**Department of the Army
Pamphlet 25–1–1**

Information Management: Management of Subdisciplines

Army Information Technology Implementation Instructions

**Headquarters
Department of the Army
Washington, DC
26 September 2014**

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25–1–1
Army Information Technology Implementation Instructions

This rapid action revision, dated 26 September 2014--

o Incorporates information about the development and use of the Army Enterprise Architecture, the Army Information Enterprise Architecture, and the latter's three primary architecture types (paras 5-1 through 5-4).

o Adds guidance for architecture development, using the Army Capability-based Architecture Development and Integration Environment (app E).

o Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
26 September 2014

***Department of the Army**
Pamphlet 25–1–1

Information Management: Management of Subdisciplines

Army Information Technology Implementation Instructions

By Order of the Secretary of the Army:

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

Official:

Gerald B O'Keefe

GERALD B. O'KEEFE
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 Army Regulation (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, Section 2223. Chief information officer functions and those of corresponding information management and/or 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.

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, unless otherwise stated. It also applies to the information technology at all Army installations, activities, and communities. During mobilization, procedures in this publication can be modified to support policy changes as necessary.

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

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (cio-g6.policy.inbox@mail.mil).

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

Contents (Listed by paragraph and page number)

*This pamphlet supersedes DA Pam 25–1–1, dated 25 June 2013.

Contents—Continued

Contents—Continued

Appendixes

Table List

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose
This pamphlet provides operational procedures and practical guidance to Army organizations furnishing and receiving LandWarNet information technology (IT) services, products, and support. This document implements policies mandated by Army Regulation (AR) 25–1. Its emphasis identifies and describes procedures, explicit and implied, stemming from Defense policies and Federal authorities, to include the Title 40, United States Code (USC), Subtitle III (Clinger-Cohen Act); 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 regulation 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 Instruction (DODI) 4640.07, 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. The pamphlet does not address procedural or practical guidance for information assurance, see AR 25–2. The pamphlet does not apply to embedded, real-time or safety-critical vetronics and avionics systems, see AR 70–1.

1–5. Overview
a. LandWarNet—the Army's enterprise-level network for delivering information to leaders and commanders conducting unified land operations—provides timely, accurate and detailed information that allows decision-makers to employ the appropriate response to the full range of global events, from humanitarian crisis to combat. Further, information and the corresponding communications architecture provide formations the most relevant and up-to-date operational picture—regardless of location or position in the deployment cycle—and accelerate response time. This operational agility is an imperative for the Army of today and the future.

b. LandWarNet consolidates smaller, fragmented networks into a single, standards-based network. LandWarNet improves the Army's ability to procure IT while eliminating duplication, isolation and compatibility issues across the Army. The Army's strategy for end-to-end network modernization has five high-level objectives:

(1) Operationalize LandWarNet. The Army is operationalizing LandWarNet by building a single, secure, standards-based environment. By focusing on standards and not hardware, the Army does not expend resources developing and maintaining proprietary standards that differ from system to system. The Army is developing the means to let units use their mission command systems on home-station networks and connect to formerly separate tactical networks in combat theaters. A single end-to-end network enables a train-as-you-fight strategy. This standards-based environment reaches the tactical edge of the end-to-end network. LandWarNet will link with the Warfighter Information Network-Tactical (WIN–T) to provide battalions and above on-the-move network access to voice, video and data services; and with the Joint Tactical Radio System program to provide network access to companies and below.

(2) Dramatically improve cybersecurity posture. Improving cybersecurity is an imperative for the Army. A robust, fully integrated network is essential to security and efficiency and the ability to empower a smaller, yet more capable, expeditionary Army. Introducing thin clients—a computing architecture where processing and data storage occurs in the data center rather than on the end user device (thick client)—will allow the Army to transition to cloud and centralized services that reduce the risk of compromise associated with a lost user-device. Enterprise directory and email services establish a single network identity for a user. In addition to increasing security, enterprise services improve access, add sharing opportunities and save resources through infrastructure consolidation.

(3) Improve operational effectiveness while realizing efficiencies. The Army is changing its business and acquisition processes to better harness the maturation of IT. By reforming processes in governance, acquisition and architecture, the Army is improving the way it manages IT, ensuring visibility and accountability of purchases, procedures and policies.

(4) Enable Joint interoperability and collaboration with mission partners. LandWarNet is being designed to be interoperable and adaptable through the use of a common operating environment (COE) and everything over Internet protocol (IP) standards. The COE, the set of standards to which all network systems must adhere, is based on open architecture that promotes commercial-off-the-shelf technologies wherever possible. Everything over IP describes a single method for transporting voice, video and data via nonproprietary IP. Having the standards in advance will

simplify the development and integration of systems and applications for joint partners and industry. Additionally, the Army will be better able to integrate commercially mature technologies and shorten development timelines for new capabilities.

(5) Recruit and retain an agile workforce to support an expeditionary Army. The Army is working to rebalance its IT and cyber workforce to better meet the needs of an expeditionary force with sophisticated cybersecurity requirements.

1–6. Pamphlet structure

a. Scope. The scope of this pamphlet includes all organizational levels. This pamphlet is structured according to five disciplines aligned in AR 25–1, Army Information Technology. The Telecommunications and Unified Capabilities chapter (chapter 7) is a stand-alone chapter since it is governed by a separate regulation (see AR 25–13, Telecommunications and Unified Capabilities).

b. Summary.

(1) Army IT Management, Chapter 2. The Army IT Management chapter outlines the procedural information for IT investments. This chapter addresses Army IT governance and the requirements for reporting, accountability, and compliance throughout the lifecycle.

(2) Web Site Management, Chapter 3. The Web Site Management chapter provides guidance for the appropriate and authorized use of Army Web sites. This chapter is comprised of two sections: Section I, Army Enterprise Portal Overview and Section II, Army Public Web Site Management.

(3) Information and Security Management, Chapter 4. This chapter is comprised of two sections. Section I, Data Management provides information on Army information and data management policies and procedures. Section II, Information and Data Security provides procedural information for conducting a privacy impact assessment (PIA) and for ensuring the quality of disseminated information.

(4) Information Enterprise Architecture Standards and Certifications, Chapter 5. This chapter is comprised of two sections. Section I, Information Enterprise Architecture provides guidance governing the composition and use of IT architecture documentation in the Army. Section II provides procedures on obtaining Army interoperability certification (AIC) and certifying information support plans.

(5) Installation Information Technology Services and Support, Chapter 6. This chapter covers services and support on Army installations. It is comprised of three sections: Section I, Managing IT at the Installation; Section II, IT User Support Principles; and Section III, IT Systems and Services.

(6) Telecommunications and Unified Capabilities, Chapter 7. This chapter covers procedural information for the management of unified capabilities (UC) and telecommunications, which include networks, base communications (BASECOM), long-haul, and deployable communications. It applies to IT contained in command and control systems, intelligence systems (except as noted), and Department of Army (DA) purchased or developed business systems.

Chapter 2
Army Information Technology Resource Management

2–1. General

a. The efficient and effective use of IT resources has a direct affect on the Army's ability to perform its missions. AR 25–1 identifies and describes roles, responsibilities, missions and functions associated with managing the Army's IT resources.

b. Army information resources management provides an integrated view for managing the entire IT lifecycle. Information resource management uses a set of procedural processes for planning, selecting, controlling, and evaluating IT investments in order to provide the Army with the right IT capabilities at the right costs. In conjunction with IT governance and other related IT processes (such as information enterprise architecture, system engineering, information assurance and IT acquisition), information resource management guides IT policy and resource investment decisions to align with the Army's network priorities. This approach ensures visibility and accountability of IT expenditures throughout the Army.

c. Command, control, communications, and computers (C4)/IT planning is an integral part of the Army's strategic plan, The 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 information resource management process.

(1) The Army Chief Information Office (CIO)/G–6 is the principal focal point for Army Information Management (IM); providing strategic direction, IT strategic planning perspective to Army's strategic planning process, and functional policy and guidance on Army IT systems and networks.

(2) The Army CIO/G–6 oversees the Army information resource management processes (including, but not limited

to, the integration of the budget, program management, and acquisition decisions affecting IT across the Army) and manages resources supporting a specific set of C4/IT Management Decision Packages (MDEPs).

(3) Senior IM/IT officials at Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), and installations must be engaged in the development of a similar process that supports both the TAP and Army information resource management for IT investment planning at their respective levels.

d. To improve and maximize the usefulness and value of IT investments, the Army is revising and streamlining the processes for information resource management, acquisition, contracting and information assurance certification. The intent is to better plan, select, acquire (reduce the time required to test and certify new devices to keep pace with rapid technological advances within the IT industry), control and evaluate Army IT investments. The processes and procedures described in this chapter are continuously assessed to determine how well they support the Army's emerging needs and, when warranted, revised to better meet those needs. For more information, contact Army CIO/G–6, SAIS–PRR.

2–2. Information Technology Planning

a. The IT planning strategy advances compliance with 40 USC (Clinger-Cohen Act) and other statutes and regulations governing IT; IT planning uses IT resource analysis, including IT-related MDEP and portfolio-based reviews, program evaluation group (PEG) assessments, IT systems assessments (as Technology Enterprise Steering Group), cost-benefit analysis and business case analyses to identify capability gaps and recommend investment prioritization, elimination of unnecessary redundancies and/or investment tradeoffs that meet Army requirements and ensure balance across the IT investment portfolio. IT planning informs decisions by the PEG, Planning Program Budget Committee, the LandWarNet/Mission Command (LWN/MC) General Officer Steering Committee (GOSC), the Army Business Counsel, the CIO/G–6 governance boards and the office of the CIO/G–6.

b. The goals of the IT planning process include:

(1) Providing for the selection management, control, and evaluation of IT investments.

(2) Integrating planning, programming and budgeting decision processes. This includes minimum criteria to be applied to undertake a particular investment in information systems/IT, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternate 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 to obtain timely information regarding the progress of an investment or information system.

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

c. The IT portfolio is the central component of the information resource management process and provides the structure for managing all IT-related investments across the Army.

(1) The portfolio structure is aligned by portfolio to three mission areas (segments): the business mission area (generating force enterprise activities), enterprise information environment mission area (network), and warfighting mission area (mission command). The business mission area encompasses the following domains (sub-segments): acquisition, financial management, human capital management, installation and environment, and logistics. The enterprise information environment mission area encompasses the following domains: communications, computing infrastructure, core enterprise services, and information assurance. Finally, the domains encompassing the warfighting mission area are: battlespace awareness, command and control, force application, force protection, net-centric, force management, and training.

(2) Structuring and aligning the portfolio to the three mission area enables like-type analysis and review of funding requirements and recognition of interdependencies and fielding timelines within these portfolios. From there, an analysis of the entire portfolio can be accomplished with a recommended funding prioritization list.

(3) The Army is transforming processes to deliver relevant, affordable, and interoperable LWN/MC infrastructure capability sets to the generating and operational forces within the Army Force Generation (ARFORGEN) process – modernizing net-enabled capabilities over time. The LWN/MC Capability Sets Development Strategy establishes deliberately planned capability increments or sets, transforming LandWarNet into an enterprise managed activity that effectively and efficiently delivers trained and ready expeditionary forces in a deliberate, synchronized method within the ARFORGEN process. LWN/MC capability sets are designated in two year increments and will be the basis for fielding capabilities to the Army within the ARFORGEN. A LWN/MC capability set portfolio comprises the new and existing doctrine, organization, training, materiel, leadership, personnel and facilities solutions inclusive of all LWN/MC mission areas. This portfolio approach is built on the development of capability sets for modular formations to synchronize and integrate all generating force processes and to deliver improved capabilities over time.

d. The Army IT planning process is a tool for making prudent information resource and capital planning investment decisions.

(1) The Army CIO/G–6 reviews and approves the IT prioritization results and recommendations which are the foundation of the C4/IT investment strategy. As the functional proponent for the Army's C4/IT investment strategy, the CIO/G–6 develops the necessary relationships with and reassures decision-makers in the budget process that the final

prioritization recommendations are intended to make the best use of scarce IT resources and are in line with supporting enterprise initiatives for the Army.

(2) The results and recommendations ensure integration between the three mission areas.

(3) The IT planning process incorporates analyzing, tracking, and evaluating the risks and results of investments made for information systems and IT. The process covers the lifecycle of each system and includes specific criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments.

e. The CIO/G–6 investment strategy is developed through the collaborative efforts of the Army's multifunctional community of C4/IT stakeholders 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 three mission areas. To accomplish this task, the CIO/G–6 depends heavily upon the subject matter experts within each mission area for the critical analysis and review of proposed IT-related investments.

(2) Subject matter experts 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 mission area capabilities and services.

(c) Reviewing existing programs and systems within the mission area, assessing the ability to contribute to future force and enterprise requirements, and recommending which programs and systems should be accelerated, sustained, transformed, and eliminated.

(d) Coordinating with appropriate PEG representatives and program managers (PMs) who have a vested interest within their mission area.

(e) Rationalizing all existing and new capabilities and services within their mission area, ensuring they adhere to an integrated architecture.

(f) Reviewing budget submission for programs and/or systems within a mission area to ensure they support all transition and/or transformation plans and enterprise priorities.

(3) To ensure the completeness and accuracy of all information presented, it is critical that mission 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) MDEP and PEG managers, PEG-integration team leads, and CIO/G–6 representatives to each PEG.

(b) PMs and subject matter experts (as appropriate).

(c) Battlefield operating system and functional representatives.

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

(e) Each ACOM, Army Cyber Command, Army Reserve Command, and Army National Guard (ARNG).

(f) Joint and Department of Defense (DOD) counterparts.

(4) The IT planning process links to the planning, programming, budgeting, and execution (PPBE) process and ensures that the prioritization results are available during the funding deliberations. This is a continuous process throughout the year to 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 planning and matching of capabilities versus requirements and to actual funding prioritization, which is shared with key players in the PPBE process.

(5) The critical part of the process is the analytical stage when programs and/or systems are evaluated for prioritization within the investment strategy. The evaluation and selection phase of the process is critical to sound investment strategy and is dependent upon timely data to support the prioritization discussions.

(6) Each program is evaluated within its investment area and then across the totality of IT requirements.

(7) The IT prioritization list developed through the process becomes the framework for the Army C4/IT investment strategy, adding value to the Army IT investments in three key aspects:

(a) Planners and programmers work collaboratively to determine optimal and affordable IT investments that will deliver a capabilities-based return on investment in support of TAP, the Army strategic planning guidance, enterprise initiatives, IT architectures, and DOD and/or Joint strategic planning guidance.

(b) The investment strategy is based upon a cross-cutting analysis of the value IT investments can leverage or balance across the three mission areas.

(c) Once the prioritization list and funding strategy is developed, they are briefed to the CIO/G–6 for refinement, revision, or approval. The investment strategy allows 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.

(8) Involving the MDEP managers and briefing the PEGs 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. For the

CIO/G–6 investment strategy process, the IT planning process develops a recommended funding prioritization list for use by the PEGs during the POM process. The 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 Army leadership in the POM and transformation efforts within the IT arena. This review can lead to potential measures, such as:

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

(b) Were the priorities linked to key enterprise initiatives and future force requirements?

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

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

(e) Was there an improvement in the "business capabilities" provided to the Army as a result of the coordinated investment strategy?

(f) Did the investment strategy coordinate the Army's technical capacity improvements across the operational and generating force, streamlining connectivity with an increase in capability, while controlling cost expenditures?

2–3. Army CIO/G–6 governance boards

The purpose of IT governance is to specify the decision rights and the decisionmaking mechanics necessary to foster desired behaviors in the management of IT. Although separate from organizational design, governance effectiveness is, in part, dependent on the existence of mature processes. This is essential to ensure IT is aligned with the Army's strategic vision and operational direction. The Army CIO/G–6 hosts two primary governance boards that support the enterprise information environment mission area: the CIO Executive Board (EB) and the Enterprise Guidance Board (EGB), see table 2–1. For more information and board charters, visit the CIO/G–6 Governance milWiki page at https://www.milsuite.mil/wiki/Army_CIO/G–6_Governance.

Table 2–1.
CIO/G–6 Governance Boards

Board Name	Purpose / Scope
CIO EB	Purpose: The CIO EB serves as a platform to share Army CIO/G–6 strategies, policies, action, and guidance with Army commands, Army service component commands, direct report units, and Department of the Army headquarters. It also will accept feedback and answer questions from the field. In addition, the CIO EB is charged with disseminating decisions from the CIO/G–6 EGB. Scope: The CIO EB is a strategic communications forum charged with advocating EGB decisions, providing and receiving feedback to and from the field, and keeping the Army abreast of key enterprise strategic initiatives.
EGB	Purpose: The Army EGB is the senior Army enterprise IT governance decision and advisory body which provides recommendations to the Army CIO/G–6. The EGB will advise and make recommendations to the Deputy CIO/G–6 to ensure that all enterprise IT decisions are in the best interest of the Army enterprise, are fiscally responsible, pose acceptable risk, and meet capability and customer requirements. Scope: The Army EGB's scope encompasses matters related to the Army CIO/G–6's Title 10, 40, and 44, United States Code responsibilities. The Board focuses on the Army's enterprise initiatives.

2–4. Performance-based strategic management

a. General. TAP is the Army's strategy, and the Army Campaign Plan (ACP) is the method by which the Army holds itself accountable for achieving that strategy. Performance-based, outcome focused management gives the Army the means to assess and track accomplishment of its strategy. Measuring performance locally and independently enhances decisionmaking at a local level. Measuring performance across an enterprise enhances decisionmaking on an Army scale and links Army effort and outcomes to the ACP, the Army Posture Statement, the Quadrennial Defense Review and the National Military Strategy. The requirement to conduct Armywide performance management across Army business operations is found in Public Law, DOD policies, ARs and orders.

b. Performance management. In general, performance management is the systematic process by which an organization involves its employees, as individuals and members of a group, in improving organizational effectiveness in the accomplishment of agency mission and goals. The process includes the high-level steps required to conduct periodic performance reporting and reviews using a consistent set of validated business rules, authoritative data, and calculated correlation with external Army and Department of Defense business processes and interdependencies. The CIO/G–6 performance management team is responsible for establishing and maintaining the IT performance management process. The performance management process includes:

(1) Reporting critical initiatives progress and trends towards the achievement of critical outcomes.

(2) Establishing business rules that govern the battle rhythm and details regarding reporting requirements, reviews, and corrective actions.

(3) Integrating with external processes or Army and DOD offices that provide input or rely on outputs of the performance management process. Using these processes and the enterprise tool, Strategic Management System (SMS), CIO/G–6 tracks current and emerging strategic trends and reports to the Army and DOD.

c. Strategic Management System. SMS is the Army's system of record for enterprise strategic management by which the Army provides an online tool to enable a linked and collaborative environment for organizations to report and track their level of strategic goals performance. SMS is administered and supported by the Under Secretary of the Army, Chief Management Officer, and Office of Business Transformation. The SMS system is available to all Army activities and is currently used by the Under Secretary of the Army, Chief Management Officer, the Vice Chief of Staff of the Army, the Assistant Secretary of the Army and other Army activities to track command initiatives and ACP objective's performance. SMS is available online at https://www.sms.army.mil/.

d. Performance framework. There are several elements of a performance framework to address for correct alignment of performance measurements across an enterprise. They include:

(1) Strategic plan. The strategic plan establishes a framework for performance management tracking and reporting. This multi-year plan should be aligned to the commander's intent, ACP major objectives, and the DOD Strategic Management Plan. The strategic plan should be a living document that is reviewed annually and updated to keep it current with superior initiatives and goals. It is from within the strategic plan that the activity's performance in support of the Army should be found. Specific elements for performance management are targets, measures, critical tasks, subordinate initiatives, strategic initiatives, and overarching strategy.

(2) Targets. Targets are the thresholds for performance levels. Targets are stated for each measure in terms of the presented data, currency, percentage or standard values.

(a) Stoplight system. In a stoplight type of system, each scored measure requires three targets. The first target is the full performance target, the next is the lower end of acceptable performance, and the third target is at the beginning of the potential failure level. In a time-series analysis, the targets would be the median, the upper control limit, and the lower control limit.

(b) Shifting targets. Targets can change over time. A shifting target width can be used to identify changing goals, such as to demonstrate improvement of process by narrowing the performance window or increasing threshold values to demonstrate shifting volumes of product. Sliding or shifting targets should never be used to manipulate measure status.

(3) Measures. Measures are the foundation of the performance reporting system. Measures must be reliable and quantifiable for credibility. Measures are the means by which objectives in terms of task completion are measured. These measures should identify timeliness, quality of execution and financial resources, commonly referred to as schedule, performance, and cost, respectively (percent of goal met, percent funded, dollars saved, quantity moved). Measures are reported against the targets over a given time period to gauge performance and evaluate effectiveness and efficiency.

(a) Measures are either leading or lagging. A leading measure is one that provides insight as to whether or not an expected outcome will be achieved. Leading measures are necessarily defined by the intersection of two related measures. A lagging measure is one that provides information about a process after the fact. These types of measures are useful in determining how a process is performed and as a basis for gauging improvement.

(b) Surrogate measures can be useful for rapidly defining and reporting project status; and as an interim or startup solution, they are acceptable but are the weakest type of measure. Nominal and ordinal scaled reporting is not a rigorous methodology for evaluating data using scientific analysis techniques, which eliminates the ability to determine process capability or provide a basis for improvement.

(4) Critical task. Tasks are the core of work. Below them are sub-tasks, which if done in isolation, do not provide a complete product; and, above tasks are jobs, duties, functions or initiatives. All of these are collections of tasks. Critical tasks require dedicated resources that are planned, programmed and monitored along functional lines of responsibility. The following task is critical and should be tracked for performance management reporting: determining if an action is a task is done by qualifying the output of the task statement. If the output is a usable product or action, the statement is a task.

(5) Strategic initiative. Aligned to the ACP or Strategic Management Plan objective shared across commands, Headquarters, Department of the Army (HQDA), and so forth.

(6) Subordinate initiative. These are activity objectives. They define strategically what must be accomplished to achieve the strategic initiatives. These should consist of one or more critical tasks. Not all subordinate initiatives must necessarily align to higher level initiatives.

(7) Overarching strategy. The overarching strategy is the high-level strategic end-state – the goal.

e. Army Information Technology Metrics Program.

(1) Purpose. The Army IT Metrics Program provides a common framework for installation commanders and IT managers to assess the status of IT operations and infrastructure. The program collects data on a quarterly basis from all active Army installations, U.S. Army Reserves (USAR) and ARNG elements, including virtual installations. By

gathering and analyzing the data and identifying mission capability shortfalls, commanders and IT managers at all levels can make informed decisions regarding allocation of IT investment resources.

(2) Overview. IT Metrics is a CIO/G–6 program, managed by Network Enterprise Technology Command (NETCOM). The data collected through the Army IT Metrics Program provides a snapshot view of the IT infrastructure and operations provided by the Network Enterprise Center (NEC) at Army installations, as well as USAR and ARNG networks and operations in their virtual installations. This same data is used to assist in developing base operations funding requirements for NEC services, substantiate budget requests and develop compelling arguments as the information management community competes for scarce Army resources.

(a) The data collected focuses on installation NEC controlled infrastructure and operations. Types of measurement data collected include response time, availability, workload and capacity. Much of the data required for IT metrics is available within the NEC organization. However, some data may be captured at an enterprise level by an Army data center or a theater network operations and security center (TNOSC) for components of a base operations service provided. This requires the Army data center or TNOSC to report specific metric data to the supported NEC.

(b) The IT metrics quarterly reporting methodology allows installation commanders and IT resource managers to identify, at a glance, which specific IT services have the greatest relative shortfall from full mission capability. Furthermore, the relative ratings of the individual metrics enhance the IT manager’s ability to determine the elements of an individual’s infrastructure that contributes most to the shortfall. Appropriate decisions can then be made regarding reallocation of resources or shifting of management focus.

(c) HQDA compilation of the data submitted to the Army’s IT Metrics Program facilitates compliance with two key pieces of legislation.

1. The Government Performance and Results Act, passed in 1993, requiring departments to develop a strategic plan prior to fiscal year (FY) 1998, to establish annual performance goals by FY1999, and to report on actual performance compared to goals in FY2000.

2. Title 40 USC (Clinger-Cohen Act), effective as of August 1996, mandates a process to select, manage, and evaluate the results of IT investments.

(3) Structure. The structure of the Army IT Metrics Program is based upon the Command, Control, Communications, Computers and Information Management (C4IM) Services List. Metrics have been developed to measure the standards for specific tasks in each primary service category.

(4) Reporting process. AR 25–1 requires senior IM officials to provide oversight and management for the installation’s participation in the Army IT Metrics Program, which includes collecting, compiling, and reporting IT data on a quarterly basis via the IT metrics Web-based application.

(a) Individual Army installation NECs collect the data measurements and report (via the IT metrics Web-based application located at https://www.itmetrics.hua.army.mil) to their respective region IT metrics representatives. The region IT metrics representatives coordinate with the installation level personnel to review the data inputs. Once the data has been reviewed, corrected, and/or modified and agreed upon between the installation level and the region level representatives, the data is then “validated” at the region level and submitted to the HQDA level for “official record.”

(b) Validation of installation data by the region IT metrics representatives is based upon several factors. Factors could include comparison of previous quarter’s data, identification of installation-wide or region-wide trends, application of personal knowledge, evaluation of the technology supporting each metric and the incorporation of Army strategic guidance and plans affecting each installation. Validation of installation data is a team effort, pulling from the experience and knowledge of the personnel located at the NEC, as well as the region IT metrics representatives, NETCOM and other Army organizations.

