles for executing the specified actions; establishes priorities among actions and relevant supporting programs; and establishes performance measures and functions for measuring performance.

**Maximum calling area**

Geographical calling limits assigned to a particular DSN access line.

**Measure**

One of several measurable values that contribute to the understanding and quantification of a key performance indicator.

**Message (telecommunications)**

Record information expressed in plain or encrypted language and prepared in a format specified for intended transmission by a telecommunications system.

**Metadata catalog**

A system that contains the instances of metadata associated with individual data assets. Typically, a metadata catalog is a software application that uses a database to store and search records that describe such items as documents, images, and videos. Search portals and applications can use metadata catalogs to locate the data assets that are relevant to their queries.

**Metadata registry**

Repository of all metadata related to data structures, models, dictionaries, taxonomies, schema, and other engineering artifacts that are used to support interoperability and understanding through semantic and structural information about the data. A federated metadata registry is one in which multiple registries are joined electronically through a common interface and exchange structure, thereby effecting a common registry.

**Mission**

A group of tasks with their purpose assigned to military organizations, units, or individuals for execution.

**Mission area**

A defined area of obligation with functions and processes that contribute to mission accomplishment.

**Mission related**

Processes and functions that are closely related to the mission (for example, the mission of Direct and Resource the Force has the mission-related functions of planning, programming, policy development, and allocating of resources.

**Mobile Satellite Service (MSS)**

A unique mobile communications service based on commercial satellites administered by DISA for DOD users. Users access the cellular telephone like service using small portable handsets.

**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.

**Multimedia**

Pertaining to the processing and integrated presentation of information in more than one form, for example, video, voice, music, or data.

**Multiplexing**

The combining of two or more information channels onto a common transmission medium. Note: In electrical communication, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM). In optical communications, the analog of FDM is referred to as wavelength-division multiplexing (WDM).

**National Security System**

As defined in Section 5142 of the CCA (40 USC 11103), the term NSS means “any telecommunications or information system operated by the United States Government, the function, operation, or use of which—involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions. NSS ”does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).”

**Net-centric**

Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and Network-Centric Warfare (NCW).

**Network**

An interconnection of three or more communicating entities and (usually) one or more nodes. A combination of passive or active electronic components that serves a given purpose.

**Network programming**

Programming supplied by a national or regional television or radio network, either commercial or noncommercial.

**Off-hook service**

Automatic establishment of a connection between subscribers as a result of lifting a handset.

**Off-net calling**

Official long-distance telephone voice calls placed through DSN via local DOD PBXs/PABXs originating from, or extending to, local commercial numbers.

**Off-premise extension (OPX)**

An extension telephone (or PBX station) located outside the boundaries of an installation or property, which is not contiguous with the location where the main station or PBX is located.

**Office telephone monitoring**

Listening to or recording office telephone conversations by use of mechanical, acoustical, or electronic devices or recording by written means, for the purpose of obtaining an exact reproduction or a summary of the substance of the telephone conversation.

**Official telecommunications service**

All telecommunications services used for the conduct of official Government business.

**Official telephone calls**

Calls made for the transaction of official Government business.

**OMA funding**

Funds providing installation level DOIM services and authorized on installation or equivalent TAADS documents. Used for follow-on maintenance, even for systems or items acquired with OPA funding.

**Ontology**

The hierarchical structuring of knowledge about things by subcategorizing them according to their essential (or at least relevant and/or cognitive) qualities.

**Operational element**

The forces, organizations, or administrative structure that participate in accomplishing tasks and missions.

**Operational level agreement (OLA)**

An internal document, owned by the service management team, that defines the working relationship between different functional areas within an IT organization. The OLA sets out the functions for the support and delivery of C4/IT services to customers.

**Optional**

Those service, features, or equipment which offerers may propose but are not required to propose. Any service feature or equipment proposed must be priced.

**Optional feature**

A feature that is not mandatory but may be offered at the option of the offerer.

**Outbound**

A switched connection made from a domestic location to a nondomestic location.

**Outsourcing**

Purchasing (goods) or subcontracting (services) from an external source (for example, other Government activity or private sector company).

**Packet switched network**

A network designed to carry data in the form of packets. The packet format, internal to the network, may require conversion at a gateway.

**Performance measure**

A quantitative or qualitative characterization of performance.

**P-forms**

Procurement forms

**Planning, programming, budgeting, and execution**

The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

**Primary rate interface (PRI)**

An ISDN interface standard (a) that is designated in North America as having a 23B+D channels, (b) in which all circuit-switched B channels operate at 64 kb/s, and (c) in which the D channel also operates at 64 kb/s. Note: The PRI combination of channels results in a digital signal 1 (T1) interface at the network boundary.