(c) The IT metrics application produces the Army Information Technology Metrics - Service Quality Rating Report. This generated report breaks down the data input for each installation and displays each individual metric’s performance ratings in a green, amber, red, or black color format.

(5) Data gathering. Installation IT managers and professionals gather, compile, and consolidate 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: Measure 1, Measure 2, Primary Funding Source, and Source of the Data. Explanations for each data element may be found at https://www.itmetrics.hua.army.mil.

(6) Percentage rating. The ratio of “Measure 2 divided by Measure 1 times 100” results in a percentage rating for each specific metric. This percentage rating then corresponds to a green, amber, red, or black “color”-formatted performance standard for each individual metric set by the Service Level Management (SLM)/IT Metrics Work Group and approved by the CIO/G–6. A performance standard rating color of “green” represents full mission capability; a rating of “amber” or “red” could represent some relative degree of degradation from full mission capability, and a rating of “black” represents mission failure.

(7) Integration with the Installation Status Report (ISR)-Services Program. The collection of individual metrics from each NEC is linked to the Assistant Chief of Staff for Installation Management (ACSIM) and other Army initiatives. Compilation of IT metrics data at each installation facilitates the NEC’s ability to provide quarterly input to the ISR program.

(a) Deployed by the ACSIM, the ISR–Services portion of the program captures the ability to provide IT support.

The evaluations of these ISR–Services are reported in the green, amber, red, or black color service quality rating format.

(b) The most important link between the IT Metrics Program and the ISR is the support of specific Army installation services. The Army's IT Metrics program feeds infrastructure capabilities and performance measures into the ISR–Services portion of the program. The ISR–Services data is in turn fed into the Defense Readiness Reporting System – Army with subsequent reporting into Defense Readiness Reporting System, a DOD system. IT metrics data is collected, and input is provided supporting the following Army installation services:

1. Service 15 (ISR PM Series 701) - Communications Systems and Systems Support.

2. Service 18 (ISR PM Series 703) - Information Assurance.

3. Service 19 (ISR PM Series 700) – Automation.

(c) The quarterly IT metrics data collected correlates the performance data (reflected in the ISR–Services green, amber, red, or black service quality ratings) to costs (contained in the ISR–Service Cost model) to provide cost estimation data. This cost estimation data is fed into the Standard Service Costing model; a methodology used to develop predictive cost equations to estimate what a service "should" cost based upon historical performance levels and standards. This information is fed by HQDA into the Battlefield Operating System Requirements Model for use by the Installations PEG and MDEP managers in defense of POM requirements, specifically for NEC services. To make it simple, the data input into the Army's IT Metrics Program is intended to assist in the development of base operations baseline requirements for NEC services.

(8) Army IT metrics Web site. The IT metrics Web-based application, supporting the Army IT Metrics Program, is common access card (CAC) authenticated behind Army Knowledge Online (AKO).

(a) To access the application, go to: https://www.itmetrics.hua.army.mil.

(b) Upon arrival to the page, the Army IT metrics "splash" page appears. From the "splash" page, a user can log into the application, request an account, access information regarding the program, access the online version of the LandWarNet Services Catalog, and download the current copy of the C4IM Services List.

(9) Summary. The Army IT Metrics Program allows for interactive support to installation managers via the IT metrics Web-based application. Commanders and IT managers at all levels can use the IT Metrics program as an effective management tool which provides a clear evaluation of the IT infrastructure readiness posture and enhances their ability to properly allocate limited IT resources. As the program matures, the intent is to include metrics that will support SLM and service level agreements (SLA) with installation IT customers.

2–5. Planning, programming, budgeting, and execution for information technology requirements and capabilities

a. General. Information resources management processes for planning, selecting, controlling and evaluating IT align with the individual elements of the PPBE process; and the CIO/G–6 is responsible for oversight of IT resources and assessment, and develops and coordinates investment decisions at the Army enterprise level for IT expenditures.

b. Planning. Understanding the requirement for IT capabilities is an important aspect of the PPBE process. Every echelon within the Army plans for its future and provides those plans to its higher headquarters to be aligned with TAP, the Army Strategic Planning Guidance, Enterprise Initiatives, and DOD and/or Joint Strategic Planning Guidance. IT requirements may be identified at any Army echelon level.

c. Requirements identification. IT requirements and/or capabilities may be identified 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. ACOM commanders may also identify urgent IT requirements and capabilities through a narrative assessment of the ACOM's ability to accomplish its mission, identify significant shortfalls and internal resource adjustments, as well as adjustments with other ACOMs, as part of the POM process.

d. Guidance for the Information Infrastructure Modernization Program. While the MDEP requirements process is generally implemented as stated above, MDEPs contain many different requirements that demand tailoring by the CIO/G–6 MDEP managers to ensure appropriate stakeholders are consulted for development, review and requirements validation. Below is the tailored process for capturing requirements for the Army's, Installation Information Infrastructure Modernization Program (I3MP):

(1) Installation functions. Senior IM officials on the installation will coordinate first with the primary IM/IT manager (for example, mission commander's senior IM official), who in turn, will work with the NEC in helping to identify new or future mission requirements which need C4/IT infrastructure and/or improvements as part of the I3MP process. Required communications, IT, and video requirements within the facility or building will be presented to the NEC as part of the I3MP requirements definition process.

(2) NEC functions. The NEC is the central collection point for all I3MP requirements for their respective installations. NECs will formally gather and/or identify I3MP requirements and forward to their respective higher headquarters for review, that is brigade or theater command. The theater commands will gather all I3MP requirements in their respective area of responsibility and forward to NETCOM for validation and prioritization.

(3) NETCOM functions. NETCOM provides a technical control review and validates all enterprise-level fielding

requirements. NETCOM validates all I3MP requirements and in coordination with the theater commanders, develops a prioritized list of I3MP requirements.

(4) Army Cyber Command/2nd Army functions. Army Cyber Command/2nd Army reviews and approves the I3MP prioritization list and forwards to HQDA CIO/G–6 for final disposition.

(5) HQDA CIO/G–6 functions. CIO/G–6 serves as the final approval authority for all requirements and requests for support from the I3MP and provides the Program Executive Officer (PEO), Enterprise Information Systems with an Integrated Requirements List directing the priority in which the requirements are to be executed, along with funding to execute the material development of the capabilities required.

e. Reporting. The reporting of Army IT budget resources to Office of the Secretary of Defense (OSD), OMB, and the Congress is submitted in separate budget exhibit documents, Exhibits 53 and 300 respectively. These exhibits are reported twice a year. OMB Circular A–11 and 40 USC (Clinger-Cohen Act) define the IT resources that must be reported and the process for reporting them.

(1) 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, 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.

(2) These business cases should include security, privacy, enterprise architecture, and provide the effectiveness and efficiency gains planned by the business lines and functional operations.

2–6. Army Portfolio Management Solution

a. In support of 40 USC (Clinger-Cohen Act), DOD Portfolio Management Directives and the National Defense Authorization Act of 2005, the Army Portfolio Management Solution (APMS) was implemented in 2005 across the Army as the sole source for meeting IT investment management requirements at the enterprise, mission area, domain, and command levels. APMS and current investment management processes allows the Army to manage IT investment spending by aligning IT investments to Army strategy and functional capabilities provided. The Army strategic objectives are as follows:

(1) Integrate architectures within investments,

(2) Develop a coordinated Enterprise IT Investment Strategy,

(3) Ensure compliancy and certification,

(4) Identify redundant and/or inefficient systems by Functional applications and Enterprise-wide,

(5) Improve program planning and execution.

b. APMS provides the ability to support the objectives listed above plus an enhanced decision support tool for improved investment rationalization. APMS also serves as a critical enabler of enterprise-wide IT investment sharing by making all investments visible, accessible, and understandable to users throughout the Army, supporting IT rationalization at all levels – enterprise, mission area, domain, and command.

c. APMS contains the Army's inventory of active IT investments. Additionally, it is the inventory of IT investments deleted from the registry, for historical reporting and reference purposes. APMS will be used for portfolio data call collection, certification of funds, and consolidated reporting to OSD and Army requiring offices. APMS is the Army's feeder system to the DOD Information Technology Portfolio Registry (DITPR). APMS includes functionality to add, delete, and transfer IT systems from the Army IT registry.

d. APMS is used for two primary functions:

(1) Portfolio and investment management. This ensures hardware, software or services are managed for strategic alignment, performance, environmental impact, risk, cost, redundancy and gaps.

(2) Compliance reporting and certification process. There are seven areas of compliance data: Federal Information Security Management Act (FISMA), E–Authentication, PIAs (Privacy Act), mission criticality, public key infrastructure (PKI), standard financial information structure (Federal Financial Management Improvement Act) and interoperability. To aid with compliance with the National Defense Authorization Act for FY12, as designated by the Under Secretary of the Army, APMS is the authoritative listing of IT investments and will be the source of information to certify business mission area IT funds.

e. All Army funded IT, including computing infrastructure, hardware, software, services, initiatives, prototypes and investments must be accounted for individually or as a component of a record in APMS with the exception of:

(1) IT that is physically part of, internal to, or embedded in a platform used to operate, guide, or steer the platform itself (for example, avionics, guidance, navigation, flight controls, maneuver control, navigation).

(2) IT which is integral to real-time execution of the platform mission (for example, sensor-to-processor links, radar, voice communications, targeting systems, medical imaging or monitoring technologies, training simulators, energy or other utility supervisory control and data acquisition systems).

(3) Additionally, any system requiring an accreditation or other specific compliance reporting requirement, regardless of funding source or amount, must be registered in APMS. IT will not be double reported, but relationships will be identified using the parent/child relationships.

(4) For APMS registration criteria, see AR 25–1.

f. APMS is the feeder system to DITPR. There are two types of registrations in APMS:

(1) DITPR reportable. This includes any investment that requires any compliance reporting aspect as well as all defense business systems including modified commercial-off-the-shelf (COTS) IT.

(2) Non-DITPR reportable. An investment for which the Army is not the executive agent but uses an Army appropriation. Command unique IT is often registered as non-DITPR reportable. An example of command unique IT that would not be reported to DITPR is accounting for the expenditure of funds on hardware for a certain command. A command could register and capture such investments under a single non-DITPR reportable item.

(3) IT investment registration. Regardless of registration method (DITPR reportable or non-DITPR reportable) – you must complete the entire registration process using the Candidate Registration folder.

g. For DITPR reportable items, all mandatory trigger questions must be completed. Completion of these questions may require conditional data elements to be completed. APMS uses both “stoplight” indicators and textual comments to aid in the completion of all required data elements. The Army Additional Data, Required and Budgeted Detail folder (for Financials), the Decision Support folder, the Joint Common Systems Function List, Joint Capability Areas, and Business Enterprise Architecture Capabilities must be completed. For non-DITPR reportable items: Required Data folder (Army required and parent/child relationships only), the Financial Data folder, the Decision Support folder, the Joint Capability Areas, Business Enterprise Architecture Capabilities and the Joint Common Systems Function List must be completed. Identify all hardware, software and services that support an investment using the Investment Components Tab.

h. The APMS Desk Side Reference Manual is updated on an as needed basis and explains the functionality of the APMS data entry module, the workflow module, and the standard reports. There is also a separate reference manual which details the functionality and use of the ad hoc reporting capability. Ad hoc reporting permits users to create and save their own tailored reports.

(1) Data entry module. The APMS data entry module is the Army’s inventory of active IT investments in APMS. This module is used to make all data updates to individual systems. A Web service with DITPR updates information on a nightly basis. Functionality in this module allows for the registration, deletion and transfer of items between portfolios.

(2) Workflow module. The workflow module is used to manage the approval processes for candidate registrations, deletions and transfer requests.

(3) Reporting module. The reporting module is used to view and customize scorecards for internal and external reporting requirements. These reports are used to manage multiple investments.

(4) Standard reports. Standard reports have been developed for the key DITPR compliance areas such as FISMA, PIA, and interoperability.

(5) Ad hoc reports. Ad hoc reports provide the functionality to create and save tailored reports. There are two ad hoc reports, one with and one without financial data elements. The ad hoc report without financial information is available to all APMS accounts holders. The ad hoc with financials is only available to administrators and analysts at the command, domain and mission area levels.

2–7. Procurement of information technology requirements

a. Requirement to use computer hardware, enterprise software and solutions (CHESS). The CHESS system is the primary source for establishing commercial IT contracts for hardware, software, and services (not applicable to IT hardware or software embedded in weapons platforms). CHESS 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 purchase of IT hardware and software from a non-CHESS vendor requires a waiver from CHESS. All waiver requests must include a rationale explaining the extenuating circumstances or unique configurations required by the mission and not available through CHESS. Waivers may be submitted through the CHESS Web site at https://chess.army.mil. If additional assistance is needed, the CHESS helpline is available at 888–232–4405 for continental United States (CONUS) and 732–532–7950 for outside continental United States (OCONUS).

(1) Anyone may search or browse the Web site. Users wishing to request a quote or execute a shopping cart must be logged in to the site. Army users who are registered with AKO are automatically registered to use the site.

(2) Business-to-business capabilities allow customers to order contract-compliant, custom-configured solutions direct from CHESS contract and blanket purchase agreement (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.

(3) Shopping carts may be sent through a user-defined approval or workflow process. This module assists customers in handling order approvals by providing cart information.

(4) Customers may issue requests for quotes to one or more CHESS contract or BPA holders simultaneously using IT e-mart.

(5) IT e-mart provides backup documentation for IT orders. Contract-specific instructions and information is

provided for Standard Form (SF) 1449, (Solicitation/Contract/Order for Commercial Items) to aid customers in completing paper-based order requisitions.

(6) Hardware acquired to support UC must be listed on the DOD Unified Capabilities approved products list, https://aplits.disa.mil/.

b. Goal 1 Waivers. AR 25–1 establishes Army policy for the procurement and sustainment of all IT hardware, software and services. Goal 1 waivers support the Secretary of Defense's IT consolidation initiative to achieve greater economies of scale, be more efficient, effective and cost-conscience by directing the use of CHESS, CHESS consolidated buys, and enterprise license agreements (ELAs). The goal 1 waiver process provides the visibility required to ensure that dollars spent on IT initiatives are appropriately justified, verified, and documented to meet Army IT guidelines.

(1) Applicability. This guidance applies to all IT expenditures using non-IT programmed funds that exceed the dollar thresholds of $25,000 for operations and maintenance, Army funds and $100,000 for research, development, test and evaluation, and any purchases subject to a moratorium regardless of dollar amount.

(2) Procedures. The Army CIO/G–6 publishes annual 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.

(3) Waivers. All waiver requirements are processed through the workflow process automation application. The waiver and accompanying workflow instructions may be accessed at https://adminapps.hqda.pentagon.mil/akmg1w/index.html. A link to the End-User Guide is also provided on the application's main page.

(4) Operational tempo funding. To migrate or reprogram Activity Group 11 operational tempo funding (ground and air), Commands must submit an operational tempo migration request, in addition to a Goal 1 waiver.

c. Purchase of energy-efficient IT equipment. All purchases of IT equipment, including computers, monitors, and other peripheral equipment (for example, printers, copiers, all-in-ones, and facsimiles) must meet the Environmental Protection Agency Energy Star and Electronic Product Environmental Assessment Tool requirements for energy efficiency per Executive Order 13514.

d. Commercial information technology management process.

(1) Modified Table of Organization and Equipment (MTOE) unit's mission essential common COTS IT equipment must be procured in accordance with the COTS IT management process which determines, validates, and resources requirements in order to accomplish operational tasks. COTS IT includes computers, printers, and digital senders that are non-acquisition program equipment. Under the COTS IT management process, U.S. Army Training and Doctrine Command (TRADOC) assesses and determines requirements by organization; ODCS, G–3/5/7 validates requirements; and ODCS, G–8 resources requirements into POM submissions.

(2) MTOE units will use the required authorization document (Common Table of Allowances 50–909) to request, purchase, or replace COTS IT hardware through their property book manager and CHESS within their resource allocations. MTOE units are authorized to replace up to 25 percent of their authorized COTS IT per year.

2–8. Information Technology Systems Acquisition and Delivery Strategies

a. Clinger-Cohen Act. The CIO/G–6 is responsible for 40 USC (Clinger-Cohen Act) compliance. 40 USC (Clinger-Cohen Act) authority determinations are made by the organizations shown in figure 2–1.

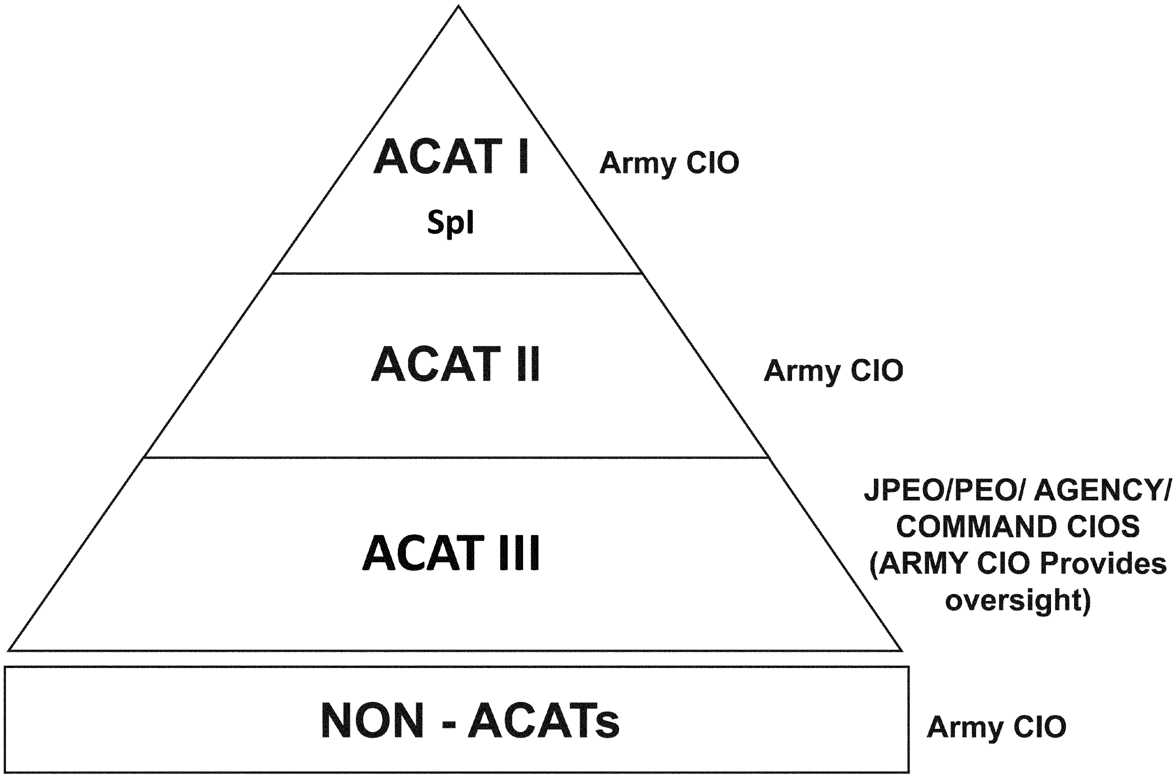


Figure 2–1. CIO 40 USC (Clinger-Cohen Act) authority

b. Business process. The CIO/G–6 tool is the automated information system on the AcqBiz Central Portal (https://acqdomain.army.mil) which is used to assess 40 USC (Clinger-Cohen Act) compliance. After the PM provides responses to a self-assessment, CIO/G–6 evaluates the self-assessment responses, and a determination is recommended and staffed for signature. This business process is highly streamlined and is reviewed and/or updated biannually to ensure current statutory, regulatory, and policy requirements are met in accordance with DODI 5000.02.

(1) The 40 USC (Clinger-Cohen Act) assessment determination is made by the CIO/G–6 for all acquisition category (ACAT) I, II, and special interest programs. ACAT I and special interest programs are, however, forwarded to DOD CIO for a final determination.

(2) ACAT III assessment determinations are made by the delegated Joint Program Executive Office, PEO, Agency or Command's CIO per AR 70–1 and AR 25–1. Upon completion of the compliance determination, the delegated CIOs are required to upload the determinations to the 40 USC (Clinger-Cohen Act) repository located in the AcqBiz Central portal. The CIO/G–6 reports semi-annually ACAT III compliance results in an oversight role.

(3) Non-ACAT assessment determinations are made by the CIO/G–6 using a streamlined process in the APMS to meet AR 25–1 and 40 USC (Clinger-Cohen Act) requirements.

c. Enterprise resource planning. The U.S. Army Shared Services Center (part of the Army's Armament Research, Development and Engineering Center) provides life cycle systems engineering and management of assigned Business Information Management Systems. The engineering and management focus is enterprise resource planning to meet Army's current and future mission requirements. This vision standardizes Business Information Management Systems through enterprise resource planning software engineering life cycle activities. The end result ensures compliance with policies, standards, procedures, and technical architectures for management IT systems and products to ensure that integral resources are planned, developed, tested, acquired, fielded and supported in a cost-effective manner. For more information, contact the Army Shared Services Center: A–SSC, Building 93, Picatinny Arsenal, NJ 07806–500.

d. Procurement strategies. Customers and providers of information systems must be aware of the various procurement approaches available for acquiring IT systems and services. CHESS is the required source for purchases of COTS software, desktops, and notebook computers, and all other IT purchases, regardless of dollar value (see para 2–7). If a contract vehicle is not available on a CHESS contract, DOD enterprise software initiative (ESI) or the Federal Supply Schedule (FSS) and the requirement is greater than $500,000, the customer should contact the Army Contracting Command, National Capital Region Contracting Center, and/or Information Technology E–Commerce and Commercial

Contracting Center (ITEC4) and provide data to support a fair and open competitive procurement. The scope and cost factors (program and life cycle) determine if the IT acquisition should be managed at the ACOM or Army level. See AR 70–1 and DA Pam 70–3 for the definitions and thresholds of acquisition categories.

e. Methods of acquiring IT supplies and services over $500,000. IM and IT managers should be aware that the ITEC4 is the Armywide 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 and IT managers must send requirements for computing-related services over $500,000 to the ITEC4 for disposition by the local director of procurement. This includes all requirements that are contemplated as outsourcing opportunities through another agency, such as the General Services Administration (GSA) or Department of the Interior. IM and 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 the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (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 not any 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.

f. Purchases. 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 additional 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.

g. Micro-purchases. Using this method, IT purchases are made using a simplified procedure.

(1) Before purchase, the NEC must validate all IT procured using the micro-purchase process to ensure supportability and compatibility with the network.

(2) A micro-purchase is a simplified acquisition procedure for purchases under $3,000. Organizations should refrain from over-reliance on micro-purchases, and consider consolidated buys to gain economies of scale benefits. Micro-purchases need not be set aside for small business and, if the price is considered reasonable, may be awarded without soliciting competitive quotations.

(3) A micro-purchase is a procedure, rather than a source, and involves the placement of an order against an existing contract. Micro-purchases 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 micro-purchase requires only going to a local store or ordering from a supply catalog. Purchase cards are used for all micro-purchases, unless an exception has been granted (see paragraph 2–10).

(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 micro-purchase threshold.

h. 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 and/or 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, after conducting a benefit to cost comparison. Army activities need to factor in the cost to overwrite, degauss, and/or destroy hard drives or any other storage media that is part of the leased equipment.

i. 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 non-mandatory 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) Multiple award schedule. 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) Blanket purchase agreements. 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 and/or 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 and/or delivery orders. BPAs are determined on best-value per FAR 8.404. BPAs should be reviewed yearly to ensure they remain 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, and so forth.

j. Other IT acquisition and delivery options. CHESS has an array of fully competed contract vehicles to meet Army requirements for purchasing IT of all types. CHESS contracts must be considered first, before buying from contract vehicles from other sources. If an Army customer chooses other than a CHESS contract vehicle that is available, CHESS must first grant a waiver. If an Army customer chooses other than a DOD ELA for a software purchase that is available, CHESS must first grant a waiver. A complete list of CHESS contracts, DOD ELAs, and the online waiver process is available at https://chess.army.mil.

(1) Outsourcing. Outsourcing IT support is an alternative or adjunct to an in-house workforce. A Cost/Benefit Analysis or other comparative analysis should be performed, before committing to a contracted form of IT support.

(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 personal computers (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 Defense Information Systems Agency (DISA) regional support activities throughout the CONUS.

(d) Additional information on Defense enterprise computing centers services may be obtained from the CIO/G–6, Architecture, Operations, Networks, and Space (AONS).

(5) Communications-Electronics Command (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, ATTN: AMSEL–CG, 6002 Combat Drive, Aberdeen Proving Ground, MD 21005–1845. Their services include: integration of battlespace and sustaining base systems, C4IM-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.

2–9. Redistribution and disposal of information technology assets

a. The screening, redistribution, and disposal of IT equipment are completed through the Defense Reutilization and Marketing Service (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 NECs 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.

c. Per DOD policy, all hard drives of unclassified computer equipment leaving the custody of DOD, including disposal through the DRMS, must be overwritten, degaussed, or destroyed in accordance with the associated security risk of the information contained within the drive. NECs and/or property book officers will ensure that hard drives are disposed of using the methods and procedures prescribed in AR 25–2.

d. Hard-drives used in a classified environment or involved in a spillage incident will never be released outside of Army. They will remain under Army control, until the end of their usefulness and then will be destroyed in accordance with AR 25–2. 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 DD Form 1348–2 (Issue Release/Receipt Document with Address Label) must accompany all property.

e. Turn-in procedures for computers without hard drives require the following:

(1) A DD Form 1348–1A or DD Form 1348–2 (filled out completely).