**Private branch exchange (PBX)**

Telephone switching equipment conforming to the FCC registration requirements for interconnection to the public switched network.

**Point of presence (POP)**

The physical location defined by a provider of FTS2001 transport services where transport services and access services are interconnected and where such interconnections are identified and managed for operational and billing purposes in the provision of FTS2001 service. A POP is the demarcation point between access services and transport services.

**Process owners**

HQDA functional proponents, MACOMs, and others who have roles in any mission-related or administrative work process.

**Procurement strategy**

Customers and providers of information systems should be aware of the various procurement approaches available for acquiring information systems and services.

**Program objective memorandum (POM)**

A memorandum in prescribed format submitted to the Secretary of Defense by the secretary of a military department or the director of a defense agency, which recommends the total resource requirements within the parameters of the published Secretary of Defense Fiscal Guidance. The POM is the principal programming document which details how a component proposes to respond to assignments in the Defense Planning Guidance.

**Public switched network (PSN)**

Any common carrier network that provides circuit switching among public users, including foreign postal telephone and telegraphs. Note: The term is usually applied to the public switched telephone network, but it could be applied more generally to other switched networks that are available to the public, for example, packet-switched public data networks.

**Purchase**

The Army gains title at the time of successful final test and acceptance.

**Reimbursable basis**

When installations have no organic DOIM assets they must contract for the services or establish ISA's with Army or other services for DOIM support.

**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.

**Requirements priority**

Based on the degree of impact they will have on the ability to carry out the proponents mission.

**Request for service (RFS)**

A request for leased long-haul telecommunications services.

**Research, development, and acquisition (RDA)**

A term that includes OPA and Research, Development, Test and Evaluation (RDT&E) Appropriations

**Satellite communications (SATCOM)**

Communications via satellite, including DOD use of military-owned and -operated satellite communication systems

that use Government radio frequency bands, as well as commercial satellite communications systems that use commercial radio frequency bands (see CJCSI 6250.01B).

### **School transfer**

Excess automation resources for which the DITMS focal point cannot identify a DOD recipient may be made available to the nations schools through the Educational Institution Partnership Program.

### **Screening cycle**

The 30-day DOD screening period begins when the report of excess is electronically released by the Agency focal point or entered by the DRMO into the processing cycle.

### **Service analysis team (SAT)**

An Installation Management Agency sponsored group, comprised of MACOM representatives, functional and installation stakeholders, DOIMs, ASBs, and garrison commanders. The SAT is designed to help the Army community define the baseline C4/IT service support it requires, prioritize the requirements, and recommend performance measures for services provided by DOIMs and ASBs.

### **Service delivery point (SDP)**

The interface point at which a service is delivered by the contractor to the user. It is defined in terms of location, contractor facilities, interface, and user facilities. The SDP is the interface point for the physical or logical delivery of a service, one of the points at which performance parameters are measured to determine compliance with the contract, and the point used by the contractor to identify the charges for services rendered. Each SDP is defined as the combined physical, electrical, and service interface between the contractor's network on one hand and on the other hand Government on premises equipment, off-premises switching and transmission equipment, and other facilities (such as those provided by Centrex and telephone central offices). The POP of the contractor may be an SDP if the Government acquires access separately.

### **Service due date**

The date when the Government expects the service order to be completed and charges to billing become effective.

### **Service improvement plan (SIP)**

A coordinated set of tactical, joint, and strategic initiatives to improve the five C4/IT services as a single C4/IT Capability program, with coordinated doctrine, training, organization, and material developments.

### **Service level agreement (SLA)**

A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer. SLAs are central to managing the quality of service delivered by an IT organization to a customer.

### **Service level indicators (SLI)**

SLIs are the performance metrics to be used to measure the agreed-upon levels of service as documented in Service Level Agreements for reimbursable services or service declarations for non-reimbursable services.

### **Service level management (SL&M)**

The disciplined, proactive process of envisioning, planning, developing, and deploying appropriate C4/IT levels of service to all customers at an affordable cost. SL&M is the coordinating process for all SM service delivery and service support processes.

### **Service management**

The practice of overall management of Command, Control, Communications, Computers, Information Management (C4/IT) services and their associated infostructure to meet customer requirements. SM processes are categorized into the service delivery and service support processes of an Enterprise. The Army Service Management Program is being developed after the Information Technology Infrastructure Library (ITIL) Service Management concept model.