(2) The computer chassis serial number in block 26 (optional).

(3) One required statement either on/or with DD Form 1348–1A or DD Form 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 computer.

(8) Removal of the following computer media and cards from all turn-in computer equipment: compact flash cards, secure data cards, optical 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 computers with hard drives require the following:

(1) Ensuring that the hard drive (notebooks, desktops, laptops, and docking stations) has been degaussed or overwritten.

(2) Completing DD Form 1348–1A or DD Form 1348–2 (filled out completely).

(3) Labeling the computer chassis and/or housing serial number in block 26 (optional).

(4) One required statement either on/or with DD Form 1348–1A or DD Form 1348–2 and two optional statements.

(5) Labeling the hard drive using DLIS Form 1867 or equivalent.

(6) Ensure the following computer media and cards are removed from all turn-in computer equipment (internal devices such as graphic, sound, network or controller cards may stay in the computer):

(a) Compact flash cards, secure data cards, optical media.

(b) Media, smart card media, microdrives, multimedia.

(c) Memory 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 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 that do not fall under the category of classified, tempest or hazardous waste:

(1) A disposal turn-in document (DD Form 1348–1A or DD Form 1348–2) for each national stock number and Federal Supply Group/Federal Supply Classification, 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 disposal turn-in document if the generator requires verification that the hard drives were turned in to the Defense Reutilization and Marketing Office (DRMO) as scrap.

(4) Removal of monitors, printer (toner must be removed), keyboards, speakers, modems, mouse/mice, plotter (toner must be removed), and external devices.

i. Turn-in procedures include the following:

(1) Hand-receipt holders will —

(a) Turn-in to the unit Property Book Office (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 sub-hand receipts are updated to reflect turn-in.

(2) The unit PBO will prepare documentation (DA Form 3161 (Request for Issue or Turn-In)) required for disposal or redistribution.

j. Procedures for IT turn-in include the following:

(1) The hand-receipt holder —

(a) Completes a DA Form 2407 (Maintenance Request) for each item requiring turn in and submits DA Form 2407 to NEC.

(b) Once the NEC 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 NEC.

(b) Prepares documentation (turn-in and/or lateral transfer, DA Form 3161) required for disposition or redistribution instructions as determined by the NEC and forward to the NEC.

2–10. 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 hardware and software, with CHESS as the required source for these purchases. CHESS contracts are the preferred source for the acquisition of IT services when no small business capability exists. 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 CHESS contract vehicles.

(2) Order from DOD ELAs.

(3) Order online from the CHESS electronic commerce (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. Most CHESS contract vehicles allow for credit card purchases. The CHESS IT e-mart allows for online credit card ordering. For FSS items, follow the online directions for competitive procedures. For open market items, the person who makes the order should verify and document 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. Approval and oversight of IT purchases. Purchases are approved by the senior IM official and coordinated with the installation NEC for concurrence, input, network compatibility, and supportability 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 the purchase card without senior IM official or NEC approval.

2–11. Information Technology Management Career Program–34

The primary asset of today's organization is its human capital. The Army must attract and develop the right talent to create an expert and enduring future force to meet the emerging challenges in IT and cyberspace operations. The CIO/G–6 oversees Career Program-34 (CP–34), one of the Army's largest civilian career programs. CP–34's goal is to create a competency-based workforce with agile skills in IT and cyberspace operations. CP–34 identifies training requirements based on competencies and career maps linked to Army IT jobs. CP–34 provides career development to Army civilians in three domains: training to develop applied knowledge and skills (outreach courses in core competencies and new technologies and Signal Center courses); education to expand the understanding of IT Management (ITM) and cyber concepts and practices (academic programs at universities and defense institutions such as the National Defense University Information Resources Management College (iCollege); and developmental assignments and training with industry. Many of today's and tomorrow's ITM civilian leaders are the products of CP–34 career development programs.

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 and 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) Army Knowledge Management initiatives, as mandated by the Secretary of the Army and the communications service authorizations.

(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) CP–34 includes the following job series:

(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.

(6) CP–34 training opportunities are available on a competitive basis to ITM professionals at GS–11 and above (GS–09 by waiver).

b. CP–34 professional development. The CP–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; https://informationassurance.us.army.mil.

(5) Cyber Security and Cyberspace Operations.

(6) ITM program and project management emerging technologies (biometrics, e-business, e-Government, and so forth).

(7) Business leadership.

(8) Public policy and/or public administration.

c. Sponsored programs.

(1) National Defense University iCollege, Fort McNair, Washington, DC (www.ndu.edu/iCollege/) offers leading edge education through the CIO and information assurance (IA) certificates and other certificate programs (eight 5-week courses), the 14-week residential Advanced Management Program (AMP), and the Government Information Leadership Master of Science degree. These programs can provide up to 15 graduate credits toward an advanced degree, offered by a National Defense University partner school. Tuition is free for Army and DOD employees who meet the eligibility criteria. Most certificate courses are also available through distance learning.

(2) The U.S. Army Signal Center, School of Information Technology, Fort Gordon, offers a curriculum of IT courses, including Microsoft and Cisco courses.

(3) Outreach training courses are provided to regional sites, including OCONUS, to reach geographically-dispersed

audiences through classroom and virtual training. Focus is on single topics such as IT Project Management, Information Technology Infrastructure Library (ITIL), Cloud Computing, the accreditation process, VMWare and other emerging technology topics.

(4) Academic degree training prepares ITM professionals to face the rapid pace of work, complex problems, and changing requirements, with a solid course of study gained through graduate or undergraduate degrees in ITM or management-related topics. CP–34 aims to have an educated workforce to develop problem-solvers, decision-makers, team-builders and organizational leaders at all echelons of the Army. Only the highest caliber applicants, whose intent for academic degree training directly supports the Army's critical mission areas, are funded. Students have a wide range of available training modalities, such as distance learning, virtual classroom, and blended learning, regardless of where in the world they are located. The CP–34 academic degree training courses are taken on non-duty hours, with the exception of certain capstone courses that may require residential or daytime participation. Notable programs that directly support the Army's IT/IA mission are located at the following universities: Norwich, Syracuse, Virginia, George Mason and other National Defense University partner institutions.

(5) All CP–34 sponsored programs and services are publicized on the ITM Careers Web site: https://www.us.army.mil/suite/page/530206/. All programs are offered by a competitive application process and require endorsements by the chain of command through the command career program manager. For additional information on CP–34, visit http://cpol.army.mil/library/train/.

Chapter 3
Web Site Management

Section I
Army Enterprise Portal

3–1. Army Enterprise Portal overview

a. The Army enterprise portal supports the Army business units and the Warfighter. AKO (www.us.army.mil) is the enterprise Web portal supporting unclassified Army Web sites and is the current source for collaboration and coordination of Army's non-public information. Army Knowledge Online secret Internet protocol router network (SIPRNET) (AKO–S) is the portal supporting classified Army Web sites. The enterprise portal 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 the AKO enterprise portal includes enterprise user authentication, user assistance, enterprise search and retrieval, self service functions, access to functional and/or domain specific applications and services through single sign-on (SSO) and enterprise collaboration services.

c. The enterprise portal 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 the enterprise portal through user assistance functions.

3–2. Army Enterprise Portal access

a. The enterprise portal is the gateway to all Army information, systems, and services. The most current version of AKO account procedures is available at https://www.us.army.mil/suite/doc/4084113/.

b. The owners of Intranet application and subordinate portals 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 via their AKO account details; the application or subordinate portal linked to the enterprise portal 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, or the Defense Enrollment Eligibility Reporting System (DEERS). As additional security measures beyond the password process are implemented for Army systems (for example, PKI, CAC, biometrics), the portal enterprise directory will make the necessary engineering changes to incorporate these features. Procedural and directory service interfaces between the portal enterprise directory and other Army applications eliminate the additional development costs for those applications.

d. To secure access to Army IT systems in accordance with DODI 8520.02 and Communications Tasking Order 07–015, all applications and devices will be configured to allow authentication only via PKI credentials. All Army IT systems utilizing usernames and passwords via AKO for authentication must convert to PKI-only authentication for users. Family members and retirees will continue to access authorized IT systems via usernames and passwords per AR 25–1. Authorized external users can access Army IT systems via the Federal Bridge, External Certification Authority.

e. In accordance with Army policy, email encryption and digital signature certificates issued on the CAC/PKI are based on DOD Enterprise Email email addresses (that is, FirstName.MiddleInitial.LastName#.PersonaTypeCode@mail.mil).

(1) The Defense Manpower Data Center is the authoritative source for DOD Enterprise Email addresses, which are unique to each persona and CAC.

(2) Active directory account administrators must ensure that the userID for active directory accounts matches the userID portion of the DOD Enterprise Email address.

f. 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, or when there is a serious rules violation on the account.

(e) Ensure all accounts for non-U.S. citizens are approved through proper channels as outlined in AR 25–2.

Table 3–1.
Account categories and types

Account category	Account category
Full account	active Army[1] ARNG[1] AR[1] DA Civilian[1] Nonappropriated fund (NAF) Civilian[1] 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 servicemember 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 email only account	A sponsored account allowing only access to AKO email. 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 (see AR 25–2).
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:
[1] Full account holders authorized to sponsor accounts.

(2) Sponsored accounts are enterprise portal accounts for users being sponsored by a full account holder. Sponsored accounts are to be established only for persons with a legitimate need for portal access to perform Army business or for morale and welfare purposes of our Soldiers. Sponsored accounts require annual renewal.

(3) "Email only" accounts are another form of a sponsored account.

(4) Family member accounts can be automatically verified through DEERS. For Family members under the age of 18, approval must be granted by a full account holder, before the activation of the family member account. A family member account will be deactivated, once eligibility is lost under DEERS. A sponsored account may be established for extended Family members, such as parents and siblings, without DEERS benefits, if legitimate needs exist.

(5) 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.

(6) 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 notated. In addition, descriptive information, including nationality, is displayed for foreign officials, as required by AR 25–2. Additional guidelines and examples for user identifiers are as follows:

(a) All full accounts and family member accounts have a friendly name (includes rank, account type, and so forth) noted after the email or in place of the email address. A full account would be displayed as jane.b.doe@us.army.mil (LTC/Army); a family member account as james.j.jones@us.army.mil (FMA).

(b) Contractors have CTR (for contractor) and abbreviation of company name added to their friendly name and“.ctr” added to their email address, for example, john.b.doe.ctr@us.army.mil (CTR–Smith Consulting).

(c) Foreign nationals and local nationals receive email addresses, including their account type and country code, for example, jane.doe.UK.com@us.army.mil or fred.jones.1n.jp.com@us.army.mil. The type of foreign official will be displayed in the friendly name, as outlined in AR 25–2.

g. Changes to AKO portal’s user account names may be required because of marriage, divorce, or other legal requirements. Full accounts and family member accounts are validated against an Army or DOD personnel database; therefore, the account holder is required 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 enterprise portal account as long as they are eligible in DEERS.

h. The following user functions and guidelines apply:

(1) Each enterprise portal 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 and are accountable for their actions on the enterprise portal. Actions of family member accounts or sponsored accounts are reported to their AKO account sponsor. The sponsor determines whether or not that account should be immediately terminated, after the initial warning that the account holder disregarded the enterprise portal rules and guidelines. 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 pay band equivalent, may request the restriction, suspension, or termination of the enterprise portal user privileges. Requests for restriction, suspension, or termination of the user’s privileges should be considered after legal review, and the command has reason to believe that:

1. Continued use of enterprise portal may hinder organizational operations (see AR 25–2).

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

3. The user has violated the terms of service and/or terms of use guidance or associated procedures, policies, or regulations.

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

(b) Reactivation of the account requires a memorandum to the account suspension officer from a commander or activity director, in the grade of lieutenant colonel or above, or pay band equivalent, stating the user has been counseled and requesting the account be reactivated.

(2) The establishment of multiple accounts will be granted to individuals with multiple roles that must be separate for legal or administrative purposes, such as a Reservist who is also a contractor or a retiree who is also a contractor. These individuals will have multiple unique addresses.

(a) A multiple-role user will have a unique enterprise email address for each role (persona). For example, an individual who is both a contractor and a Reservist would have the following two enterprise email accounts: john.a.doe35.ctr@mail.mil and john.a.doe35.mil@mail.mil.

(b) Email users with two accounts, such as contractor/government or contractor/retiree, will use the appropriate account when sending e-mails. Users with two accounts will authenticate using the personal identity verification authentication certificate on their CAC(s).

(3) The use of group accounts is generally unavailable. Exceptions may be granted by the designated approval authority (DAA) within the enterprise portal 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.

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

i. The following apply to deleted or inactive enterprise portal accounts:

(1) Orphaned accounts are still active in the directory, but the requirements for an individual to access the account are no longer met. This includes an individual who leaves the Army, ARNG, or USAR 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 to inactivate contractor-sponsored accounts, upon expiration of contracts for security purposes.

(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 the enterprise portal. An email notification is sent to the account holder and sponsor that the account will be deactivated in five business days, if not used. Account holders are able to reactivate the account by resetting their passwords. Full and family member 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 enterprise portal 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 members separating from active duty (regardless of type of discharge) will be made inactive the day the individual has completed outprocessing. It is the role of the system or network administrator in each unit to ensure this occurs.

(5) The enterprise portal account information of a deceased Soldier is not considered "personal effects." The enterprise portal records are properly classified as "government" records. Requests for enterprise portal information must be processed under the Freedom of Information Act (FOIA) procedures. The Casualty Affairs Officers may advise Family members seeking enterprise portal 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) Requests from the AKO program officer to print out 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.

(6) There is no requirement to get a new CAC, unless the CAC is expiring. Expired CACs require new certificates.

3–3. User assistance

a. Enterprise portal user assistance is accessible from the AKO homepage via the "Help" link. The Help function includes training materials, frequently asked questions, user guide, and provides feedback.

b. In addition to using the AKO homepage, users may telephone or email the help desk 24 hours, 7 days a week at +1- (866) 335–2769, or email help@us.army.mil.

3–4. Content management

a. Content management as an enterprise service. The amount of data and information stored on Army systems has grown exponentially over the last ten years. Currently information is stored across multiple systems, including AKO, shared drives, collaboration platforms, and individual devices (mobile, desktop). Enterprise Content Management is undergoing a transformation to improve data and information transparency, consistency, and availability. Content management will enable Soldiers and business users to execute their mission knowing their content is stored and managed in full compliance with legal and policy requirements, on any trusted device, anywhere in the world. The details below describe how to manage content using the tools available today. This information will be updated as new services and capabilities are delivered.

b. Enterprise portal content management. The AKO portal has a broad range of content that includes resident and linked content objects. The primary AKO content repository is the folder which allows the user, community or team to create folders or personal team areas available from any Internet connection. This repository allows the user, based on the type of user account, 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.

c. Roles within the folder. 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 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 folders and personal team sites and control the following permissions: the ability to delete 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 a user with access to a folder and permission to download and upload files.

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

d. 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 folders or 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.

e. Advanced content management capabilities. Users with extensive information needs can use the folder'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 folder 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) Archiving, by providing authorized users a direct link to Army Records Information Management System for archiving documents contained in the folder.

3–5. Collaborative environment

a. Services and capabilities. AKO provides synchronous and asynchronous services and capabilities:

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

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

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

(4) Member lists.

(5) Sharing and storage of content and documents through folders and their related files.

(6) Self-service links.

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

b. Site creation. AKO provides multiple types of sites that can be used to present information to an audience. Each type of site is designed to give the site creator the most common elements used by that type of group (team, community, organization). These can be changed as the site is edited. To create a site, go to the quick links menu and select create a site.

(1) 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 enterprise collaborative environment, organizational sites are based on the official Army hierarchy and can be cascaded from the ACOM or HQDA-level down to individual units and divisions. Commanders also have the flexibility to grant varying levels of access by establishing areas targeted to all AKO users and limiting areas to internal organizational groups.

(2) 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 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 and/or project related products.

(3) Individual work sites. Individual work sites increase personal productivity by empowering all Army personnel with the ability to create a personalized site on the enterprise portal that centralizes the services and content required to accomplish everyday tasks and missions.

(4) 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 enterprise portal 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:

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

(b) Communities of interest (COIs) (see DOD CIO memorandum, DOD Net-Centric Data Strategy, and AR 25–1 for definition).

(c) Communities of purpose, similar to a community of practice, except that the community is gathered and exists for a shorter duration of time, usually to expedite the research, discussion and agreement on options for a solution to an important short-term problem or challenge.

(d) Structured professional forums, a community of practice subtype, employed by the Center for Army Lessons Learned to support practice areas and functions within the leader development and training domain (see glossary for definition).

c. Knowledge networks. Knowledge networks provide an official Army organization with the ability to aggregate and organize into a cohesive whole 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 enterprise portal sites and services with the integration through SSO of additional function specific applications and services (see table 3–2).

Table 3–2.
Collaborative Web sites

Type	Subtype	Mission	Sponsorship
Enterprise portal homepage		Army Sr. leadership communication to portal users	Chief of Staff, Army office
Organizational sites	ACOM/functional	Functional/ACOM leadership communication	ACOM/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 within 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

3–6. Requirements and functional configuration management

a. The AKO requirements management process is the authoritative means for all AKO users to provide constructive feedback directly to the AKO personnel. The process is initiated by users via the AKO "Tell CPT AKO" button located on the list of buttons on the left side of the home page. By utilizing the feedback button, AKO users contribute to the development and implementation of new functionality on AKO. Users should submit new functional change requests solely via the feedback button, as it expedites the review and evaluation process.

b. Additional information for the AKO enterprise portal policies and procedures is located at: https://www.us.army.mil/suite/page/278081.

3–7. Joint capabilities

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

b. Global information grid. The GIG enterprise services, consisting of hardware, software, policy, processes, and procedures, provide 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 enterprise services enable DOD information and decision superiority from the command center to the Warfighter.

(5) The Enterprise Services program is a joint IM/IT effort administered by OSD and managed by the DISA. This program provides core enterprise services in the form of Web services and in a service-oriented architecture. Enterprise Services program details and information about core enterprise services may be found on the Enterprise Services portal (http://www.disa.mil/Services/Enterprise-Services) using a common access card or DOD PKI certificate for access.

c. Enterprise services management and network operations. This set of services provides end-to-end GIG performance monitoring, configuration management and problem detection and/or resolution, as well as enterprise IT resource accounting and addressing 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, LWN/MC mission areas and domains, and COIs will leverage core enterprise services 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 email, 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, online meetings, and work group software.

(5) Applications — the infrastructure that hosts and organizes distributed online 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.

Section II
Army Public Web Site Management

3–8. 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 an enterprise portal, such as AKO or other approved private Web site.

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.

(5) 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.

d. Restricted information. Army organizations using the Internet will not post the following types of information on Army's publicly accessible Web sites:

(1) FOIA-exempt information (see AR 25–55).

(2) Records currently and properly classified in the interest of national security.

(3) Records related solely to internal personnel rules and practices that are not meant for public release.

(4) Restricted or limited distribution information.

(5) Records protected by another law that specifically exempts the information from public release. This includes information protected by copyright.

(6) Trade secrets and commercial or financial information obtained from a private source which would cause substantial competitive harm to the source if disclosed.

(7) Internal records that are deliberative in nature and are part of the decisionmaking process that contain opinions and recommendations. This exemption includes draft documents, draft publications, or pre-decisional information of any kind.

(8) Records which, if released, would result in a clearly unwarranted invasion of personal privacy.

(9) Lists of names and other personally identifying information of personnel assigned within a particular component, unit, organization, or office in the DA. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties-such as general officers and senior executives, public affairs officers, or other personnel designated as official command spokespersons-is permitted. In addition, command Web sites may publish the name, rank, and duty station of military personnel in photo captions and news stories. Point of contact information on posted memoranda is also excluded from this restriction.

(10) Investigatory records or information compiled for law enforcement purposes.

(11) Web logs (blogs), video logs (vlogs), or chat rooms.

(12) 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 above and in AR 25–1. 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.

e. 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–PRG.

f. 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.

g. Registration. Information regarding site registration is available at www.us.army.mil/suite/page/600053/.

(1) Army Internet registration is a part of the mission of the CONUS–TNOSC. CONUS–TNOSC is part of NETCOM. NETCOM supports Army installations needing to apply for IP addresses via the non-secure Internet protocol router network (NIPRNET) and SIPRNET.

(2) NEC 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/.

h. Web records administration. Web records must be managed per OMB Circular A–130 and guidance from the National Archives and Records Administration (see Parts 1220–1238, Title 36, Code of Federal Regulations (36 CFR 1220–1238) and www.archives.gov/records_management/index.html/).

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

j. 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.

k. 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.

l. Web site linking. The linking policy found on FirstGov.gov is suggested as an example for Army public Web site linking policies. 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. Hyperlinks to Web resources, other than official U.S. Government Web resources, are permitted only if the organization’s mission requires them.

(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. The 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.

m. 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 and/or maintainers should include a statement such as, "Last updated on __" or a date stamp to each page altered or reviewed.

n. Social media sites. All social networking sites (SNS) and social media sites must register with www.army.mil/socialmedia/. Social media sites are a sub-category of Web sites and all Web site operations security and maintenance rules apply. Guidance on how to set up and manage an organization's SNS or social media presence can be found at http://www.defense.gov/socialmedia/. External official presences should be established in accordance with the best practices and guidance provided by the Office of the Chief of Public Affairs. This can be found in The United States Army Social Media Handbook and other documents at http://www.slideshare.net/USArmySocialMedia/.

o. 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).

3–9. 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.

c. Content organization. Information should be organized by subject and/or 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 they need and want 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 and/or 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 email address or Web-based contact (for example xxxwebmaster@us.army.mil/)).

(d) The organization's policy and procedures for responding to email 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, and/or 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, USAR, ARNG, ACOMs), 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 email addresses, phone number, office, name, or position.

(e) Information about jobs at the organization. The preferred method is to link to Civilian Personnel Online (https://acpol.army.mil/ako/cpolmain/).

(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.

3–10. 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 AR 25–1).

b. Public Web site requirements. Public Web sites must be developed, according to the following guidelines:

(1) Web master and/or 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 must include a link to an accessibility policy that describes compliance with the Rehabilitation Act of 1973 (amended 1998).

(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 are 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 and/or 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 five 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 and/or 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. Web masters and/or 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.

3–11. 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.

b. Training. All individuals appointed to be Web masters and/or maintainers, reviewers, and content managers must complete training and certification, as necessary, equal to the duties assigned to them. All IA support staff will maintain their certification status within the Army Training and Certification Tracking System database. Web-based training is available at AKO (https://iatraining.us.army.mil). Web Content and Operations Security Certification courses are mandatory for all Web masters and/or maintainers.

3–12. 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). Subordinate elements of a major command should provide links back to the respective major command and the Army Home Page.

d. USA.gov link. Major organizational home pages (Army Home Page, ACOMs, HQDA staff elements) should link to the USA.gov home page (www.usa.gov) with the entry: "USA.gov: U.S. Government Web Portal."

3–13. Federal law, regulation, and policy compliance

a. Army public Web sites must comply with applicable Federal law, regulations, and policies, including DODI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."

b. Refer to AR 25–1 for official and authorized use of Government communications and prohibited usage and for Army Web policy. Refer to www.defenselink.mil/webmasters for DOD policy and guidance and http://www.usa.gov/webcontent/index.shtml for additional guidance.

3–14. Network Enterprise Center Web site administration

a. NEC functions. NECs 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 Internet service provider (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 NEC or designee contacts the supervising Web site owner to move 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. See AR 25–2.

b. Procedures. NECs 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 NEC control are 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 and/or maintenance.

(14) A feedback mechanism for users' comments, in accordance with the Paperwork Reduction Act.

(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 the Army Web Risk Assessment Cell (AWRAC) for notification of a violation. NECs will ensure that Web sites' links are disconnected, until corrections have been completed.

(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 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 hertz and lower than 55 hertz.

(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 of 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. The AWRAC reviews the content of Army publicly accessible Web sites (.mil and all other domains used for communicating official information, including SNS) 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 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, Government Information Locator Service registration).

(4) Notifies the Web site owner with operational authority and the Information Assurance program managers of respective command and/or activity of violations and suspense dates for reporting corrective action.

(5) As required, reports deficiencies and corrections to the Army CIO/G–6 and Joint Web Risk Assessment Cell.

d. System security considerations.

(1) Each organization will establish information system security certification and accreditation procedures, in accordance with DODI 8510.01, DOD Directive (DODD) 8570.01 and AR 25–2.

(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 personnel certified in accordance with DODI 8510.01, DODD 8570.01 and AR 25–2. 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. For additional information on risk assessment, see NIST Special Publication 800–100.

(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 Processing Standards (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) Employing 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).

3–15. Collaboration capabilities

a. Collaboration capabilities are necessary to enable two or more individuals who are not co-located to use an electronic synchronous or asynchronous environment to communicate, plan, coordinate and make decisions to achieve an objective. The procedures for the acquisition and implementation of Army collaboration capabilities to be deployed on the Army enterprise network, local enclaves, or domain level apply to active Army, ARNG, the Army Reserve, Army Civilians and applicable Army support contractors, and those organizations operating under contract to the Army.

b. The collaboration procedure includes:

(1) Army commands will submit their collaboration requirements to the CIO/G–6, SAIS–PRU through their core enterprise services domain representative.

(2) CIO/G–6, SAIS–PRU will review the requirements and determine if the requirements are met by DOD Enterprise Services capabilities, AKO or an existing product on the Approved Products List (APL). If the requirement is met by DOD Enterprise Services, AKO, or the APL, the request will be disapproved and returned back to the core enterprise services domain representative.