### **Service and network management (SNM)**

S&NM is managing the network and the devices connected to it. S&NM includes three management areas: Network Management (including network devices, servers, storage devices, and end-user devices like printers, workstations, laptops, and hand-held computers), Satellite Communications (SATCOM) Management, and Frequency Spectrum Management. Network Management includes Systems and Applications Management and covers measures needed to ensure the effective and efficient operations of networked systems. Network Management is composed of fault,

configuration, accounting, performance, and security management. SATCOM Management includes day-to-day management of apportioned and non-apportioned SATCOM resources. Frequency Spectrum Management ensures Combatant Commanders and subordination commanders are aware of spectrum management decisions impacting the area of operations. Frequency Spectrum Management is composed of the efficient management of the electromagnetic spectrum including the acquisition, allocation, protection, and utilization of radio frequency and call-sign resources.

#### **Standard data element**

A data element that has been coordinated through the standardization process and approved for use in DOD information systems (see DOD 8320.1-M-1).

#### **Shared database segment (SDS)**

An SDS is a database used by several applications. The applications access shared data through shared database segments. This approach is appropriate for related applications that use a compatible DBMS and share a single data schema either directly or through the use of middleware (see DOD DII Shared Data Engineering (SHADE) Capstone Document, V 1.0).

#### **Shared space**

Storage on a file server or in electronic media that is addressable by multiple users or COIs. Also, Web services that are made available to the enterprise that expose the business or mission processes that generate data in readily consumable forms.

#### **Signaling**

The information exchange concerning establishment and control of a connection and management of the network, in contrast to user information transfer.

#### **Simplex operation**

That mode of operation in which communication between two points occurs in only one direction at a time. Contrast with half duplex or duplex operation.

#### **Special purpose (dedicated) telecommunications**

Telecommunications services or circuits used by one or more special users and authorized and used for specific purposes between predetermined and fixed locations (for example, point-to-point, data, command and control) and may or may not be switched.

#### **Software**

A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compiler, library routines, manuals, circuit diagrams); usually contrasted with hardware.

#### **Software reuse**

Licensed COTS software no longer needed for the originally acquired purpose must be reported for internal DOD redistribution screening unless redistribution is an infringement of the licensing agreement.

#### **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.

#### **Strategic goal**

Long-range changes target that guides 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.

#### **Statistical sampling**

An administrative certification that long distance phone calls are necessary in the interest of the Government, determined by estimates of the percentages of similar toll calls in the past that were official calls. The process provides reasonable assurance of accuracy and freedom from abuse.

**Straight lease**

Lease resources for a specific base period and usually has an option for additional periods.

**Structured professional forums**

Groups of people who share a concern, a set of problems, or a passion about a topic, and who generate understanding, solutions, and capabilities (knowledge, skills, and attributes) in this area by interacting on an ongoing basis.

**Supported activity**

An organization, activity, or unit located on or off an installation or supplantation belonging to another command, and from which it is receiving specified types of supply or other services.

**Supporting DOIM**

The DOIM is the installation information manager. As the installation DOIM, assigns the functions of the installation staff officer who monitors information management.

**Switched access**

A type of access in which a communications channel is provided to users on a demand basis, via circuit switching and is generally billed on a per call, or per session basis.

**Switched service types**

The access and transport service types generally based on the use of switched transmission media and generally billed on a unit of time or unit of data basis, per call, session, or virtual communications link. Some Switched Data Service switched service types will use dedicated service-like billing structures for certain virtual circuit arrangements.

**Synchronous services**

Synchronous services are characterized by the client invoking a service and then waiting for a response to the request. Because the client suspends its own processing after making its service request

**Synchronous transmission**

Digital transmission of a continuous stream of information bits in which the time interval between any two similar significant instants in the overall bit stream is always an integral number of unit intervals. Note: "Isochronous" and "anisochronous" are characteristics, while "synchronous" and "asynchronous" are relationships.

**System**

An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JCS Pub 1).

**Systems architect**

Has the functions for integration and oversight of all Army information systems. The ASA (ALT) is the Army systems architect

**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.

**Taxonomy**

A taxonomy is how a Web site organizes its data into categories and subcategories, sometimes displayed in a site map.

**Technical architecture profile**

In addition to the parts of the DISR that are relevant to a specific operational architecture view and a specific systems architecture view a technical profile contains data on those systems that do not comply with the DISR but are used in the architecture. These data are needed to determine interoperability.

**Technical report**

An assemblage of technical documentation to report on a single mission or project-related event.

**Telecommunications coordinator**

An individual in the supporting DOIM who has been appointed, in writing, by the 7th Signal Command Office of Acquisition, for the purpose of issuing commercial communications work orders, DD Form 1367, against an ML-CS.