(3) Army commands and developers requesting collaboration tools or services which are not on the APL are required to follow the guidance set forth in the Networthiness Implementation Program. They are also required to insure that the product has been certified and accredited.

(a) The Networthiness Certification Program is managed by NETCOM. For additional information on the Networthiness Certification Program, see paragraph 7–2, Network Operations, within this pamphlet.

(b) Certification and accreditation (C&A) is independent of Networthiness and is required before the Networthiness process can be finalized. Army commands are required to obtain IA C&A per DODI 8510.01, DODI 8500.01, and AR 25–2.

(4) Once the DAA approves the authority to operate and Networthiness issues a Certification of Networthiness, the CIO/G–6, Policy and Resources, Director will issue a letter for inclusion on the APL for collaboration tools.

(5) Following approval:

(a) The collaboration tool or service is linked to AKO through SSO. AKO provides the only authoritative Army enterprise directory and the ability to manage identities, profiles and key information at the enterprise level. Information and instructions on executing AKO SSO, including forms and technical platform requirements, are available on AKO. Linking to AKO through SSO does not apply to hardened tactical systems that exchange information or capabilities being deployed in bandwidth-constrained tactical environments. For collaboration capabilities already in place for which there is no current technical solution to enable SSO, a waiver, to include a migration plan, must be obtained from the CIO/G–6, SAIS–PRU.

(b) The APMS requires that collaboration tools acquire Government funding immediately after being registered in APMS. The APMS system is the Army's authoritative inventory for all IT systems and collaboration tools at the unclassified collateral level. Collaboration tools that will be used in the classified environment may be registered only if classified data is not disclosed. Once the collaboration tool is registered in the APMS system, it is incumbent on the perspective organization and/or system owner to execute continual data maintenance, data accuracy and data completeness of the IT system.

c. For more information on collaboration capabilities, see the Implementation of Collaboration Tools and Service site on AKO.

Chapter 4
Information and Security Management

Section I
Data Management

4–1. Army Data Management Program

a. The Army Data Management Program (ADMP) establishes required policies and procedures for the production of data standards to ensure enterprise-wide machine processability of Army information resources and interoperability for all pertinent data exchanges among Army information systems. The ADMP addresses the creation and implementation of data standards applicable to automated systems, software applications, data exchanges, databases, enterprise infrastructure, record and document management, and information presentation within and across warfighting and business systems. For Army Data Board structure, positions, responsibilities, and other information, see AR 25–1 and http://architecture.army.mil/.

b. The ADMP facilitates the dissemination and exchange of information among organizations and information systems throughout the Army, DOD, and the Federal Government. The ADMP implements the information standards portion of the DOD IT standards registry (DISR) and supplements the DOD Net-Centric Data Strategy. Net-centricity is dependent upon the ability to locate and retrieve information and services, regardless of where they are stored. A common data management strategy is essential to allowing authorized users to access required information. (See DODI 8320.02 for information sharing restrictions.)

c. Army data focus areas include:

(1) Making data visible by creating discovery metadata and deploying discovery capabilities that catalog information assets for users to find. Refer to AR 25–1 for information on Army data standards management.

(2) Making data accessible by offering data assets over the network through commonly supported access methods (for example, data services layer – Army, AKO, Intellipedia, Intelligence Community Content Discovery and Retrieval, and the DISA provided GIG content delivery service) and providing access to the underlying information, so that authorized users can make use of it.

(3) Making data understandable by reaching an agreement on the meaning of information provided by data assets and making that understanding available to consumers through the DOD Metadata Registry (MDR). Refer to the sections below in this chapter and AR 25–1 for information on Army data standards management, including Army support of the DOD MDR.

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

e. The ADMP facilitates internal, Joint, and combined interoperability through the standardization and use of common data standards.

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

g. The ADMP improves data quality and accuracy and minimizes the cost of data production and data maintenance.

h. The ADMP applies to any information system passing information through Army networks and/or Army IT assets in the net-centric information environment.

i. All data will be protected per AR 25–2 and AR 380–5. Specifically:

(1) Data security classification, such as the Intelligence Community Information Security Markings, will be identified and maintained as part of the data standards documentation if independent of specific use.

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

j. The ADMP ensures that as the Army is transforming to maintain and increase its information superiority, information will flow to those who need it in real time to empower not only the commanders and decision-makers, but also individual Warfighters and civilians. Specifically, the ADMP supports the vision of enterprise-wide information accessibility by facilitating the transition from an environment of information stovepipes to one of data sharing via a paradigm shift in data "ownership": from "need to know" to "need to share responsibility." To that effect, the Army will:

(1) Create a data-enabled environment and support the infrastructure that allows access to enriched data in a timely and secure manner, regardless of operational environment.

(2) Ensure that data owners expose (that is, make visible and accessible) to the Army enterprise the authoritative data assets under their control, except where limited by law, policy or security classification.

k. The ADMP ensures that data exchange metadata, for example, Web services description language (WSDL), schemas, Extensible Stylesheet Language Transformations, will be validated for conformance to applicable standards and will be registered in the DOD MDR, DOD Enterprise Authoritative Data Source Registry, and the Enterprise Services Registry, as applicable.

l. The ADMP ensures that data architectures from the mission area (segment) and domain (sub-segment) leads, system owners, PEOs, and PMs will comply with Army and DOD data requirements by developing and maintaining data performance plan (DPP) artifacts in a DPP system environment wherein the standards, policies, procedures, data models, and business rules reside and are employed as appropriate. Refer to AR 25–1 for additional policy related information.

m. ADMP data quality practices promote efficient use of resources and data management practices by eliminating duplication, improving synchronization, and reducing software development costs.

4–2. Army Data Management Program net-centric data strategy

a. Purpose and scope. The purpose of the ADMP 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 ADMP. This chapter gives guidance and procedures about ADMP policy. The procedures contained in this chapter apply to all Army organizations and programs that manage data and address the engineering of the ADMP, the identification and planning of ADMP projects, and the accomplishment of ADMP 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.

(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 (such as, the DOD Enterprise Catalog) that is visible to the enterprise, and the data is 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.

c. Information architecture guidance. The COE Army Information Architecture (AIA) provides the foundation to accelerate Army transformation to net-centric information sharing. The AIA augments and extends the DOD Information Enterprise Architecture by identifying Army-additional principles, business rules, and processes that govern IT development. The AIA also augments the Army's COE by identifying standards. It provides the guidance and compliance requirements that enable Army stakeholders to envision, design, develop, deploy, and use information systems that are consistent, comprehensive, compatible, and integrated across the Army enterprise and realize the DOD net-centric information sharing vision. The AIA identifies the policy and guidance documents that govern the data-centric information sharing features of system architectures and ensures Army information systems meet the information sharing requirements of the Army enterprise. The DOD Information Enterprise Architecture provides core guidance for the ADMP. For the DOD Information Enterprise Architecture data and services deployment principles and business rules, see http://dodcio.defense.gov/Home/Initiatives/DIEA/dsdprins.aspx.

4–3. Terms and concepts

a. Overview. This section presents a description of the net-centric environment within which the ADMP exists. Standards, data assets, and metadata are basic concepts that constitute the elements of the net-centric data solution. 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 enables effective and timely decisions are the core of the net-centric environment. Here, data implies all data assets such as system files, databases, documents, official electronic records, images, audio files, Web sites, and data access services. One CIO/G–6 goal is to make the data network accessible and shift the paradigm from "process, exploit, and disseminate" to "post before processing." Under this concept, all data is advertised and available for users and applications when and where needed. Users receive alerts when data they have subscribed to is 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.

(3) For guidance on the protection requirements and accessibility requirements based on the type of data, see AR 25–1.

c. Standards.

(1) AR 25–1 identifies four Army data standards vital to implementing the data goals: authoritative data sources (ADS), unique identifiers (UID), information exchange standard specifications (IESS) and eXtensible markup language (XML). An ADS is a recognized or official data production source with a designated mission statement or source and/ or product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources. DODI 8320.02 directs all Services to register their ADSs in the Enterprise Authoritative Data Source Registry. The Army process to register ADSs is in compliance with this mandate. UID 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 markup 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. 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 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, and rules.

(3) Reuse industry-standard information exchange data structures (schemas) where possible.

(a) If an industry-standard schema is not suitable, reuse COI-managed schemas associated with Web services deployed by the appropriate ADS.

(b) If a COI-managed schema is not suitable, reuse the National Information Exchange Model schemas for reuse.

(c) If no existing suitable schema(s) exist, leverage the National Information Exchange Model naming and design rules and data structures to create new schemas. Validate the final message structure with Conformance Testing Assistant.

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 UID, so that UID-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 and/ or registered with a proper MDR; registered in an enterprise searchable catalog; understandable; and accessible to the widest possible community.

(7) Data assets also include big data. As technology advances over time, it is expected that the size of datasets (big data) will also increase. This will impact hardware and software by mission areas and echelon, depending on what kinds of tools are available and the sizes of datasets common to supporting a particular decision-maker's need. Big data in many sectors today ranges from a few dozen terabytes to multiple petabytes. Data aggregation and analysis are becoming increasingly valuable with the result that data generators are adding those capabilities to more fully realize potential value. As an ever larger amount of data is digitized and travels across organizational boundaries, there is a set of policy issues that will become increasingly important, including, privacy, security, intellectual property, and liability.

e. Data performance plan.

(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 DOD Architecture Framework (DODAF) views or may exist implicitly within DODAF views. 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, for instance, constitutes metadata. Types of metadata include:

(a) Structural metadata are the physical characteristics of the data; such as datatype (varchar, date, integer, number, and so forth) field length, precision (where the decimal point goes), and so forth.

(b) Semantic metadata are the definition of the data element, logical name, physical name, and known aliases.

(c) Content-related metadata are the structural and semantic metadata often associated with the discovery service.

(d) Security metadata are the tags used to identify the needed information security markings for a given instance of data.

(e) Discovery metadata are the tags established to make data visible. The DOD Discovery Metadata Specification provides the minimum required structure and content for discovery related tags.

(2) All the architecture products and/or diagrams in the DODAF must be Unified Profile for DODAF/Ministry of Defence Architecture Framework (UPDM) conformant. The UPDM provides a metadata structure for storing architecture data. All metadata management tools used in architecture product development must be capable of creating UPDM conformant products.

(3) 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.

(4) 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) Data must be both interoperable and understandable to be a value to the users in different domains. According to the DOD Net-Centric Data Strategy, the terms are described as:

(a) Interoperable: Many-to-many exchanges of data occur between systems, through interfaces that are sometimes predefined or sometimes unanticipated. Metadata is available to allow mediation or translation of data between interfaces, as needed.

(b) Understandable: Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.

(2) The data aspects of interoperability may be summarized by the term data 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.

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

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

(5) 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.

(6) The role of IESS is to specify the physical data format and semantics of the data used to convey information between information systems. Rules for the use of IESSs are specified in Rules for Cross-Cutting Capability Information Exchange Specifications in Interface Specifications.

(7) Finally, XML is valuable for taking content from one system and sharing via file sharing or Web service techniques. Embedded within the XML stream are the UID 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. Accordingly, it is desirable for the IESS to include a logical data model that represents the COI's shared vocabulary. 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 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).

h. Community of interest.

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

(2) The COI structure consists of three layers. The first layer is the Chief Data Officer (CDO) Construct consisting of the Army Data Board and Army Data Counsel. The CDO Construct establishes the central terms 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 CDO Construct. Whatever data schema an institutional COI develops would have to be conformant (in the ISO 11179 sense) to the common schema(s) 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 is the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. 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), master data management, and data services. DBMSs support the definition, storage, and retrieval of data elements from monolithic and distributed DBMS. Information systems that employ COTS DBMS must conform to the requirements of SQL: 2008, Core.

4–4. 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 Data Board that consists of the CDO, who also functions as the lead data steward, in cooperation with other data stewards, functional data managers, mission area leads, domain leads and COI leads. The following items provide initial guidance on the way ahead for Army Data Management. The primary set of functions is specified in AR 25–1. Additional functions are specified below.

a. Community of interest 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 areas leads. Mission area and COI leads coordinate with the CDO 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 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. Functions of the Army, Chief Data Officer. The CIO/G–6 is the CDO of the Army and is the Army lead for implementing the DOD data sharing policy, 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 and/or Joint body to request formation of that particular COI. If the request is not supported by the DOD and/or 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 and/or 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 priorities, resources, proponency, 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 CDO 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 infrastructures 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 CDO 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 and/or 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 the COI. Each COI creates and maintains the COI's shared vocabulary, shared data spaces, metadata catalogs, IESSs 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 DODAF architecture views 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 Enterprise Services Program, including tagging data assets with discovery metadata and posting data assets to appropriate shared spaces.

(8) Register their data asset products through the Army CDO for posting to the DOD MDR.

(9) Create and maintain a metadata catalog of data assets. All data owners ensure that their data assets are described using the COIs 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 Enterprise Services Program discovery service, in accordance with the DOD Discovery Metadata Specification, 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 UIDs, 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 and/or 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.

f. 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 and/or application to operate in a net-centric environment using Web services and associated protocols (for example, XML, SOAP, UDDI, and WSDL).

g. Additional functions of Army components. During the information management process, Army ACOMs 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 and/or semantic metadata are registered with the DOD MDR.

(8) Develop and use a common vocabulary (derived from an 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 Army data management policy in their function area.

4–5. Layers

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

a. Army Data Management Program layer.

(1) Strategy.

(a) The strategy of the ADMP 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 MDR and harmonized across DOD as appropriate.

(b) The ADMP 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 ADMP 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. ADMP 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 ADMP process projects include the data policies and procedures, the management of data asset product specifications, the management of those products into the DOD MDR, and the ADMP methodology through which all ADMP 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 uses 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 Army data management 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 UID to uniquely identify instances of data assets.

(f) The DPP is a structured approach through which the full set of Army data management 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 ADMP can be understood and completed.

b. Data performance plan layer.

(1) Strategy.

(a) The ADMP applies Army direction for managing COI activities and the development of data asset products. DPP is the term coined by the Army CDO to describe this process. It is the COI program management plan for the development, scheduling, resource management, and evolution and/or migration strategy of the COI systems to the common COI net-centric interoperability solution(s). Programs of record (POR) 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, UIDs, 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 affect 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 stove-piping of data interoperability solutions, data related architecture products must be integrated with the supporting, nondata-related products within the 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 and/or 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. In addition to the required analysis, all DPP projects must conduct a data quality analysis to ensure the system has the required level of quality for its information resources.

(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). Particular attention must be paid to those DPP goals and objectives pertaining to data quality.

(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. As a part of the monitoring of every DPP project, there must be a data governance component that will ensure the proper allocation of responsibilities and rights to the individuals charged with the implementation of the DPP project, so that the data quality goals and objectives are achieved.

(3) Project classes. Army data management projects are accomplished in support of some aspect of the ADMP 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, resources loaded and staffed, and managed during its accomplishment. All deliverables must fit within the overall set of all deliverables from all the other 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 ADMP. Included are the ADMP's overall process, specific standards (such as SQL, XML, 11179 data element metadata), metrics, project management, the Army data standards (such as UID, 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, UID, IESS, XML), and the federated metadata environment (for managing and exposing structural, semantic, and discovery metadata).

(c) DPP infrastructure projects are generally in these areas: metadata management, 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 ADMP 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 ADMP project.

c. The project execution layer.

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

(a) From the ADMP layer, the projects include those related to policy, guidance, the DPP process, explicit and implicit data asset product engineering and specification, 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 UID, development of XML schemas, configuration management, and test of COI interoperability solutions.

Section II
Information and Data Security

4–6. Privacy impact assessment process

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

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

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

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

b. Army system owners and application owners will—

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

(2) Document completion of the assessment using the DD Form 2930 (Privacy Impact Assessment [PIA]). The digital signature portable document format (PDF) version of the DD Form 2930 is required for all PIA submissions. The form is available on the DOD's Web site. Submit all forms to cio-g6.pia.inbox@mail.mil. The CIO/G–6 PIA team will not accept a scanned DD Form 2930. We must have the original form.

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

(4) In order to complete a PIA, DD Form 2930, IT system and/or application owners must adhere to the following steps (refer to http://ciog6.army.mil/Portals/1/PIA/ArmySampleHowToGuideasofJul09.pdf for step-by-step guidance):

(a) Once an IT system and/or application is registered in APMS, a PIA is required. IT system and/or application owners determine if the IT system and/or application collects PII. Systems and/or applications that do not collect PII must still complete a modified version of DD Form 2930. A DITPR number, which will be assigned once the system and/or application is registered, is required in order to submit a PIA. Systems and/or applications that collect PII must determine who they collect PII from (for example, general public, Federal personnel and/or Federal contractors).

(b) When IT system owners submit a PIA for processing, it is required for the IT system to have a valid or be undergoing C&A. If the accreditation renewal package has been accepted by CIO/G–6 Cybersecurity, the CIO/G–6 PIA team can begin processing the PIA.

(c) If the system and/or application does not collect PII, the system/application owner must submit the modified PIA, which requires the IT system and/or application's DITPR number, all accreditation information, and a system description that references APMS and states that no PII is collected. Digital signatures on the first three signature blocks are reserved for the local approving staff: the PM, component or local Information Assurance manager or official, and component or local privacy official signatures. Submit the draft version of the PIA, without digital signatures, to the CIO/G–6 PIA mailbox at cio-g6.pia.inbox@mail.mil/.

(d) All IT systems and/or applications that collect PII must provide the following data within the PIA:

1. What audience the IT system and/or application collects information from. If the IT system and/or application collects information on ten or more people of the public, the system and/or application owner must obtain OMB approval. The OMB control number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period, regardless of form or format (see the Paper Work Reduction Act).

2. Why the PIA is being created or updated (for example, new DOD IT system and/or application, new electronic collection, or major change).

3. The appropriate System of Records Notice (SORN) (refer to http://privacy.defense.gov/notices/army/ for guidance), if necessary. A SORN is required if the IT system and/or application or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other UID.

4. A clear and concise summary and/or description that describes the functions of the IT system and/or application or electronic collection and the types of PII collected. The system and/or application summary or description must match the description in APMS. Also include categories of PII that is collected (for example, personal, financial, medical, education, employment, military record, law enforcement).

5. A brief summary or description of the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

6. Who will have access to PII collected and with whom the PII will be shared throughout data exchange; both within the DOD component and outside the IT system and/or application's component.

7. Whether or not individuals have the option to decline providing PII, if so, how and why, if not.

8. What information is provided to an individual when asked to provide PII data (Privacy Act Statement, Privacy Advisory, other or none).

9. Specifications on the type of PII (a data element alone or in combination that can uniquely identify an individual) collected (for example, date of birth, name, social security number, marital status), the source, collection method, purpose, and intended use of the PII. Any spousal or children information gathered is considered general public information.

10. Who has or will have access to PII in the IT system and/or application or electronic collection.

11. How information will be collected and secured (for example, paper format, fax, and email).

12. Current status and granted date of accreditation.

13. What measures have been put into place or planned to address identified privacy risks.

(e) System and application owners should submit the draft PIA to their PIA point of contact. The draft PIA version without any digital signatures will be forwarded to the CIO/G–6 PIA team for initial review to address any recommended changes. Upon review, the CIO/G–6 PIA team will coordinate with the Army Privacy Office for privacy risk content review and guidance.

(f) Once all required information is correctly entered into the official DD Form 2930, the PIA team will request for IT system and/or application owners or PIA points of contact to submit the PIA with electronic signatures from the system and/or application owner or program manager, local privacy office official and any other official signature (to be used at component's discretion). All completed forms should be emailed to cio-g6.pia.inbox@mail.mil/.

(g) CIO/G–6 PIA team will provide final review for any edits and submit all completed PIAs to OSD for final approval. All completed PIAs, which collect PII from the general public and/or both the general public and Federal employees or contractors will be posted on http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx.

c. A PIA must be reviewed and updated annually in conjunction with the accreditation. The Army Senior Information Assurance Officer (CIO/G–6, SAIS–CB) will review all PIAs to ensure compliance with Information Assurance policies prior to CIO/G–6 approval.

d. The Office of the Administrative Assistant to the Secretary of the Army will review completed PIAs and confirm compliance with DODD 5400.11 - DOD Privacy Program and ensure SORN issues have been properly identified and evaluated prior to CIO/G–6 approval.

4–7. 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, 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, pre-distribution 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 4–1 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 five 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.

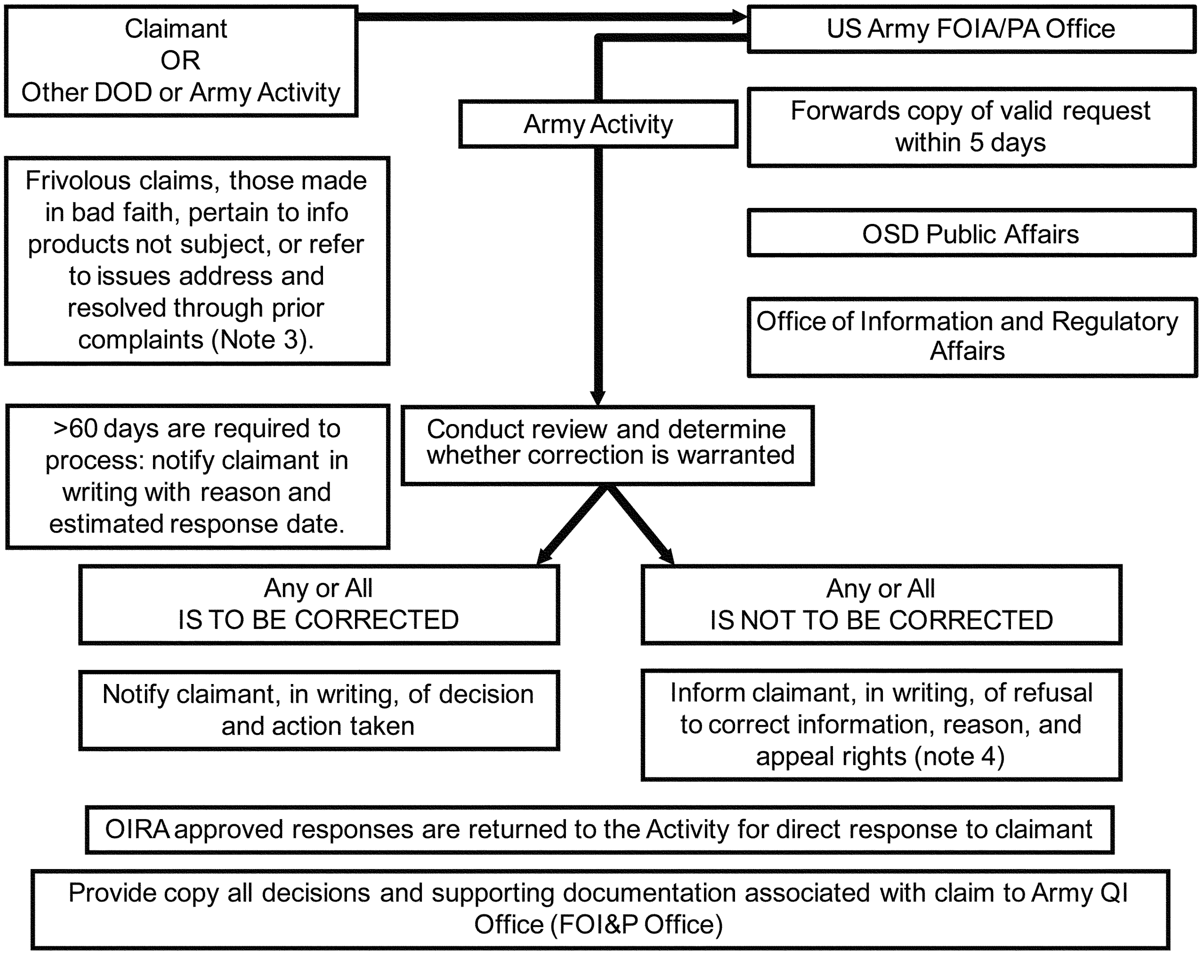

Claimant
OR
Other DOD or Army Activity
US Army FOIA/PA Office
Army Activity
Forwards copy of valid request within 5 days
OSD Public Affairs
Office of Information and Regulatory Affairs
Frivolous claims, those made in bad faith, pertain to info products not subject, or refer to issues address and resolved through prior complaints (Note 3).
>60 days are required to process: notify claimant in writing with reason and estimated response date.
Conduct review and determine whether correction is warranted
Any or All
IS TO BE CORRECTED
Any or All
IS NOT TO BE CORRECTED
Notify claimant, in writing, of decision and action taken
Inform claimant, in writing, of refusal to correct information, reason, and appeal rights (note 4)
OIRA approved responses are returned to the Activity for direct response to claimant
Provide copy all decisions and supporting documentation associated with claim to Army QI Office (FOI&P Office)

Figure 4–1. 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(s) of the information that clearly bears on any determination to correct the information. These guidelines are found at http://www.whitehouse.gov/omb/foia_5cfr1303/, www.apd.army.mil/, and the DA Freedom of Information and Privacy Act Division, https://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 addressed 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 any 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 three 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 seven 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 seven working days, before its intended issuance. The address is: Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th 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, SBU: 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.

Chapter 5
Information Enterprise Architecture Standards and Certification

Section I
Information Enterprise Architecture

5–1. Army Information Enterprise Architecture Development

a. The Army Enterprise Architecture (AEA) is the Army's blueprint to transform its operational visions and required capabilities through an integrated and interoperable set of information systems and National Security Systems (NSS). That blueprint, in turn, informs enterprise-wide network modernization.

b. The AEA is a strategic process that organizational leaders use for enterprise planning, resource investment, management decision-making, and key process executions. As shown in figure 5-1, the Army Information Enterprise Architecture (IEA) is a component of the AEA, and represents the total architecture for the LandWarNet as it supports the Army's warfighting, business, and defense intelligence missions. The IEA consists of the following three types of architecture: Operational, Systems, and Enterprise Architecture. This section describes the architecture development process that will evolve the Army IEA.

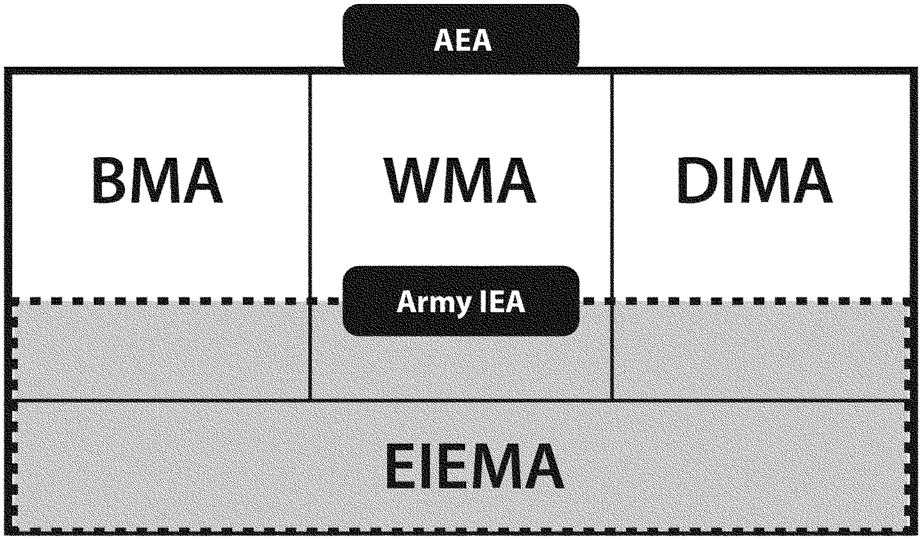


Figure 5–1. LandWarNet mission support represented in the Army Information Enterprise Architecture

5–2. Components of the Army Information Enterprise Architecture

Existing within the Army IEA are three primary architecture types – the IEA Operational Architecture, the IEA Systems Architecture, and the IEA Enterprise Architecture. Together, they depict the complete as-is state, to-be state, and roadmap to evolve the LandWarNet over time. Each of these architecture views (Operational, Systems, and Enterprise) is critical to understanding the totality of the LandWarNet, and must be completely integrated. The information related to the specific content and processes associated with each architecture at the DOD level is found in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H; DOD Architecture Framework (ver2.0), 28 May 2009; and DOD Reference Architecture Description, June 2010. Relevant Army guidance can be found within AR 71–9, AR 70–1, and AR 25–1.

a. IEA Operational Architecture.

(1) The IEA Operational Architecture answers the question "What does the Army do?" It describes the functions, tasks, activities, capabilities, and information exchanges required to accomplish or support Army warfighting, business and intelligence missions.

(2) The IEA Operational Architecture is led by TRADOC and provides a description of today's Army warfighter and business processes and how they will evolve over time. The IEA Operational Architecture potentially contains IT and non-IT functions (as derived from one or more Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities - Policy solutions). In each instance, the respective Mission Area lead for the Warfighter Mission Area, Business Mission Area, Defense Intelligence Mission Area, and Enterprise Information Environment Mission Area

(EIEMA) will provide oversight and prioritization of the Army's IEA Operational Architecture and requirements development, and use the capability-set framework strategy for enterprise architecture and required capability implementation and integration.

b. IEA Systems Architecture.

(1) The IEA Systems Architecture answers the question "What materiel solutions will reside on the LandWarNet?" It describes the IT materiel solutions that make up the LandWarNet and identifies the interconnections providing for, or supporting, Army mission and functions, with a focus on specific physical systems with specific geographical locations. It is constructed to satisfy operational requirements within the standards defined in the IEA Enterprise Architecture.

(2) The IEA Systems Architecture is led by Assistant Secretary of the Army (Acquisition, Logistics, Technology) (ASA (ALT)) and represents the individual solutions and services that comprise LandWarNet. These architectures are at the solution and systems layers, and are detailed enough to support system acquisition and integration. Information related to the specific content and processes associated with Systems Architecture is found in AR 70–1 and its associated DOD and Army reference documents.

c. IEA Enterprise Architecture.

(1) The IEA Enterprise Architecture answers the question "What are the architectural characteristics and technical standards that LandWarNet systems must adhere to?" It enables senior leaders at the point of decision, and guides system developers at the point of implementation. The IEA Enterprise Architecture describes the technical guidance, policy, constraints, forecasts, standards, implementation conventions, business rules, and criteria that govern the Army IEA. It sets the rules for the arrangement, interaction, and interdependence of systems, parts, and elements across the Army IEA.

(2) Figure 5–2 summarizes the HQDA organizations responsible for developing and maintaining the different architecture types within the IEA. Mission area leads, as determined in AR 25–1, remain responsible for providing oversight for the prioritization, development, synchronization, and approval of these architectures.

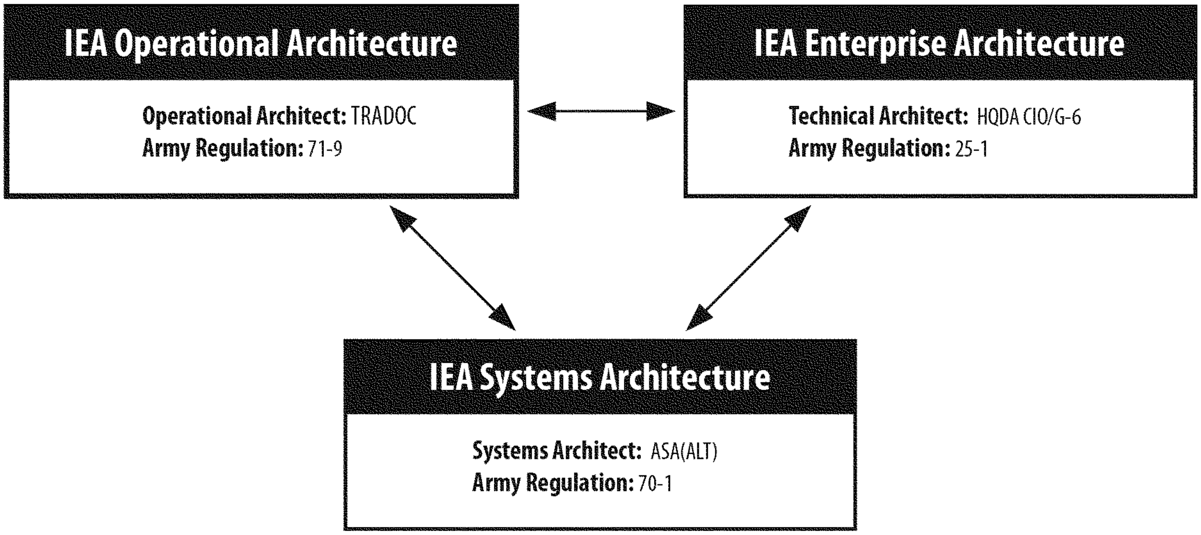

IEA Operational Architecture
Operational Architect: TRADOC
Army Regulation: 71-9
IEA Enterprise Architecture
Technical Architect: HQDA CIO/G-6
Army Regulation: 25-1
IEA Systems Architecture
Systems Architect: ASA(ALT)
Army Regulation: 70-1

Figure 5–2. Components of the Army Information Enterprise Architecture

(3) The IEA Enterprise Architecture is led by the Army CIO/G–6. It translates the Army Network Strategy (ANS) and other driving documents into a roadmap that provides a minimal set of rules governing the arrangement, interaction, and interdependence of network components to ensure that a conformant system satisfies a specified set of requirements. The IEA Enterprise Architecture, as shown in figure 5–3, is captured in three architectures – the LandWarNet Enterprise Architecture, the Network Capability Set (NCS) Reference Architecture, and the Enterprise Reference Architecture. Figure 5–3 shows the relationship and flow of information between the IEA Enterprise Architecture products. The following sections describe the development process, information flow, and governance in more detail.

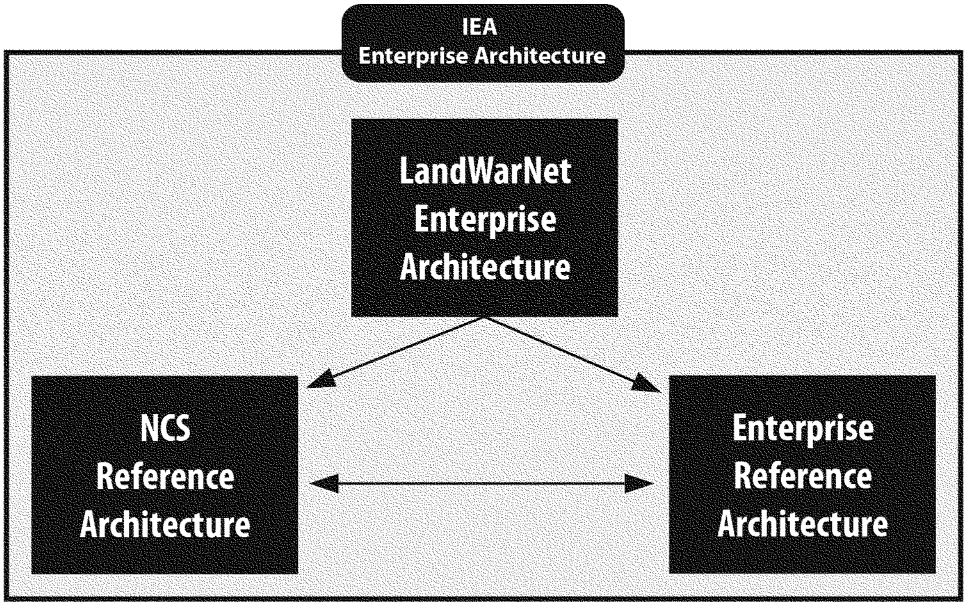

IEA
Enterprise Architecture
LandWarNet Enterprise Architecture
NCS Reference Architecture
Enterprise Reference Architecture

Figure 5–3. Primary architecture products in the Army Information Enterprise Architecture

5–3. Information Enterprise Architecture overview

a. The IEA Enterprise Architecture is performance and outcomes driven (for example, improving the Army's mission performance; saving money and avoiding costs; enhancing the quality of the Army's investment portfolio; and improving the quality, availability, and sharing of data and information). The CIO/G–6's Army Architecture Integration Center (AAIC) in coordination with Office of Business Transformation (OBT); ASA (ALT); DCS, G–3/5/7; DCS, G–2; and TRADOC will oversee execution of the IEA through the Army Enterprise Network Council (AENC), an existing, structured governance & decision-making forum. This executive-level body will be supported by action officer and colonel-level forums charged with vetting and elevating architecture and architecture management related issues to the executive body for decision. As IEA Enterprise Architecture artifacts are developed and published, they will be lifecycle and configuration managed by the Architecture Configuration Control Team (ACCT).

b. IEA Enterprise Architecture Development Process.

(1) Aspects of the architecture development process are being continually executed, driven by asynchronous factors such as the validation of Army warfighting and business requirements through the Joint Capabilities Integration and Development System and Business Capability Lifecycle processes, respectively; the maturation of IT technologies; and the emergence of new technical standards and best practices. The architecture products generated within this process are updated and revised as necessary.

(2) The architecture development process is synchronized with the Army PPBE timeline to provide three primary information elements—

(a) A current LandWarNet baseline to inform Army IT planning activities.

(b) A future-state architecture that enables the AENC to make IT planning and investment decisions.

(c) A roadmap for IT portfolio leads to consider when making IT investment decisions.

c. The input to the Army IEA development process is one or more validated IT requirements that must be satisfied. It is important to note that IT requirements, similar to architectures, exist at the strategic, operational, and tactical levels. The generation and validation of IT requirements and the extraction of IT requirements from Army warfighting and business requirements are outside the scope of this Pamphlet. Figure 5–4 identifies the high-level IEA Enterprise Architecture product development process. The full processes can be found at: https://cadie.tradoc.army.mil/CIO–G6_20Architecture/SitePages/Home.aspx.

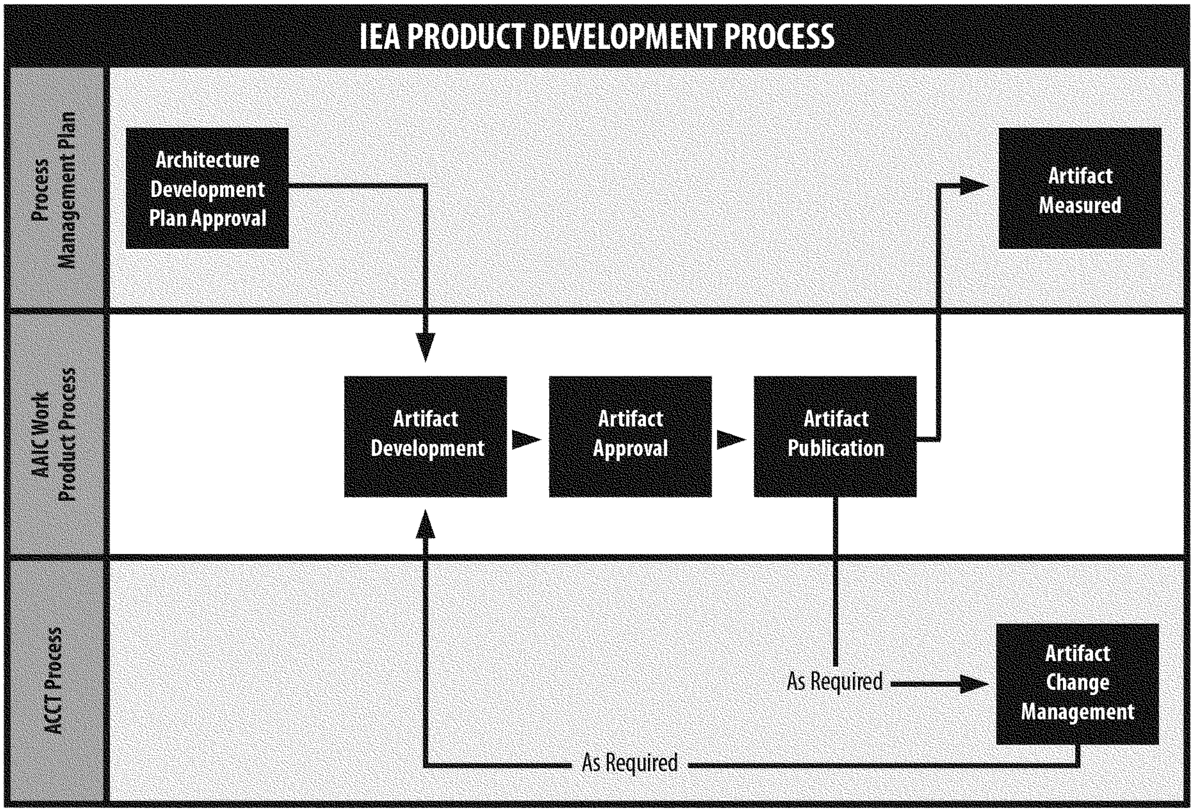


Figure 5–4. Information Enterprise Architecture product development process

d. Although not strictly a part of the AEA development process, there are other documents that significantly influence the generation of architecture decisions and products. The documents describe the Army's intended LandWarNet outcomes and capabilities and the constraints required for possible solutions. Key driving documents include:

(1) ANS.

(2) Mission Area Requirements Specifications.

(3) Domain Functional Architectures.

(4) Army Operational Architectures.

(5) DOD Joint Information Environment (JIE) Architectures.

(6) DOD Technical Standards (DOD IT Standards Registry).

(7) Army Enterprise Reference Architectures, including the NCS Reference Architecture.

e. IEA Enterprise Architecture artifacts are a design-focused translation of AENC decisions. As supporting documents to the Army Network Campaign Plan (ANCP), they provide strategic-level guidance on how the LandWarNet, as an Army asset that supports all Mission Areas, will be designed and configured to meet the "ends" in the strategy. It is aligned with the DOD IEA in order to provide traceability and alignment with the emerging JIE.

(1) Overview.

(a) Scope: LandWarNet as covered by the Army IEA.

(b) Level of Abstraction: Strategic.

(c) Timeframe: Targeted to be realized within seven to 10 years (document will specify).

(2) Roles and Responsibilities.

(a) Approval: Director, AAIC.

(b) Lead: AAIC.

(c) Assist(s): Operational Architects – OBT; DCS, G–3/5/7; and DCS, G–2 provide information and support to ensure the Enterprise Architecture addresses strategic-level functional requirements for the LandWarNet. Systems

Architects – ASA (ALT) provides strategic-level information related to technology trends and implementation strategies.

(3) The Enterprise Architecture evaluation criteria—

(a) Is revised in concert with changes to the ANS and/or with significant changes in IT requirements or technologies.

(b) Satisfies the ANS.

(c) Captures all CIO/G–6 architecture guidance and direction regarding LandWarNet.

(d) Is sufficiently detailed to support the evaluation of potential IT investments and architecture options for their alignment with the ANS.

(e) Accurately conveys CIO/G–6 architecture guidance and direction regarding LandWarNet to stakeholders.

(f) Accurately conveys Army and DOD technical standards that are applicable to LandWarNet in the desired timeframe.

f. The NCS Reference Architecture applies architecture guidance from the Enterprise Architecture to the capability investment priorities documented in the LandWarNet Network Roadmap. Specifically, it sets architecture guidance that drives the design of future NCS for each fiscal year. It is the architectural roadmap to understand how the LandWarNet will transform from its current state to its future state.

(1) Overview.

(a) Scope: EIEMA.

(b) Level of Abstraction: Operational.

(c) Timeframe: Targeted to be realized within two to five years (document will specify).

(2) Roles and responsibilities.

(a) Approval: Director, AAIC.

(b) Lead: AAIC.

(c) Assists: EIEMA Domain Leads – Domain Leads and subordinate Capability Managers ensure the EIEMA investment priorities and capability relationships and timelines are accurately captured and understood.

(3) The NCS Reference Architecture evaluation criteria—

(a) Is revised and updated with the AENC's publication of the annual LandWarNet Network Roadmap, known as the ANCP – Mid Term.

(b) Captures and accurately describes all of the capabilities identified in the LandWarNet Network Roadmap, known as the ANCP – Mid Term.

(c) Aligns with the architecture characteristics identified in the Enterprise Architecture.

(d) Is sufficiently detailed to inform ASA (ALT) System of Systems Engineering & Integration of information necessary to plan and design the NCS, to include - but not limited to - capability descriptions, relationship maps, and installation and organization prioritization.

(e) Provides references to technical standards and other technical requirements that must be met to satisfy network requirements.

(f) Provides information related to the alignment of Institutional and Operational Capability Sets.

g. Enterprise Reference Architectures provide timely architectural guidance that is applied to, and supports, a business objective of the Army. The IEA Enterprise Reference Architectures will follow a rules-based methodology that organizes architecture data around operational and system rules to solve a specific problem set or enable a specific capability. The Enterprise Reference Architectures incrementally provide architecture data with the intent of codifying the LandWarNet strategy and AENC position and intent. The rules-based approach produces architecture information that is clear and understandable, and enables accurate and relevant policy, investment, and acquisition decisions. The intent of this approach is to guide and synchronize Army investment and acquisition decisions, enable the standardization of LandWarNet materiel solutions, and translate Army Enterprise Network (AEN) decisions that inform, and are informed by, NCSs for a given timeframe to enable network modernization.

(1) Overview.

(a) Scope: Includes all rules-based architecture development efforts within the Army CIO/G–6. This includes, but is not limited to, all architecture development efforts under the programmatic oversight of the director AAIC.

(b) Level of Abstraction: Strategic, Operational, and Tactical.

(c) Timeframe: Targeted to be realized within two to five years (document will specify).

(2) Roles and Responsibilities.

(a) Approval: Director, AAIC.

(b) Lead: AAIC.

(c) Assist(s): Operational Architects – provide guidance, direction, and clarification regarding intended capabilities and capability relationships. System Architects – provide guidance, direction, and clarification regarding expected system fielding schedules and represent implementable solutions. DOD and Army partners including, but not limited

to, DISA, Second Army, ASA (ALT), and Intelligence and Security Command ensure technical and engineering guidance are aligned with current priorities.

(3) Additional information on the rules-based methodology. Architecture rules have always been a component of enterprise-level architecture constructs. Within the DOD, architecture rules are the controls applied to activities and services and describe how a given activity or service operates within the enterprise.

(4) Summary of Defense Information Environment Architecture guidance regarding the establishment of rules:

(a) Capabilities are described in terms of rules as necessary to ensure the capability is achieved.

(b) Rules are associated with capabilities to guide testing of program capabilities.

(c) Rules are used to guide IT investments.

(d) Rules are used to ensure compliance.

(e) IT solutions are based on IE capabilities and services that adhere to rules.

(5) Summary of DODAF architecture guidance regarding the establishment of rules—

(a) Specifies operational or business constraints on the way business is done in the enterprise.

(b) Describes constraints on the resources, functions and data used in the enterprise.

(c) Based on business imperatives contained in doctrine and guidance.

(d) Control, constrain or otherwise guide the implementation aspects of the architecture.

(e) Rules must be written in English.

(6) Summary of DOD Reference Architecture development guidance—

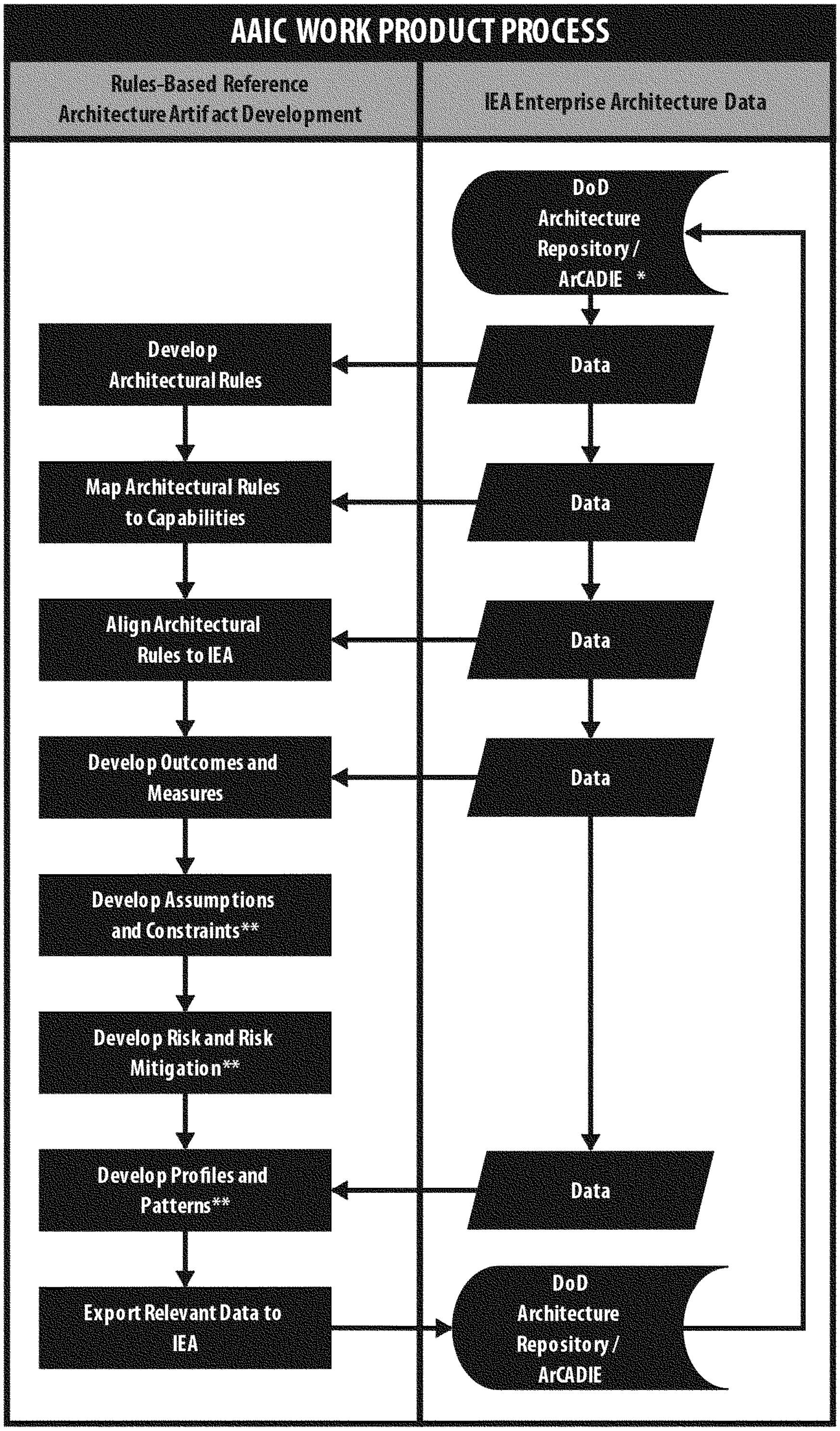
(a) Reference Architectures may be developed by various organizations throughout DOD for their own purposes and intended uses.

(b) No DODAF artifacts are required within component level Reference Architectures.

(c) Reference Architectures may address different levels of abstraction.

(d) Reference Architectures solve a specific (recurring) problem in a problem space, and explain context, goals, purpose, and problem being solved.