**Telecommunications device for the deaf/teletypewriter (TDD/TTY)**

A device that permits individuals with speech and/or hearing impairments to make and receive telephone calls without assistance from others. A TDD or TDD-compatible device will be used by the speech/hearing-impaired user community to access the Federal Relay Service. A TDD generally consists of a keyboard, display screen, and a means (via modem or direct connection) to access a telecommunications network. It is recognized that this function can be performed by a computer with software enhancements. The term TTY may also be used in referring to this type of device.

**Telecommunications service request (TSR)**

A valid, approved, and funded telecommunications requirement submitted to DISA or DISA activities. TSRs may not be issued except by specifically authorized TCOs.

**Teleconferencing**

A conference between persons remote from one another but linked by a telecommunications system. Note: The conference is supported by audio and/or video communication equipment that enables the live exchange of information among remotely located persons and devices

**Telephone communications security monitoring**

Listening to or recording the transmission of official defense information over DA-or DOD-owned or-leased telephone communications, by any means, for the purpose of determining whether such information is being properly protected in the interest of national security (AR 380-53).

**Telephone control officer (TCO)**

An individual appointed by the installation commander supervising management and implementation of the installation telephone system usage control program.

**Threaded discussion**

A series of messages and replies relating to a topic or theme in an email exchange or Internet newsgroup. .In programming, a thread is one part of a larger program that can be executed independent of the whole.

**Toll calls**

Army long distance calls where the Government is charged cost and is billed by a commercial carrier or exchange company based on call characteristics; that is, time and distance.

**Transfer circuit**

A circuit provided for the transfer of message traffic from a system operated by one nation or international alliance into a system operated by another nation or international alliance.

**Transport**

The facility-based service arrangements that provide service specific connections between the contractor's POPs.

**Trunk**

A communications path connecting two switching systems (for example, private branch exchange, tandem switch) used for establishing an end-to-end connection.

**Trunk group**

A set of trunks, traffic engineered as a unit, for establishing connections within or between switching systems in which all of the paths are interchangeable except where subgrouping is utilized.

**Undue burden**

A significant difficulty or expense

**Underpinning contracts (UC)**

A contract with an external provider covering the delivery of goods and/or services that contribute to the delivery of C4/IT services to customers. The terms and conditions of underpinning contracts should reflect and be reflected in the appropriate service-level agreement of service declaration.

**Understandable**

Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors.

**Uniform resource locator (URL)**

The Internet addressing scheme that defines the route to a document, file, or program.

**Unfinanced requirements**

Requirements that cannot be financed within the resources available.

**User**

Any person, organization, or unit that uses the services of an information processing system. Specifically, it is any TOE/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.

**Unofficial telephone calls**

Unauthorized calls for other than official Government business in support of an Army installation.

**Validation of telecommunication requirements**

Actions involving evaluation and acceptance of the operational necessity of a requirement at the various command levels. Validation does not constitute approval of the requirements but will be used as a basis for commitment of resources.

**Video**

Pertaining to bandwidth and spectrum position of the signal that results from television scanning and is used to produce an electronic image.

**Video teleconferencing (VTC)**

Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video; includes full-motion video, compressed video and sometimes freeze (still) frame video.

**Video teleconferencing service (VTS)**

The transmission of compressed or wideband video signals in support of teleconferencing.

**Visible**

Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes.

**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**

Use of one or more of the various visual media with or without sound. Generally speaking, it includes still photography, motion picture photography, video or audio recording, graphics arts, visual aids, models, displays, visual presentation services, and the processes that support them.

**Warfighter**

A 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.

**Web browser**

Client software for connecting to and viewing documents on the Web. A browser interprets HTML documents and displays them.

**Web browser/server (WBS)**

A Web browser, a Web server and their intended interaction. Web browsers and servers may communicate over the Internet and/or intranets.

**Web server**

A Web site including hardware and software that includes the operating system, Web software, other software and data, or the software that manages Web functions at a Web site.

**Web services**

A standardized way of integrating Web-based applications using open standards over an Internet protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.

**Web site**

A computer on the Internet or an intranet running a Web server that responds to HTTP and HTTPS request from Web browsers.

**World Wide Web**

An Internet function for sharing of documents with text and graphic content that links documents locally and remotely.

**Wire center**

The location of one or more local switching systems; a point at which customer loops converge.

**Wireless**

A categorization of switched and non-switched service types that generally use radio (for example, mobile, cellular, packet, or satellite) as their principal transmission medium.

**Wireline**

A categorization of switched and non-switched service types that generally use metallic cable, optical fiber cable, and point-to-point terrestrial microwave radio as their primary transmission media.

**Section III****Special Abbreviations and Terms**

This section contains no entries.

**UNCLASSIFIED**

**PIN 068572-000**