(7) The Army CIO/G–6 will continue to adhere to the above DOD guidance as well as expand the use of architecture rules. The current flow of architecture data as it relates to IEA Enterprise Reference Architectures is depicted in figure 5–4.


AAIC WORK PRODUCT PROCESS
Rules-Based Reference Architecture Artifact Development
IEA Enterprise Architecture Data
DoD Architecture Repository / ArCADIE *
Data
Develop Architectural Rules
Data
Map Architectural Rules to Capabilities
Data
Align Architectural Rules to IEA
Data
Develop Outcomes and Measures
Develop Assumptions and Constraints**
Develop Risk and Risk Mitigation**
Data
Develop Profiles and Patterns**
Export Relevant Data to IEA
DoD Architecture Repository / ArCADIE

* Federated access to JIE and Army architecture data via the DoD Warfighter Mission Area portal.
** Process steps (as needed)

Figure 5–5. Architecture data in the Information Enterprise Architecture

h. IEA Enterprise Architecture products inform Army leaders, architects, and analysts across multiple decision forums. Table 5–1 identifies primary consumers of IEA Enterprise Architecture products and their anticipated use.

Table 5–1.
Consumers of Information Enterprise Architecture products and anticipated product use

Groups and Forums	Use of IEA Enterprise Architecture Guidance, Rules, and Data
AEN Service Providers	Identification of IT performance objectives. Identification of minimal set of technical requirements. Communicate Army operational requirements.
AEN End-Users	Communicate CIO/G6 intent for IT modernization. Inform IT support requirements.
Acquisition and IT Solution Developers	Identification of minimal set of technical requirements. Guide acquisition planning and development activities. Support budgetary requests. Provide alignment to DOD enterprise requirements.
Army Doctrine Modernization	Integration with TRADOC Cyber Center of Excellence developed Army Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities Operational View development. Identify Capability Based Assessment gaps and relevant consolidation efforts to gain organization, training, materiel, leadership, personnel efficiencies.
AEN Domains	Identify IT capability gaps. Inform capability set development. Provide performance metrics.
JIE / DOD	Inform JIE architecture development. Validate JIE architectures. Communicate Army equities and requirements.

5–4. Information Enterprise Architecture governance

a. HQDA CIO/G–6 is the lead for the Army IEA. The CIO/G–6 is responsible to ensure architecture components (that is, Operational, Enterprise, and Systems) are aligned, synchronized, and integrated. This includes publishing architecture policy, standards, guidance, constraints, and forecasts. The individual architecture components are developed, maintained, and governed by the respective Architects, as shown in figure 5–2. The AAIC is delegated the authority to review, approve, and release IEA Enterprise Architecture products on behalf of the CIO/G–6. The AAIC will coordinate with the other Architects, the NCS Architecture Integrated Product Team, and other DOD and Army architecture stakeholders as necessary.

b. Each Mission Area has a responsibility to internally integrate the architecture and coordinate architecture activities. The LandWarNet/Mission Command GOSC, the Army Business Council, and the AENC perform this function for the Warfighter Mission Area, Business Mission Area, and EIEMA, respectively. The DCS, G–2 will ensure synchronization of the Defense Intelligence Mission Area and will align architecture integration through the DOD intelligence boards.

c. ACCT is the Army's chartered organization to maintain configuration control of Enterprise Architecture products addressing the EIEMA. The ACCT, established by the CIO/G–6 and chaired by the AAIC, is comprised of voting members from TRADOC; DCS, G–3/5/7; OBT; ASA (ALT); and Second Army. The ACCT collects, reviews, and adjudicates change requests for IEA Enterprise Architecture products in order to assure all updates are aligned with Army strategies and policies, and to ensure stakeholders are aware of pending updates and changes. The ACCT maintains a standard operating procedure for specific instructions on specific processes and procedures.

Section II
Certifications for Network Operations

5–5. Army Interoperability Certification and Baseline Configuration Management

a. General. All Army IT or National Security System (NSS) are required to achieve an AIC and will not be authorized access to the network without an AIC. Successful AIC testing demonstrates compliance with DOD and Army policies. The CIO/G–6 will issue AIC memorandums that indicate what systems and software configurations are authorized to be placed on active networks. The AIC test process validates and certifies that systems meet operational and technical requirements and do not introduce vulnerabilities or cause decrements in service when connected to active networks. The CIO/G–6 will conduct an assessment to determine if an IT or NSS requires an AIC test or if an AIC waiver or exemption should be granted. The AIC testing to validate and certify an IT or NSS is conducted at the Central Technical Support Facility at Fort Hood, Texas, which is the test agent for the CIO/G–6. The CIO/G–6, Cybersecurity Directorate manages the AIC certification process and ensures Army systems have approved information support plans, meet entrance and exit AIC criteria, have no test incident reports impacting end-to-end system interoperability and government Materiel Developers (MATDEVs) or PMs comply with associated CIO/G–6 configuration management requirements. Any questions regarding the AIC process should be directed to CIO/G–6, SAIS–CBC, by email at usarmy.belvoir.hqda-cio-g-6.list.aic-guidance-npe-mgt@mail.mil. Supplemental guidance is available in the Army Interoperability Certification folder on the AKO at https://www.us.army.mil/suite/files/38346957.

b. Entrance criteria for an AIC testing event.

(1) Government MATDEV, PM or system owner of any IT or NSS is responsible for meeting all entrance criteria before the CIO/G–6 will authorize the system to operate on the Army network for an AIC test. Prior to undergoing AIC testing, the MATDEV, PM or System Owner must:

(a) Submit a signed memorandum requesting to undergo AIC testing so the test community can approve and plan for the test of the specific system. The memorandum should be routed through the higher headquarters of the MATDEV or PM and addressed to: Headquarters, Department of the Army, Office, CIO/G–6, ATTN: SAIS–CBC, 5850 23rd Street, Building 220, Fort Belvoir, VA 22060. Required memorandum contents:

1. Subject. In the subject of the memorandum, identify the system title and specific version of software to be tested (for example, SUBJECT: Request for AIC Testing of the Global Information Exchanger System, Version 12.34).

2. Date and location. Provide the desired test date and proposed test location. Testing outside the confines of the Central Technical Support Facility or a CIO/G–6 FaNS accredited test facility will require an additional CIO/G–6 approval.

3. Justification. State the reason or need for an AIC test (for example, Acquisition Milestone, Materiel Release, AIC Expiration, Validated Urgent Operational Need, and so forth).

4. Standards statement. Enclose the Technical View – 1, Technical Standards Profile, and in the body of the memorandum provide a statement as to software conformance with the Technical View – 1.

5. Waivers or exceptions. Identify any approved waivers of technical standards. If applicable, enclose waiver or exemption memorandums.

6. Joint requirements. Identify Joint interoperability requirements and, if appropriate, the status of Joint Interoperability Test Command (JITC) testing and certification.

Note. Note: Program representatives are requested to contact CIO/G–6, SAIS–CBC prior to contacting the JITC and request their facilitation of a test event. The CIO/G–6 may be able to save the program time and funding, possibly arrange a combined Joint and Army interoperability test, or negotiate for the reuse of test data.

7. Authority to operate. Include the status of any current interim authority to operate (IATO), authority to operate (ATO), or certificate of networthiness approved by the system's DAA. Attach a copy of existing approvals.

8. Information support plan. Provide the status of the system's information support plan.

9. Mission Threads. Provide the status of TRADOC developed and approved Mission Threads.

10. Points of contact. Include name, title, and associated telephone and email addresses.

(b) Submit an Army approved information support plan for the system that identifies interoperability requirements and software configuration to be tested. There must be a discussion of backwards compatibility with previous software releases.

(c) Submit information on how to access the repository holding combat developer or proponent developed and approved mission threads documenting required information exchange requirements.

(d) Submit documentation of demonstrated compliance with all information assurance vulnerability management requirements and incorporation of the most recent applicable anti-virus patches.

(e) Submit developmental integration and testing reports showing severity levels and current status of open faults for the system software to undergo interoperability testing.

(2) Government MATDEV or PM of a system must coordinate directly with the CIO/G–6 Test Agent (that is, Central Technical Support Facility) to establish:

(a) Amount of funding required for performing the AIC test.

(b) Method for delivering software for the test event so CIO/G–6 approved configuration management procedures can be applied to ensure test site configuration control. The MATDEV or PM is required to provide all pertinent software artifacts. Memorandum from the Government MATDEV or PM must be provided that establishes the submitted software is the configuration to be tested.

(c) Which combat developer or proponent developed and approved Mission Threads will be decomposed into test cases by the Test Agent.

(d) The scope and content of the AIC test site test plan.

c. Program executive officers self-determination. PEOs have been authorized by the CIO/G–6 to approve minor software changes to previously CIO/G–6 AIC certified systems that have no affect on system interoperability. PMs must request approval from their PEOs in writing and meet criteria established by the CIO/G–6.

(1) PM requests to their PEO should contain:

(a) System Name: (Full title, acronym, nomenclature, model, and version number).

(b) PM and product manager point of contact information.

(c) Date of effective AIC.

(d) Target date for release or fielding.

(e) Justification for this request.

(f) Description of change.

(g) Description of internal testing results and IA compliance.

(h) Coordination with all affected system owners and concurrence on the proposed changes to the certified software configuration must be included in the packet. The request should list titles of the other systems, names of their PMs and the dates of acknowledgement.

(i) Assessment of Risk.

(2) Self-determination guidance:

(a) PMs need to consider:

1. Risk to interoperability supported by documentation of internal testing.

2. Can the change be fielded to entire baseline within reasonable effort and time?

3. Combat developer and evaluator or independent test agent input.

(b) If the system changes have an interoperability impact, then the PM must coordinate with the CIO/G–6 for an AIC determination. An AIC determination can result in a certification, non-certification, waiver, exemption or an interoperability capabilities and limitations assessment.

(c) PM must coordinate and notify all systems with whom they exchange information, obtain written acknowledgement of notification (electronically signed email is sufficient), and ensure there are no unresolved issues. If the PM cannot resolve issues with other systems owners, then the system is not a candidate for PEO self-determination.

(d) If the PEO or Life Cycle Management Command decides the change potentially impacts interoperability, the PM must apply to the CIO/G–6 for an AIC determination.

(e) Any changes to previously AIC certified software, though no impact to interoperability, must be on record in the Army Configuration Management Office (ACMO) that supports AIC testing and maintenance of associated baselined software. PMs must submit self-determination documentation and software changes to the ACMO, which will coordinate with test sites for integration of the software changes into test configurations.

(f) Upon receipt of a favorable PEO Self-Determination ACMO will notify the CIO/G–6, which will issue a memorandum titled “Change of Software” to authorize adding the system software version that identifies the changes to the next HQDA CIO/G–6 Quarterly Baseline Release.

(g) PM must request and receive materiel release (see AR 700–142) from the appropriate Life Cycle Management Command prior to releasing software for operational use.

d. Configuration management of the Army interoperable certified fielded baseline.

(1) All software certified to operate on the Army network must comply with CIO/G–6 approved configuration management procedures. Software submitted for interoperability testing is placed under configuration management by the ACMO, Fort Hood, Texas. Upon certification, software will be controlled until retired from use. MATDEVs and PMs are responsible for ensuring all changes to certified system software are coordinated with the ACMO. ACMO will coordinate with test sites to ensure test configurations are up-to-date and the Army has an appropriate record of its baseline software to support risk mitigation activities and capability decisionmaking. The ACMO effort is in addition to normal configuration management performed by developers and maintainers of systems. The ACMO configuration management plan is available on the Internet at https://ctsf.army.mil/cmweb/Documents/CM/CM%20ABCS%20Plan%20Final.pdf.

(2) The CIO/G–6, Cybersecurity Directorate assesses test results and issues appropriate AIC determinations. The AIC determinations result in inclusion of certified software in the AIC Fielded Baseline which is the compilation of software of systems that have AICs approving use in a networked environment. The AIC Fielded Baseline is composed of multiple software sets, blocks or packages, each containing unique integrated software capabilities that are certified for operations during different time periods. ACMO compiles the AIC Fielded Baseline for the CIO/G–6. Any questions regarding the configuration management process should be directed to CIO/G–6, SAIS–CBC by email at usarmy.belvoir.hqda-cio-g-6.list.cm-and-isp-guidance-npe-mgt@mail.mil.

5–6. Information support plan process

a. General. The information support plan is a document that specifies IT and NSS functional and interoperability requirements. This document is used throughout the DOD as a means for the MATDEV to convey and illustrate how their system, family-of-systems or system-of-systems meets the interoperability and supportability requirements specified in program capabilities documentation validated in JCIDS and needed to support approved Mission Threads (Army, Joint, or Coalition). The architecture descriptive products of the information support plan establishes the baseline interoperability requirements critical for interoperability testing. The information support plan process provides a method for demonstrating system net-centric interoperability capabilities and addressing any issues with shortfalls in capabilities. The information support plan should include Net Ready Key Performance Parameter content as specified in CJCSI 6212.01F and interoperability compliance information specified in DOD interim guidance at http://jitc.fhu.disa.mil/jitc_dri/jitc.html. The information support plan must reference all Army, Joint and Coalition approved Mission Threads, which identify time-ordered interaction requirements for the system and software to be tested. If appropriate Mission Threads are not available, the submitter must include in their information support plan a system view – 10c, systems event-trace description. The system view – 10c is valuable for moving to the next level of detail from the initial solution design, to help define a sequence of functions and system data interfaces, and to ensure that each participating resource or system port role has the necessary information it needs, at the right time, to perform its assigned functionality.

(1) Information support plan submission life cycle events:

(a) Initial information support plan is submitted 90 days prior to the preliminary design review and milestone B.

(b) Revised information support plan is submitted 90 days prior to the critical design review.

(c) Final information support plan is submitted 90 days prior to milestone C decision and used for initial interoperability certification test.

(d) Updated information support plan is submitted 180 days prior to re-certification interoperability test.

(2) Submitted information support plans must contain the latest technical information on system and software.

b. Roles and functions.

(1) Chief Information Office/G–6. In accordance with AR 25–1, CIO/G–6 is the approval authority for all Army information support plans and ensures Army compliance to overarching DOD and CJCSI information support plan policy. Any questions regarding the information support plan process should be directed to CIO/G–6, SAIS–CBC by email at usarmy.belvoir.hqda-cio-g-6.list.cm-and-isp-guidance-npe-mgt@mail.mil. As the approval authority, the CIO/G–6:

(a) Defines Army information support plan policy and supporting procedures.

(b) Serves as the HQDA interface with the DOD CIO, Joint Staff J6, DISA, JITC and Army program offices.

(c) Serves as the Army organization responsible for handling information support plan processing and interface with the GIG Technical Guidance Federation (https://gtg.csd.disa.mil).

(d) Serves as the approval authority for Army information support plan waivers when appropriate for component unique IT and NSS (that is, no Joint interfaces) and for tailored information support plan requests.

(e) Provides to Joint Staff J6 and DOD CIO the Army's statement of concurrence or non-concurrence on ACAT I and DOD special interest information support plans.

(f) Informs milestone decision authorities on the status of information support plans during milestone reviews.

(2) Program executive officers. PEOs provide a memorandum endorsing each information support plan submission, which states the PM, TRADOC Capability Manager, and other affected Army and Joint organizations have concurred with the information support plan and it is ready for release to the CIO/G–6.

(3) System owners. PMs and government MATDEV prepare information support plans for their systems in accordance with this pamphlet, Army and Joint policies, and DOD guidance (see DODD 4630.05, DODI 8330.01, and interim guidance available at http://jitc.fhu.disa.mil/jitc_dri/jitc.html). PMs and government MATDEV should —

(a) Use the information support plan tool at the GIG Technical Guidance Federation. Architecture views and Mission Threads may be hyperlinked to the information support plan if the links are readily accessible to all reviewers.

(b) Coordinate with the CIO/G–6, Army Architecture Integration Center (SAIS–AEA) for guidance on Army's approved technical architecture.

(c) Ensure the information support plan shows compliance with the system Net Ready Key Performance Parameter as specified in CJCSI 6212.01F; compliance with applicable standards mandated in the DISR, Army technical architectures for COE, and relevant organization unique standards; compliance with DOD IA directives and policies; identifies any IA and interoperability certifications; and identifies spectrum issues and whether or not there has been an appropriate submission of a Frequency Management Office DD Form 1494 (Application for Equipment Frequency Allocation).

(d) Show linkage between information support plans, JCIDS approved capabilities documents, and approved Mission Threads. The architecture views in an information support plan should be updated with each subsequent submission. Views must be built upon the latest set of integrated architecture views referenced by approved system capability documents (see CJCSI 3170.01H). Information support plans should reference approved Mission Threads that identify time-ordered interaction requirements for the system and/or software. Alternatively, the information support plan should include a system view – 10c, system events-trace description.

(e) Ensure the information support plan submission includes a submittal cover memorandum signed by the system's PEO or proponent at the Senior Executive Service or General Officer level. The memorandum must state the PM, TRADOC Capability Manager, and other affected Army and Joint organizations have concurred with the information support plan and it is ready for release to the CIO/G–6. Memorandum should state that all PMs and MATDEVs for interfacing systems attest that the information support plan accurately states current threshold interoperability requirements and capabilities.

(4) U.S. Army Training and Doctrine Command Capability Manager. The TRADOC Capability Manager or, if a

TRADOC Capability Manager is not assigned, the system proponent will review the information support plan for accuracy, completeness, and co-sign the submittal cover memorandum attesting that the information support plan is ready for release to the CIO/G–6.

c. Tailored information support plans. PMs and/or MATDEVs for ACAT II and below, non-ACAT, non-OSD special interest and fielded programs may request to develop a tailored information support plan, which demands fewer resources than producing a normal information support plan. A PM and/or MATDEV may develop a tailored information support plan only upon approval from the CIO/G–6, Cybersecurity Directorate. Requests must be submitted to CIO/G–6, SAIS–CBC and contain the following information:

(1) System information:

(a) Full system name.

(b) System acronym.

(c) Nomenclature.

(d) Model number.

(e) Version number.

(f) DITPR number.

(g) JITC system tracking program number (if assigned).

(2) Contact information, including email addresses and postal addresses:

(a) Army representative to the Military Communications-Electronics Board Interoperability Steering Group (CIO/G–6, SAIS–CBC).

(b) Requesting agency.

(c) Technical point of contact.

(d) Program manager.

(e) Alternate program manager.

(f) JITC action officer (if assigned).

(3) System description:

(a) Key operational nodes and system components.

(b) How the system fits into the operational environment.

(c) Existing DODAF artifacts (such as, capability development document, capability production document, test and evaluation plans, Mission Threads, and so forth).

(4) Eligibility criteria:

(a) Program acquisition category.

(b) System milestone status and dates.

(c) Whether the system is a rapid acquisition or legacy program.

(d) Will it be employed on the Sensitive but Unclassified (SBU) Voice Network (formerly Defense Switching Network (DSN)) or Public Switched Telephone Network (see CJCSI 6211.02 for descriptions).

(e) Year the program began.

(f) Type of funding (provide details on future Operations and Maintenance, Army; Other Procurement, Army (OPA); and Research, Development, Test and Evaluation funding).

(g) Status of requirements documentation.

(5) Questions to be answered:

(a) How many systems will be fielded and where?

(b) Joint connectivity requirements? (Identify other Service and Agency interfaces.)

(c) Past JITC or Service testing efforts? If so, provide a short summary of past testing efforts and copies of test reports. (Identify exercise evaluations, if appropriate.)

(d) Road Map and specific date of when the system can be certified and whether it is currently scheduled for Joint interoperability testing?

(e) Known problems or issues that could delay or prohibit JITC certification?

(f) If you feel you have no Joint interfaces, do you plan on submitting a test exemption?

(6) Statement: “I (PM and/or MATDEV Printed Name) affirm the information in this request is complete and accurate to the best of my knowledge and understand I have six months to complete the tailored information support plan from date of approval.” Request must be signed by the PM or MATDEV and dated.

(7) Army Interoperability Steering Group representative justification for approving the tailored information support plan. (Provided by CIO/G–6, SAIS–CBC.)

(8) Statement: “I (Army Interoperability Steering Group Representative Printed Name) affirm the information in this request is complete and accurate to the best of my knowledge and I understand the program has six months to complete the tailored information support plan from date of approval.” Request must be signed by the representative and dated.

d. Information support plan waivers. Waiver requests will be provided to the CIO/G–6, SAIS–CBC for endorsement prior to submission to DOD CIO and Joint Staff J6. PMs and MATDEVs may apply for an information support plan waiver on Joint programs if their program satisfies one of the following requirements:

(1) The operational chain of command and the Chairman of the Joint Chiefs of Staff have validated an urgent operational need.

(2) A pilot program is coordinated with, and validated by, DOD CIO or the DOD Component concerned. Typically to accommodate the introduction of new or emerging technology.

(3) The fielded system is scheduled for retirement, and the cost of complying with this policy outweighs the benefit to the DOD.

(4) The system has no Joint interoperability requirements.

e. Information support plan submission method and staffing procedures.

(1) The Army will lead the review of all information support plans regardless of ACAT level. If a program meets the criteria for a Joint review listed below, the Army will coordinate the review with the Joint community (including DISA).

(a) For ACAT II and below programs, the Army will select the appropriate additional DOD Components for the Joint review; however, the review will include at a minimum the Joint Staff and DISA.

(b) For all ACAT I and DOD CIO special interest programs, the information support plan will be staffed to all DOD Components as part of a DOD-level Joint review. The DOD CIO will participate in ACAT I and DOD special interest information support plan reviews, and will provide concurrence, concurrence with comment, or non-concurrence for consideration during Army final approval.

(2) Joint reviews will be conducted for all IT and NSS information support plans that:

(a) Have a Joint staffing designator (formerly Joint potential designator) of Joint Requirements Oversight Council Interest; Joint Capabilities Board Interest; or Joint integration with a Net Ready Key Performance Parameter.

(b) Implement information exchanges across DOD Component boundaries.

(c) Implement a Web service with the explicit or implicit intention to share information across organizational boundaries.

(d) Have received a DOD Component determination that a Joint review is necessary.

(3) Information support plan will be reviewed in the GIG Technical Guidance Federation for 30 days and will result in a set of comments for the PM to adjudicate. The PM will adjudicate critical comments within 90 days by actively engaging with the organization and person who made the comment to ensure adequate resolution. For critical comments that cannot be resolved, the issue will be elevated to the CIO/G–6, SAIS–CBC for resolution. Critical risks and issues identified through information support plan reviews will be briefed by the PM to integrated product teams and overarching integrated product team, as appropriate.

(4) PMs or MATDEVS, after the adjudication and revision process, will submit their final information support plan with submission cover memorandum to the CIO/G–6 through the GIG Technical Guidance Federation.

(5) Upon receipt, CIO/G–6, SAIS–CBC will conduct a 14 day review of the information support plan and adjudicated comments. If there are no identified issues, the CIO/G–6, SAIS–CBC will issue an information support plan approval memorandum.

f. Information support plans submission for test support. The final information support plan is updated to support each AIC and Joint interoperability testing event. Updated information support plans will be submitted to the CIO/G–6 180 days prior to a scheduled test. The CIO/G–6 will conduct an Army only staffing of the updated information support plan which will take 30 days. If no critical issues are identified during staffing, the CIO/G–6 will authorize the approved test site to use the updated information support plan for test case development.

Chapter 6
Installation Information Technology Services and Support

Section I
Managing Information Technology at the Installation

6–1. General

a. NETCOM provides common C4IM services and applications to installations Armywide through their subordinate theater commands, signal brigades and/or battalions and ultimately, the NECs on all Army posts, camps and stations. NECs are resourced to deliver three specific Service Support Programs from the ACSIM common level of support services listing. The IT Service Support Programs are: Service 15 – telecommunications; Service 18 – information assurance; and Service 19 – automation. The Army CIO/G–6, with the support of NETCOM, documents, maintains, and updates the many discreet services and associated tasks that comprise these three Service Support Programs. The IT Service Support Programs are documented in what is called the C4IM Services List. The list and the appropriate method of delivery and/or resourcing are updated annually. The latest list is located at https://www.itmetrics.hua.army.mil/.

b. Senior IM officials representing the mission commander or key tenant units and organizations will play a key role in coordinating with the NEC and negotiating their perceived C4IM services support requirements via a SLA. These senior IM officials must ensure their unit's or organization's voice, data, and video or visual information needs are provided within available resources and play a key role in ensuring metrics to gauge the effectiveness of NEC support are developed and monitored.

6–2. Network Enterprise Center

a. An installation NEC provides C4IM services to the installation's tenants or assigned geographical area through a fully integrated IT activity. The directors of the NECs are information managers and are fluent in the business processes and technology to help tenant organizations achieve mission goals. A NEC may provide C4IM services and assistance to both the operational and generating forces and/or organizations assigned to their installations or in their geographical area of operations. NECs may aid CONUS and OCONUS emergency operations centers, in accordance with agreed upon service level agreements. Installations and/or activities require an array of IT services based on size, location, and a varied customer base. The NEC performs several vital roles in the installation's capital planning and investment management processes, in addition to delivering required services. Most importantly, a NEC validates new initiatives and ensures they comply with C4/IT guidance and Army enterprise architecture. A NEC establishes and aids application of the most suitable knowledge management technology services and products for the agency.

b. In both CONUS and OCONUS, the NECs are aligned under regional NETCOM signal battalions or brigades. NEC structures are based on capacity of common level services provided, and the size or workload of the NEC influences the structure and staffing levels of the NEC organization. A NEC organization staffing may be enlarged, flexed or surged, based on the immediate customer's mission and/or business needs over the baseline and is in accordance with the developed service level agreement with this particular customer.

c. The NEC provides a standard set of C4IM services at a delivery level and resourcing methodology designated in the C4IM Services List for automation, communication systems support, and information assurance. Should Army permit and/or require tenants to reimburse for services over the level of support found in the C4IM Services List, the NEC and the tenant will establish a SLA in accordance with NETCOM format and standards. NETCOM oversees SLA development and performance through their subordinate commands.

6–3. Senior information management office/officer concept and functions

a. The Senior IM official is the principal staff officer for all matters concerning command, control, communications, and computer operations. The Senior IM official works at senior levels of command, just under the ACOMs, advising the commander, staff, and subordinate commanders on IM/IT matters. They are responsible for implementing the command's IM/IT program, in accordance with IM/IT policies as prescribed by the Army CIO. The command senior IM official directly supervises the IM/IT staff, related programs, and activities and executes LandWarNet global network enterprise activities, as prescribed by Army Cyber Command/2nd U.S. Army. Whenever a Senior IM official is present in the command structure, they typically serve as the primary coordinator with external service providers (for example, the NEC) and the assessor for quality of these services.

b. The Senior IM official's tasks deal with oversight, guidance, governance, plus short- and long- range planning activities.

6–4. Information management office/officer concept and functions

a. The Information management office/officer (IMO) is the office or individual that represents their organization or assists the senior IM official in effectively managing the organization's IM/IT processes and resources to enable the organization's business and mission processes. The IMO is essentially a liaison to the NEC that reports and tracks user requirements, alerts the NEC of any network issues, documents and shares all IT purchases and system deployments with the NEC, maintains a list of users and IT assets as well as provides guidance to organization's users on IT policy. General duties and functions of an IMO are to:

(1) Monitor all common-user C4IM baseline service delivery and support provided by the NEC or signal battalion.

(2) Identify, validate, and negotiate C4IM-enhanced and mission-specific service delivery and support requirements with the NEC or signal battalion.

(3) Implement and enforce IM/IT policies and procedures within their organization, in coordination with their local NEC and appropriate information assurance management personnel.

b. An IMO's task is to develop requirements for operational instructions for applications and systems to include:

(1) Information assurance, to include supporting IA personnel in the administration of and compliance with IA policy and procedures, see AR 25–2.

(2) IT management, to include:

(a) C4/IT resource management, to include:

1. Providing C4/IT operational requirements to NECs or signal battalions.

2. Developing C4/IT plans, requirements and strategic investment strategies, in coordination with ACOM.

3. Reimbursing for enhanced and mission unique services.

(b) Requirements validation, to include:

1. Identifying, validating, and consolidating requirements for submission to NEC or signal battalion.

2. Programming functional unique C4/IT requirements through ACOM.

3. Programming all requirements for enhanced and mission-unique services.

(c) C4IM performance management, to include:

1. Assessing the effectiveness and efficiency of C4/IT support.

2. Reporting effectiveness and efficiency of C4/IT support to ACOM.

3. Notifying and working with the NEC or signal battalion to resolve issues concerning substandard C4/IT support effectiveness and efficiency.

(d) IT metrics (as relates to ISRs), to include:

1. Measuring (or cause to have measured) those command and/or organizational items reportable through the IT Metrics Program.

2. Responding to reporting requirements of the supporting NEC or signal battalion.

(e) Service agreements, to include:

1. Participating in the development of the SLAs, as required by mission.

2. Coordinating with ACOM on agreement and funding of enhanced and mission-specific services.

(f) Developing supporting architecture.

1. Operational architecture, to include:

a. Outlining and documenting missions, functions, business processes, and information requirements.

b. Submitting C4/IT requirements to NEC or signal battalion.

c. Recommending to ACOM functional applications for their mission requirement.

2. Systems architecture, to include:

a. Recommending to ACOM applications for their mission requirement.

b. Providing configuration layout and connectivity of C4/IT systems to NEC or signal battalion.

3. C4/IT architecture management, to include:

a. Providing an integrated framework involving or maintaining existing IT and acquiring new IT to achieve the agency's strategic goals, information management goals and support to the Soldier. This includes interoperability, scalability, and standardization.

b. Acting as liaison to the NEC or signal battalion on behalf of the customer population.

(g) Data management and interoperability (see chapter 4).

(h) 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 PPBE 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. Routing office automation acquisition and local C4/IT purchase requests through the NEC or signal battalion.

2. Performing business process reengineering and/or 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 (PDAs), 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. Purchasing of office automation via Army enterprise contract vehicles.

6. Providing system specifications and functionality and obtain approval from the NEC or signal battalion.

7. Obtaining (and providing) a certificate of networthiness through the NEC or signal battalion, if office automation requires network connectivity and/or Web-based application.

8. Inputting requirements to ACOM for input to the planning, programming, budgeting and executing system for the life-cycle replacement of office automation equipment and software upgrades at the desktop level.

9. Capturing and reporting all C4/IT expenditures to NEC or signal battalion (to include international merchants purchase authorization card purchases).

10. Identify requirements for contracting support for short-haul communications and/or post, camp, station and

BASECOM. Short-haul communications consist of local telephone systems and associated trunking to the nearest serving commercial central office.

11. Managing C4/IT.

(i) Update and maintain installation-level technical support and service, to include testing equipment and evaluating software and/or hardware.

(j) 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 and/or 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 NEC or signal battalion.

(k) Synchronization of change; migration of modernization; change management, to include:

1. Updating and maintaining site content.

2. Submitting requests for networthiness to NEC or signal battalion.

3. Providing a certificate of networthiness to the NEC or signal battalion.

(l) Networthiness certification, to include:

1. Submitting a request for a networthiness certificate to the NEC, before any new or enhanced system or capability is connected to the Army data information structure. Information on the Networthiness Certification Program is available at https://www.us.army.mil/suite/page/137030.

2. Identifying policy from Army Enterprise Infostructure Management Steering Group as review council of negative results.

3. Identifying networthiness criteria and submit systems, applications, or capabilities for testing.

(m) Providing C4/IT support services, which include:

1. Server management. The IMO task is to identify tenant servers through the local NEC or signal battalion for consolidation at Army processing centers and installations.

2. Functional processing center operations. The IMO task is to develop requirements and operate developed applications and systems.

3. 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.

4. Functional application development. The IMO publishes procedural guidance for mission and/or business-based requirements, functional applications and data requirements definition and specification. The IMO task is to develop requirements and operate developed applications and systems.

5. 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.

(n) NEC support services, to include acting as a NEC liaison for 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 IP). Tasks include:

1. Providing first-line of assistance for the local user on hardware and software.

2. Establishing service level agreements with NEC or signal battalion to provide funding for enhanced and mission-unique services.

3. Identifying a primary organizational point of contact for problem identification and resolution.

4. Providing requests for customer support service to NEC or signal battalion.

5. Providing operational data services. The IMO follows published procedural guidance for data ownership, access control, data management, and data manipulation. The IMO task is to manage and administer organizational data.

(o) C4/IT hardware utilization, reutilization, and/or 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 support of an installation and/or facility or assigned

area's networks, to include those supporting DOD, DA, and ACOM initiatives. The IMO task is to assist the information assurance support officers (IASO) or NEC tasks.

(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 NEC or signal battalion.

Section II
Information Technology User Support Principles

6–5. 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 NEC. 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 (DISN) 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, SBU Voice, 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 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.

c. Privacy and security provisions include the following:

(1) The Privacy Act of 1974 (5 USC 552a) and the FOIA govern 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 email, are notified that their use of this equipment is subject to monitoring and recording. Per DODD 5240.01, 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 in accordance with 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). The following actions are recommended:

(a) Limit the use of graphics in email 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 to All" email feature, when responding to an individual.

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

(e) Rarely use the "Return Receipt" email feature. Use only on official email, when receipt must be verified (for example, where the email 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, AR 500–3, and DODD 3020.26).

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

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

(2) SLAs.

(3) Interservice agreements.

(4) Support to non-DOD Federal agencies.

(5) Customer service guide(s).

6–6. 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 email service for personal email 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.

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 and DODI 1100.21. The Army Community Service 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 Army Community Service information management officer would advise on proper workstation and IT usage, help-desk information, and reporting and/or 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) 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) NECs should work closely with the Army Community Service Directors to ensure that military spouses that are designated as statutory volunteers receive the support to which they are authorized under AR 608–1.

6–7. Support for health, morale, and welfare or morale, welfare, and recreation telecommunications

a. Health, Morale, and Welfare (HMW) communications (voice/IP, video teleconference) will be primarily made over the HMW or morale, welfare, recreation (MWR) provided nonappropriated funded communications services.

b. DOD members assigned to a CONUS installation, ACOM, or other organization and deployed OCONUS may place HMW calls through a CONUS installation phone switch or to Europe through an automated attendant in Europe. 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 receive their phone calls.

(3) Emergency calls may exceed specified limits (per CJCSI 6211.02D), when approved by the commander.

(4) The Government does not incur costs associated with the extension or 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) SBU Voice switchboard locations have been reduced because of base closures and force reductions. Another system for morale calls is the automated directory assistance system, installed on several Army CONUS installations. Calls made by deployed Soldiers and authorized personnel to automated directory assistance system sites will be connected to an automated call attendant and its voice-recognition morale call subsystem. Soldiers and authorized personnel can access the automated directory assistance system with SBU Voice phone lines. The Government cannot pay toll charges for extending personal calls. The SBU Voice directory (http://www.disa.mil/Services/Network-Services/Voice/SBU–Voice) is a third source for possible off-netting of approved morale calls.

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

(1) DOD members and their family may use Family Readiness Group accounts created by their command to send personal email messages. The subject line should identify the receiving party. Units may establish Family Readiness Group email distribution and access procedures within their units. No email 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 email 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 email use will usually be after duty hours or at the discretion of the unit commander.

(3) Army members may use assigned email 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.

6–8. Information access for the disabled

a. General. All Federal agency acquisition of electronic and information technology (EIT) should meet the accessibility standards of Section 508 to improve the accessibility of Government information and data and ensure EIT is accessible to Army employees and citizens with disabilities. Unless an exception applies, all Federal and DOD acquisitions of EIT must meet the applicable accessibility technical standards and/or the functional performance criteria (36 CFR 1194) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board) (see AR 25–1).

b. Definition. EIT has the same meaning as IT, 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 Federal employee 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/).

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). 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). GSA provides technical assistance to Federal agencies and the general public in many forms such as, but not limited to, policy support, training, coordination, and showcasing of assistive technologies. The BuyAccessible program (www.buyaccessible.gov) is part of GSA’s commitment to provide standard processes and tools to support Government-wide compliance with Section 508. These tools and processes were developed by industry stakeholders’ determination on how to best implement the Section 508 standards. The BuyAccessible System has three components, all made available to any agency at no cost, to help with the quick, easy, and efficient implementation of all Section 508 standards.

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) National Security Systems. 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 will 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 $3,000 and under are no longer exempted from Section 508. Contracting officers and purchase cardholders are to use the same accessibility standards in micropurchases as any other EIT purchases.

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.

(5) 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.

(6) 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.

(7) 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.

(8) 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, and frequently asked questions is provided at www.section508.gov/. In addition, the CIO/G–6 is available to give technical and NSS assistance. Email cio-g6.pia.inbox@mail.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.

6–9. Information technology support for telework or telecommuting

a. General. 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 DODI 1035.01.

b. Policy. AR 25–1, authorizes individuals to telework according to DOD and Army policy. See DODI 1035.01 and DA Memo 690–8.

c. Terms and conditions. A DD Form 2946, (Department of Defense Telework Agreement) that outlines the terms and conditions (including IT support) of the arrangement is required before the employee commences regular or recurring telework (see appendix B for more information). The DAA 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. There are various types of telework categories and definitions (see www.telework.gov for more information).

d. Government-furnished equipment. Use of Government-furnished IT equipment and supplies for use in an employee's home for regular and recurring telework arrangements. All DD Form 2946s will address mandatory information assurance requirements and be approved by the DAA prior to implementation. In addition, the use of government-furnished equipment must comply with the appropriate provisions of AR 25–2, Information Assurance.

(1) Local procedures address issues such as Federal and/or local laws, workplace requirements (safety, hardware and/or software issues, security and/or accreditation, and so on), and union requirements. The local command decides if telework or 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 program management.

(3) Organizations may contact the Army point of contact via email at cio-g6.dms.manager@mail.mil.

e. Employee-furnished equipment. Where approved by the DAA, the use of employee-owned computers and equipment for telework is authorized. All DD Form 2946s will address mandatory IA requirements and be approved by the DAA prior to implementation. Use of resources to fund limited operating costs associated with communications (for example, digital subscriber line, cable modems, and analog dial-up lines) within an employee's residence as an alternative worksite may be determined by the local commander. (IT resources for telework resources are not intended for individuals who occasionally check email from their residences.)

(1) Army assumes no responsibility for any operating costs associated with the employee using his or her residence as an alternative worksite, including home maintenance, insurance, or utilities. Army is not liable for damages to an employee's personal or real property, while the employee is working at the approved alternative worksite, except to the extent the Government is liable under the Federal Tort Claims Act or the Military and Civilian Employees Claims Act.

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

(3) Subject to agreement by the DAA, a teleworking employee may use employee-owned equipment, software, and/or communications devices, with appropriate security measures, for work on unclassified data (including controlled unclassified, for official use only (FOUO), and Privacy Act-protected data) provided the teleworking employee accesses and processes such data using HQDA-provided virtualization and remote access software, such as CITRIX, and does not retain copies or derivatives of such data on any part of the employee-owned system. Employee-owned information systems will be used in accordance with AR 25–2. Additionally, employee-owned systems must be firewall-enabled and contain antivirus and anti-malware software. Employees are responsible for the installation, use, and maintenance of all employee-owned equipment, in accordance with these criteria.

(4) Whether an employee uses a Government-furnished or an employee-owned computer, the CAC will be used to enable cryptographic logon entry into IT systems and applications that reside on DOD computer networks and systems. The CAC will also be the primary platform for implementation of public key infrastructure.

(5) Telework employees who do not obtain proper CAC credentials will not have access to any DOD IT systems, including their office email accounts.

(6) Once a user sets up his or her CAC for cryptographic logon, the user is responsible for maintaining possession of his or her CAC at all times. Users will not be issued additional CACs in the event their cards are not available to access their accounts. Until a user retrieves his or her CAC, that user will not be able to access any DOD IT computer networks or systems.

(7) Telework employees will comply with all security provisions.

(8) Telework employees are responsible for protecting any Government-furnished equipment and property at the alternative worksite. Employees will return all Government-furnished equipment (equipment, software, and communications devices) to the organization's property book officer or designated representative on the termination of the employment relationship with an HQDA organization, at the termination of the telework arrangement, or at the organization's request.

(9) Telework employees are responsible for safeguarding all official information and data as required by applicable law and regulation.

(a) Classified information (hardcopy or electronic) will not be removed from the traditional worksite to an alternative worksite. No classified documents (hardcopy or electronic) may be taken to, or created at, an employee's alternative worksite. FOUO and controlled unclassified information may be taken to an alternative worksite, provided the employee takes necessary precautions to protect the data consistent with Army and DOD directives, regulations, and policies.

(b) With a view to preventing the loss of any official information or data, the supervisor will determine how frequently, if at all, a telework employee must backup copies of official information or data on network drives or removable disks. The supervisor may require the employee to send backup copies of information or data to the traditional worksite.

(c) Telework employees will apply approved safeguards to protect official information and data from unauthorized disclosure or damage and will comply with the Privacy Act of 1974 and implementing regulations.

(10) The supervisor or other representative of the employee's organization retains the right to inspect the alternative worksite to ensure that safety standards are met and Government-furnished equipment is properly maintained. When the employee's alternative worksite is in the employee's home, such inspections will occur by appointment only.

(11) A telework employee remains subject to the provisions of the Joint Ethics Regulation, the general principles of Federal employment, and all other Federal and agency standards of conduct, while working at the alternative worksite.

f. Government resources. Use of Government IT resources (such as computers, facsimile machines, modems, and so on) for telework is authorized, contingent upon availability of funds 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 with unclassified data (including controlled unclassified, FOUO data, and Privacy Act-protected data), when the access method involves a direct connection to the headquarters enterprise network, such as through the virtual private network or remote access server. The employee must agree to comply with the terms of any computer software license and copyright agreements, as well as with any Army computer virus protection requirements and procedures as authorized for any regular and recurring telework arrangement. A DD Form 2946 that outlines the terms, conditions, and limitations of IT support for the arrangement is required, before the employee commences regular or recurring telework. Information for the DD Form 2946, telework safety assessment, supervisory-employee policies and procedures list, and telework arrangement cancellation are available in appendix B.

6–10. Training

a. User requirements.

(1) Training is a key service of the NEC. In establishing a training program, the NEC considers factors that impact the types of training offered to the users supported. The NECs provide training in IT management, regulatory requirements such as computer security, IT support and personnel training requirements (for example, IMOs), as well as special training for requirements of a single unit or segment of the NEC's customer base.

(2) The NEC determines and publishes a standard list of items to be supported. The software applications included in the list serves as one component of the NEC's training program. Typically, these products consist of a standard COTS office suite package (word processing, spreadsheet, presentation, database management, and so on), the Defense Message System (DMS) email 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, https://usarmy.skillport.com/.

(3) Regulatory required training may be included in the NEC'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. DODI 8500.01 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 and certification requirements can be found in AR 25–2. 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. IA training is available at https://ia.signal.army.mil/ and https://iatraining.us.army.mil/.

(4) The unit IMO 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 and the NEC'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 at https://usarmy.skillport.com/.

(2) The NEC 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 NEC's customer base is ever changing. Continual growth is expected in the automation of business processes and enhancements in technology. NECs should plan for new technology training for the NEC 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 and/or program. Many training companies offer a way for the NEC 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 (https://usarmy.skillport.com/), the ITM CP–34 (https://www.us.army.mil/suite/page/530206/) 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 NEC 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 NEC and support staff the needed training, based upon the agreement in place.

6–11. 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) SBU Voice procedural guidance prepared by the DISA, including Joint Uniform Telephone Communications Precedence System and troubleshooting procedures.

b. Authorization. Installation Management Command (IMCOM) Regions, ACOMs, ASCC, DRU, and designated subordinate commands are authorized to print information systems directories for their units and/or 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 and/or 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 Armywide 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, official U.S. Army phone or communications directories must display appropriate warning banners and labels.

e. Master directory. Each IMCOM region, installation, ACOM, ASCC, DRU, 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 NEC. 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 SBU Voice numbers.

(1) The NEC 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, ACOM 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, ACOM 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 listing of 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 private branch exchange

(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 and/or 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 IMCOM region, installation, ACOM, 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 NEC, 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 NEC 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 and/or 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.

6–12. Information technology requirements in military construction projects

a. Information technology 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. I3A technical criteria, for NIPRNET and SIPRNET respectively, is available at https://www.us.army.mil/suite/folder/5745483 and https://www.us.army.mil/suite/folder/5744948.

b. Information technology 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 and/or switch upgrade, phones and local area network (LAN) equipment, are not included in this definition. These items are normally user/NEC-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. Network Enterprise Center functions.

(1) The NEC documents the project's IT requirements; develops the input to 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 for inclusion in the project's DD Form 1391.

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

(3) NEC personnel will coordinate mission-unique requirements with the senior IT/IM office under the senior mission commander or key tenant units and/or organizations on the installation. The IT/IM manager will outline customer inside plant and infrastructure voice, data, video and/or visual information requirements with the NEC to assist the NEC in determining related outside plant infrastructure and/or equipment locations. The NEC ensures that the proposed outside plant solutions support both the needs of the customer as well as the service provider, bearing in mind long term growth impacts of the installation.

(4) The NEC provides the director of public works with a dated and signed copy of the ISCE for inclusion in the project's input for section 17 of 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 NEC reviews, revises, and updates Section 17, if the project scope or building functional requirement or site location is changed. The ACOM 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 NEC 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 NEC in producing a project's initial ISCE. The NEC incorporates a minimum amount of project information that combines

with user requirements to generate an ISCE. After reviewing the ISCE and making any required modification, the NEC forwards the recommended ISCE to the ACOM for review and concurrence.

d. Design agent.

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

(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 and/or 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- FDED in coordination with HQDA, U.S. Army Community and Family Support Center NAF construction office.

(3) USAISEC–FDED exercises oversight of MILCON IT. USAISEC–FDED performs these functions:

(a) Provides planning, programming, and budgeting input to the United States Army Communications-Electronics Command for procurement of common user IT instruments and switching equipment in support of IT in MILCON-funded construction. The appropriate program manager or program executive office provides planning, programming, and budgeting input for mission oriented IT in MILCOM-funded communications facilities construction.

(b) Reviews user IT, in functional terms, 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 Theater Signal Command or the ACOM, 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 ACOMs.

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

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

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

e. Information systems cost estimate 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 NEC 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) Theater Signal Command or ACOM functions. The Theater Signal Command or ACOM reviews and certifies the NEC's ISCE for the project. The Theater Signal Command or ACOM 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–FDED functions.

(a) The USAISEC–FDED plays several roles with respect to the project's ISCE. As an agent of the ACSIM, USAISEC certifies the ISCEs intended for the military construction, Army program prior to the PRB. This certification ensures that the ISCE is a reasonably accurate estimate of the costs related to the project. USAISEC–FDED routinely reviews and updates the ISCEs of the military construction, Army 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–FDED updates the ISCE and gives copies to USACE, the ACOM, and the NEC involved with each particular project.

(b) USAISEC–FDED routinely reviews and updates the ISCEs of the military construction, Army 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–FDED updates the ISCE and gives copies to USACE, the ACOM and the NEC involved with each particular project.

(c) USAISEC–FDED participates as a member of the planning charrette as the technical advisor to the NEC, Theater Signal Command, and ACOM. USAISEC–FDED coordinates with the installation NEC to determine the telecommunication requirements for the project.

(d) USAISEC–FDED integrates the ISCE into the project's overall requirements and tracks subsequent ISCE throughout the project.

Section III
Information Technology Systems and Services

This chapter offers guidelines on hardware and software management, acquiring and delivering IT systems, information processing services, and equipment. See AR 70–1 and DA Pam 70–3 for more information on the Army's acquisition policy and procedures.

6–13. Hardware and software management services

The best method of acquiring hardware and software 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 NECs or the PEO associated with this acquisition. The evaluation should also determine integration risks associated with the COTS products.

a. Enterprise Software Initiative. 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. CHESS is the Army's software product manager. As the designated software product manager, CHESS 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 CHESS Web site, https://chess.army.mil/. The DOD ESI homepage lists all ESI managed software and is located at 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 CHESS 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. Computer Hardware, Enterprise Software Solutions office. CHESS is the required source for all commercial IT purchases, regardless of dollar value (see section 2–7). All commercial IT purchases must be submitted to the CHESS office. In the event CHESS cannot support an organization's requirement, CHESS will notify the acquiring organization that other DOD and Federal activity contracts will be considered to satisfy their documented requirements.

c. Commercial off-the-shelf 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. Try to 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 FIPS for the four-digit date format for data exchange. PMs are required to identify Government off-the-shelf/COTS software that uses the two-digit date windowing technique and then modify it to the four-digit standard. Modification requires either replacing the system with a later version not employing the two-digit date windowing technique or installing four-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 and/or Government off-the-shelf and hardware products acquired comply with the standardization required by the current version of the DISR and the NETCOM technical control on desktop and server standardization. The goal is to ensure standardization and interoperability in each system (see CIO/G–6 Common Operating Environment Architecture (http://ciog6.army.mil/)). 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 https://gtg.csd.disa.mil, AR 25–1).

e. Thin Client Computing.

(1) The Army endorses the use of thin client computing, to include zero client technology, but only when it meets organizational mission requirements. Prior to implementing a thin client computing environment, the proponent organization should determine the risks to mission and cost, including those associated with investment, migration, baseline support, above-baseline operations and maintenance, and LCM.

(2) Organizations considering implementing thin client computing should consult the resources available at https://www.us.army.mil/suite/files/21928696. In order to guide the decisionmaking process, Army organizations are encouraged to use the Mission Analysis Criteria and Cost Benefit Analysis Guide. Implementation and support of thin client should conform to the Thin Client Computing Technical Authority document.

(3) NETCOM and subordinate NECs are the responsible agents for the operation and maintenance (O&M) of all thin client computing environments for NEC-supported Army organizations. Thin client computing is currently an above-baseline service, funded by the requiring Army organization or mission command. Army organizations that maintain a non-NEC-supported thin client computing environment will coordinate with the NEC, upon end of life, to transition into the computing architecture provided by the NEC. Each NEC is permitted to operate no more than one thin client computing architecture. This architecture will be scalable to support multiple tenant missions.

f. Accountability.

(1) IT and computing resources account for a significant portion of an organization's budget. NECs may reference existing supply regulations (for example, AR 710–2) for guidance on IT resource accountability. The NEC's close coordination with the PBO assists the NEC in developing a sound asset management program. It is vital that the NEC be given prompt notification of the receipt of computing resources at the installation. This information assists the NEC in providing a more complete service to customers in the area of computing resources acquisition. With regular feedback from the PBO, the NEC can help ensure a customer's order is received in a timely manner. Once software and/or hardware is received, it is placed in the NEC's asset management and LCM 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 is to assist HQDA, field operating agencies, ACOMs, 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 five years.

(3) For information on the screening, redistribution, and disposal of IT equipment, refer to chapter 2 of this document for information on the 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 NEC maintains the accompanying license. If software is installed and accessed from a central server maintained by the NEC, the NEC maintains the license. If the hardware is installed and accessed as part of the installation server plan and is maintained by the NEC, then the NEC 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 and/or section's IMO maintains the license and issues the software to individuals using hand receipts. The NEC or 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.

g. Life-cycle management.

(1) The NEC's implementation of a strong 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 for guidance concerning the NEC'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 NEC, including purchase date, cost, vendor data, warranty data, and specific identifying data about the hardware or software itself, such as license and 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 senior IM official, IMO, IASO and the NEC. Other data are added, either initially or through the life cycle of the hardware or software, as the NEC 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.

h. Hardware and software control procedures.

(1) Once hardware or software has been received, the NEC, 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) The use of employee owned information systems and other non-DOD owned equipment within the Army enclave is prohibited. If allowed by exception, the equipment used must comply with Army IA requirements and have DAA approval prior to use, see AR 25–1 and AR 25–2. The use of employee owned information systems outside the Army enclave (for example, telework) must comply with paragraph 6–9, appendix B, and AR 25–1.

(3) When software is due for updating, the senior IM official and 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 https://www.acert.1stiocmd.army.mil/Antivirus/Home_Use.htm/.

(4) The NEC and senior IM official or 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). 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.

(5) All users will sign the Acceptable User Agreement that outline copyright infringement and the AR 25–2 punitive

measures for non-compliance. 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.

(6) Organizations require NEC 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.

i. Reutilization and 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. Hardware and software providing direct security protection to automation or telecommunications equipment systems that process classified information, or is designated under DODM 5200.01, 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.

6–14. Energy management of information technology equipment

a. In today’s office environment, after lighting, IT equipment uses the most electricity. To conserve energy and reduce the Army’s carbon footprint, energy-saving features must be used to their full advantage. CIO/G–6 is responsible for energy management for IT equipment within the Army and coordinates with ACSIM to provide cohesive energy management.

b. Energy savings can be realized by turning off equipment; however, the largest savings can be realized simply by putting computers, monitors, and other peripheral equipment (for example, printers, copiers, all-in-ones, and facsimiles) into a power save mode during periods of inactivity. Energy-efficient computers, monitors, and other peripheral equipment generally can enter sleep mode, which is a power-saving mode that allows the equipment to resume full-power operation quickly. This mode puts all data in random access memory, and the whole system goes into standby mode.

(1) Computers. After 30 minutes of inactivity, computers—desktops and laptops—will enter into sleep mode. The power options for the Army Golden Master will be set to put the computer to sleep in 30 minutes, and a group policy will be used to push this requirement out to ensure consistency.

(2) Monitors. After 15 minutes of inactivity, monitors and laptop displays will enter into sleep mode. The power options for the Army Golden Master will be set to put the monitor or display to sleep in five minutes, and a group policy will be used to push this requirement out to ensure consistency. In addition the monitors will be turned off at the end of the work day.

(3) Other peripheral equipment. After 30 minutes of inactivity, other peripherals such as printers, scanners, facsimiles, all-in-one devices, and copiers, will enter into sleep mode. When setting up new equipment, the NEC needs to set the appropriate sleep mode, before putting the equipment in service. For existing equipment, NEC personnel should update the equipment by setting the sleep mode for the designated time.

(4) Servers, storage area network devices, and other network infrastructure. These devices are not required to be powered off during periods of non-use.

6–15. Army Centralized Army Service Request System

a. The Army Centralized Access System (ACAS) provides an automated method for enabling units to request DISN services (for example, phone numbers, IP addresses for SIPRNET and NIPRNET, and so forth). This system is a custom-built Web site and database that consolidates the Army Service Request (ASR) processes (worldwide) and provides centralized ASR processing through an easy to use Web browser interface. All Regional Satellite Communications Support Centers will use the Joint Integrated Satellite Communications Technology (JIST) for Satellite Access Request (SAR) and Gateway Access Request input. Army will use ACAS for capabilities not included in JIST. NETCOM will work with JIST programmers to develop a feed from JIST to ACAS. Army users will use JIST to prepare SARs and Gateway Access Requests. When a user needs services from a WIN–T Regional Hub Node (RHN), JIST will open a link to ACAS and Army users will fill out that portion of the SAR or Gateway Access Request in ACAS. In ACAS, the RHN provision the requested services and will send the unit the necessary cut sheets.

Additionally, the SAR is also generated, and the necessary frequencies are sent to the requesting unit from either the Global Satellite Support Center or Regional Satellite Support Center. ACAS is currently operational on NIPRNET, only for training requirements.

b. ACAS is the standard application to request and generate SARs and ASRs for Joint Network Node and/or Command Post Node satellite communications (SATCOM) bandwidth authorization and connections to the Network Service Center-Training and RHNs. To generate an SAR or ASR, visit the ACAS Web site at https://www.acas.army.mil/.

c. This system is not available to all Army users; each user must be involved in the SAR and ASR request process of your unit or organization. Account requests will be reviewed and approved or rejected accordingly. Follow the instructions below to register:

(1) Open the ACAS site: https://acas.army.mil/.

(2) Login via the AKO authentication methods.

(3) If you have already registered and been approved, you will be automatically logged in. If not, you will need to select the unit, RHN, or organization that your account should be associated with.

d. The ACAS provides:

(1) Centralized data repository.

(2) Change tracking and audit log.

(3) Report generation.

(4) Integrated bandwidth scheduling.

(5) Alert capabilities.

(6) Standardized ASR document.

6–16. Information processing services

a. General.

(1) Within their service regions, Army NECs must offer an array of support services to a diverse user community. Continued growth in the use of technology increases the competition for NEC resources. This competition requires users to involve NEC staffs at the start of planning, if new or changing office automation requirements are projected. NECs 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 NEC office are carefully examined. NECs should suggest nontechnical alternatives when viable, such as changing processes. If the NEC cannot provide a needed automated solution, the NEC assists the customer in procuring the capability from other sources.

(3) NECs make every effort to respond to critical requirements. However, the ability of NECs to respond is affected by customer requirements. NECs 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, and so forth. 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 NECs 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) LAN.

(b) Gateways to communications service.

(c) System administration of common-user systems, such as email.

(d) Connectivity with DA systems.

(e) Soft switches and local session controllers.

(3) System analysis and programming support for system development, including:

(a) Assisting in performing feasibility studies and developing cost-to-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 NEC resources are unavailable.

(5) Security guidelines.

c. Systems support coordination. In providing support, NECs focus on integration and standardization that brings efficiencies to operations and increases customer satisfaction. NECs 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 ACOMs and installations without conversion, data loss, or re-keying. Army NECs must adhere to a common office automation product set in their service areas, as NEC 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.

6–17. Technical documentation

a. Documentation is the process of recording information produced by a software and/or 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. AR 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 at the top and bottom of each documentation unit.

e. ISO/ International Electrotechnical Commission (IEC) 12207: 2008 is an international standard adopted for use by DOD. It is 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.

6–18. Army Data Center Consolidation

a. The Federal Data Center Consolidation Initiative (FDCCI) is an OMB-directed initiative. The objectives of the FDCCI are: to promote the use of Green IT and thereby reduce the overall energy and real estate footprint of government data centers; to lower the cost of data center hardware, software and operations; to increase the overall IT security posture of the Government; and to shift IT investments to more efficient computing platforms and technologies. As required by OMB, Army has:

(1) Conducted an initial inventory (self-reported) of data center assets to provide a high-level understanding of the scale and size of data centers, IT infrastructure assets, and supported applications.

(2) Developed an initial data center consolidation plan to identify potential areas for consolidation, areas where optimization through server virtualization or cloud computing alternatives may be used, and a high-level transitioning roadmap.

(3) Collected a significant baseline inventory containing more detailed data to serve as the foundation for development of the final data center consolidation plan.

(4) Developed an executable data center consolidation plan that includes a technical roadmap and approach for achieving the targets for efficient infrastructure utilization, rack density optimization and consolidation.

b. The Army Data Center Consolidation Plan (ADCCP) is the Army response to the OMB FDCCI requirement to develop a plan to consolidate data centers. HQDA CIO/G–6, who serves as the overall Army ADCCP project lead on behalf of the Secretary of the Army, developed the plan. The ADCCP establishes standards and assigns responsibility for the migration of applications and consolidation of data centers. The effort will consolidate data centers and applications, provide enterprise hosting as a managed service, and improve the security of Army information assets.

c. The Army will accomplish data center consolidation through initiatives at the enterprise, command and/or data center owner and Army application portfolio management levels. Consolidation will continue based on lessons learned and analysis of the initial five-year plan. The ADCCP Execution Order (EXORD), pertinent reference documents, and other relevant background information are available on AKO in the ADCCP Public Folder at https://www.us.army.mil/suite/files/23122929. The ADCCP EXORD and its subsequent Fragmentary Orders establishes standards and assign responsibility for the migration of applications and consolidation of data centers.

d. In order to meet the Army's goal of 185 data center closures, the CIO/G–6, NETCOM and 7th Signal Command (Theater) have developed the installation approach to data center consolidation. The installation approach recommends an installation-level consolidation plan that provides opportunities to expedite data center closures through a collaborative effort. The Installation Approach utilizes the ADCCP Center of Excellence Discovery Teams more effectively by having them discover existing data center information: (utilized and available capacity, facility infrastructure, storage and network capacity) and application level data on an installation concurrently, allowing commands and owners to make more informed decisions to support consolidation of data centers on an installation. The Installation Approach recommends an installation-level consolidation plan that provides opportunities to expedite data center closures through a collaborative effort, and upon CIO/G–6 approval, will be implemented to best support the goals of data center consolidation. In addition to the installation approach, command-initiated data center consolidation will help to accelerate Army's goal of maximizing data center consolidation.

e. The following key tasks are delineated in the ADCCP EXORD and its subsequent Fragmentary Orders: establish application migration Centers of Excellence; coordinate enterprise hosting services; discover and rationalize and/or consolidate Army applications; migrate and virtualize Army applications; and track and/or report efficiencies. Requirements associated with these tasks are outlined below.

(1) General Requirements.

(a) Any location identified with two or fewer servers will be designated to close with a scheduled closure date automatically assigned in the ADCCP Tracking Tool six months from the date of identification. Within 30 days of that date, the owning command will notify ADCCP of the planned disposition for these assets. Further details on requirements can be found at https://www.us.army.mil/suite/files/23122929.

(b) Per AR 25–1, the following IT equipment will not be procured without a written waiver, granted in advance by the CIO/G–6: servers, voice switching equipment, racks, storage area network storage, matrix switches, optical storage systems, tape drive and storage devices, high-speed printers and mainframe and minicomputers. Data centers or server rooms are not to be constructed, renovated and/or leased without a written waiver, granted in advance by the CIO/G–6. Web-based waiver requests can be submitted at https://adminapps.hqda.pentagon.mil/akmg1w/index.html. Once approved by CIO/G–6, the request will be submitted to the DOD CIO for approval to obligate funds in accordance with Public Law 112–81 (National Defense Authorization Act for Fiscal Year 2012, Section 2867).

(c) Army commands, organizations and data center owners need to register all data centers in APMS and populate data center and application information in the ADCCP tracking tool (https://hqdadst.army.mil). Army data center inventory, closure, and application consolidation processes and activities are all inventoried and tracked through the ADCCP Tracking Tool.

(d) IT portfolio management mission area (segment) and domain (sub-segment) leads, commands, and application owners will jointly rationalize the entire inventory of Army applications. Application inventory must be reviewed and revalidated in order to retire applications that are rarely used or obsolete, and eliminate those that are redundant.

(2) ACOM, ASCC and DRU requirements.

(a) Provide quarterly reporting requirements in accordance with the ADCCP reporting schedule to meet DOD CIO, OMB FDCCI deliverables and Army senior leadership reporting in support of the ADCCP Quarterly Updates. Provide

and validate the current list of planned (through FY18) and completed (with general officer or civilian equivalent signed closure report) data center closures. In addition, ACOMs, ASCCs, and DRUs should use the ADCCP Tracking Tool quarterly to update and validate the Application Inventory Report, the Quarterly Data Center Update to the ADCCP Office Report, the Data Center Resource Report, the Data Center Closure Timeline Report and Command Resource Module (see the ADCCP EXORD for examples of these reports). The Command Resource Module requires funding and cost information for three fiscal years.

(b) Support data center discovery on specified installations when requested by the CIO/G–6 and ADCCP project office. Commands and data center owners will provide any pre-site visit requirements and support the on-site discovery activities of the ADCCP Center of Excellence Discovery teams.

(3) Data center owner requirements.

(a) Support data center discovery on specified installations when requested by the CIO/G–6 and ADCCP project office. Data center owners will provide any pre-site visit requirements and support the on-site discovery activities of the ADCCP Center of Excellence Discovery teams.

(b) Update and validate the Data Center Resource Report in the ADCCP Tracking Tool quarterly to support the command level validation of the Command Resource Module. This task applies to all data centers, except closed data centers, deployable or data centers operating in Operation Enduring Freedom. The Data Center Resource Report data will be reviewed quarterly at the CIO/G–6 ADCCP Quarterly Updates.

(c) Ensure tenanted application data is properly captured in the ADCCP Tracking Tool and supported by the data center.

(4) Application owner requirements.

(a) Identify, rationalize and categorize applications identified in data centers.

(b) Commands and organizations are required to submit justification to the ADCCP project office if the application or system rationalization yields less than a 50 percent reduction in applications.

(c) Update and validate the Application Inventory Report and the Applications Rationalization Results Report in the ADCCP Tracking Tool quarterly. These reports will be reviewed at the CIO/G–6 ADCCP Quarterly Updates.

6–19. Electronic document management

a. Electronic 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 organize 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 organization and computer industry standards.

(2) Is scalable over the entire organization 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 email.

(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. For more information on document security, please see AR 380–5.

(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).

6–20. 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.

(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 electronic 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 the Army CIO/G–6 Cyber Directorate Identity Management Division, SAIS–CB at 2530 Crystal Drive, Arlington, VA 22202.

Chapter 7
Telecommunications and Unified Capabilities

7–1. Network systems

a. Local area network (LAN) and wide area network (WAN).

(1) The NEC 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 NEC advises user organizations about procurement of LAN equipment.

(3) An organization must coordinate with the installation NEC and request a waiver prior to purchasing, installing and maintaining LAN equipment that will be operated separately from the NEC supported installation infrastructure. If the waiver is approved, the organization must coordinate with the NEC for connecting to and gaining access to the installation WAN.

(4) 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 NEC must give data to support a competitive procurement.

b. Wireless local area networks.

(1) Where wireless LANs are to be implemented, a thorough analysis, testing, and risk assessment must be done to determine the risk of information interception and/or monitoring and network intrusion, prior to installation of these devices. Only properly trained IA personnel can successfully determine these risk factors. IA personnel will have all training documented and meet all training requirements outlined in DODD 8570.01, reference (I). At a minimum, individuals who conduct risk analysis of wireless networks will have a relevant computing environment certificate and demonstrate a thorough understanding of FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

(2) Wireless LAN (WLAN) may be used as an extension of the departmental LAN or the common user installation transport network where fixed infrastructure connectivity is unavailable. A 10BaseT patch cable to the departmental LAN hub or the common user installation transport network area distribution node router provides the interface.

(3) Standard interfaces for WLANs are IEEE 802 series. WLANs operate in the 2.4 to 2.484 gigahertz and 5.743 to 5.830 gigahertz range. The DOD mandates that all WLAN devices used within the USP must be registered with the local spectrum management office. OCONUS use of the spectrum for WLAN is subject to host nation agreements and local command spectrum management policies.

(4) NECs analyze user needs to spot possible WLAN applications and help user organizations request WLAN equipment needed to meet requirements.

(5) Wireless networks needing remote or local access to the NIPRNET submit their requirement through the NIPRNET connection approval process.

c. Internet access via Virtual Private Network or Terminal Server Access Control System.

(1) A VPN is a secure way of connecting to a private local area network at a remote location, using the Internet or any insecure public network to transport the network data packets privately, using encryption. The VPN uses authentication to deny access to unauthorized users and encryption to prevent unauthorized users from reading the private network packets. The VPN can be used to send any kind of network traffic securely, including voice, video or data.

(a) A VPN gives remote access for authenticated Army users to their email accounts and allows access to the Internet as needed for conducting official Government business.

(b) VPNs should be the primary remote access method. Terminal Server Access Control System (TSACS) should be used at a minimum, as it is considered obsolete. All accounts which were not deemed critical mission have been deleted. The CONUS–TNOSC no longer accepts or opens trouble tickets for TSACS. Redirection for management and authentications should be by the local NEC.

(2) TSACS gives remote access for authenticated Army users to their email 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 non-authorized access to the IP router network. Dial-in service is given through local terminal servers or over remote 1–800 service.

(a) Army ACOMs 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 email and send data over NIPRNET. NIPRNET can handle data up to unclassified but sensitive.

(b) The installation NEC, 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/). Once the process is complete, the user may dial

into TSACS and access email servers via NIPRNET. TSACS phone numbers and OCONUS numbers may be obtained from the TSACS Web page. Some OCONUS numbers are not published, because of other considerations, and may be obtained from the local NEC 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.

(c) NECs and service providers help to better manage the dial-in access by:

1. Obtaining local dial-in access numbers for temporary duty locations, before going on temporary duty. Access numbers for locations visited may often be programmed into a laptop.

2. Helping users in setting up a laptop computer to limit online time. The laptop may be set up to first view email headers, so users select ones to download. Messages are worked off-line, and users re-log on to send responses.

(d) Exceptions to this are those approved COI networks and non-Army enterprise.

d. Requests for wired and wireless telephone and telephone-related service.

(1) BASECOM funding. The supporting NEC will be the focal point for all common-use BASECOM on the installation or the supported area and the initial focal point for tenant organizations and activities to obtain support for unique BASECOM requirements not provided in the C4IM Service List. BASECOM falls into one of four categories that are funded on a reimbursable or non-reimbursable basis, depending on whether the service requested is on the C4IM Services List. If an Army user is in a location where there is no NEC support available, the user will coordinate procurement directly with the NETCOM. A lack of NEC support does not negate the requirement to procure devices and service through the NETCOM or the use of the BPAs.

(2) Service requests. NECs will submit BASECOM service requests to NETCOM (G5) with a courtesy copy provided to the respective Signal Command (Theater) office. NETCOM will obtain BASECOM telecommunications service requests - such as local central office trunks, commercial business lines, and foreign exchange trunks and/or lines via consolidated local service contracts that are competed among interested service providers. NETCOM will satisfy requirements for BASECOM local leased telephone services through BASECOM consolidated contracts and wireless requirements via BPA contracts. NECs will obtain O&M for installation telephone plants through NETCOM. Those interested in acquiring local leased telephone and telephone-related services should email the point of contact at the following email address: usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil. If the existing consolidated contract cannot be used to satisfy the requirement, NETCOM will competitively award a new contract to satisfy the requirement. NETCOM will determine whether an existing consolidated contract will be modified or if a new contract is required to fulfill service requirements.

(3) Work orders. NECs will submit a DD Form 1367 (Commercial Communication Work Order) against an existing consolidated contract, when acquiring telecommunications services for the installation. NEC ordering officers, appointed by the NETCOM contracting officer, are authorized to place orders up to the dollar limit defined in their appointment orders. NECs will submit all orders over the NEC ordering officer's threshold to the NETCOM contracting officer.

(4) Wireless. NETCOM G–3 is the exclusive point of contact for procuring wireless services and devices in accordance with UC APL multi-function mobile devices, https://aplits.disa.mil/processAPList.do. When procuring wireless services and devices, all Army users are required to utilize the ordering procedures established by NETCOM and procure the services from established BPAs.

(5) Central procurement. In the event that a desired PDA or wireless service is not on the Army's BPAs, a request for exception to procure from other sources will be submitted to NETCOM. The exception will be evaluated on a case-by-case basis, and no action will be taken to procure the services from other sources until approved by NETCOM. Use of the Army's BPAs will ensure the requirements are being fulfilled using the best available option for service and pricing.

e. Secure wired and wireless communications equipment. This term encompasses all of the devices used to secure telephone communications, to include, but not limited to: secure telephone equipment (STE), secure cellular (and other secure mobile devices), and secure wireline terminals.

(1) Equipment requirements. Secure phone communication is critical to most agencies and units and should be used as needed to assure voice and data communications security. Secure wireless devices will communicate securely with any device that is future narrowband digital terminal-compatible, such as the secure wireline terminals and upgraded STEs. These secure devices may only be used for classified conversations or transmissions, when the devices are loaded with a National Security Agency-approved Type 1 key and only to the level designated by that key.

(2) Use with standard telephone. Secured wired and wireless devices can be used with standard telephone equipment, international maritime satellites (INMARSATs), PCs, and unclassified fax machines to provide security that is not present in those unsecured devices. Only National Security Agency-approved secure wired and wireless devices will be used to encrypt data from portable computers, when operating on any telephone network.

(3) Secure key. Secured wired and wireless devices are unclassified, controlled cryptographic items without the personal identification number (PIN) or crypto ignition key loaded or in place; however, with the PIN or crypto ignition key in place, the devices assume the level of the key and may not be left in unattended environments except for specific circumstances allowed by AR 380–40 (that is, approved vaults and sensitive compartmented information

facilities). Secure wireless cellular devices will be procured via normal communications security (COMSEC) channels. Organizations may submit inquiries and requests to acquire secure wireless service to usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil.

(4) Environment. When talking at a classified and/or sensitive level, personnel will observe procedures required for secure environments, to include maintaining distance from uncleared individuals. The security authority should implement a common-sense approach to acoustic security concerns.

(5) Notification. Organizations conducting classified or unclassified operations will notify all attendees in advance of prohibitions or limitations on carrying such devices into the operational area.

(6) COMSEC managers will take the appropriate measures to secure all communications with approved products and devices to the level of security classification of the information to be transmitted over such communications equipment, in accordance with AR 25–2 and AR 380–40 updates.

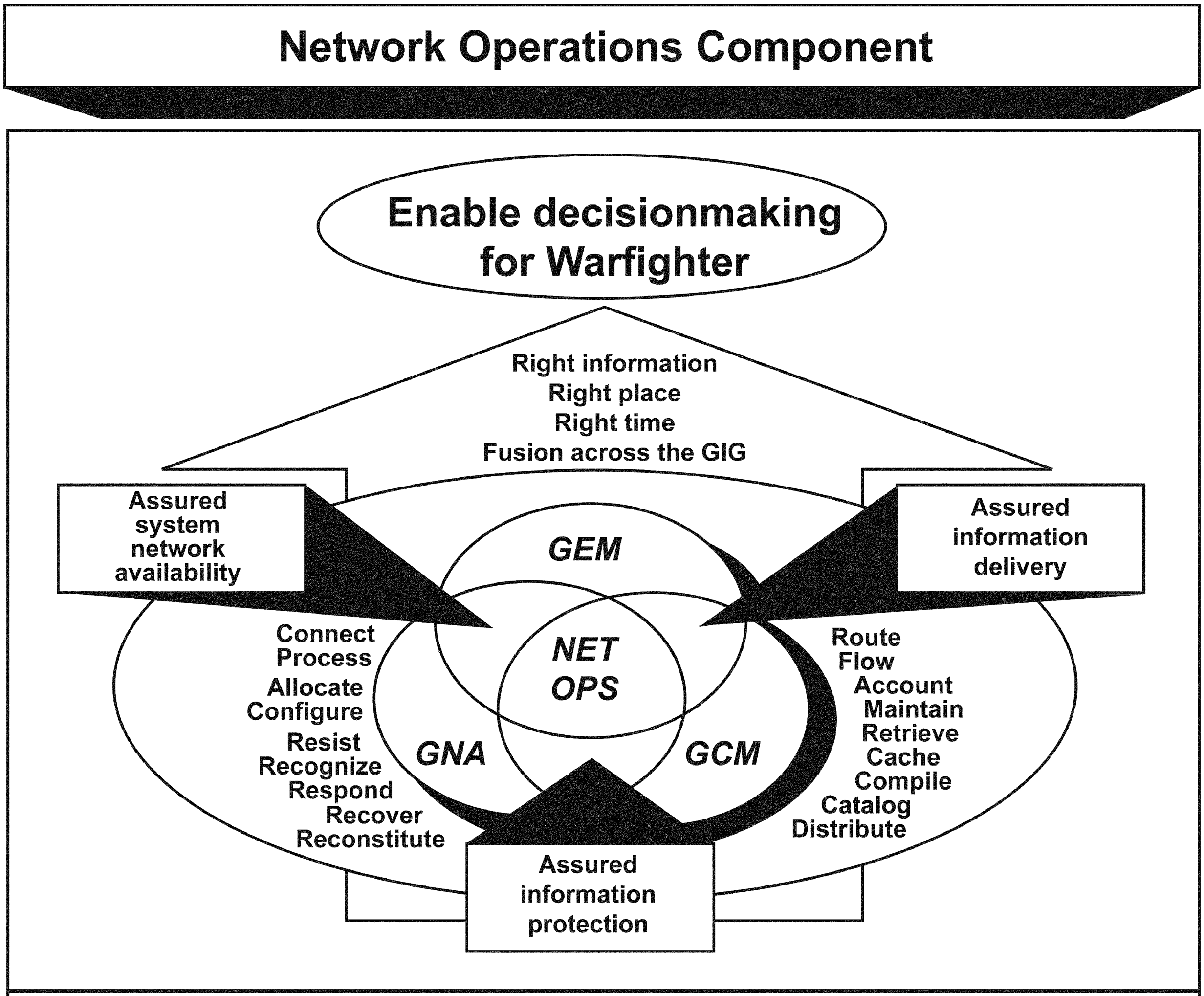
(7) All wired and wireless networks require the use of wireless intrusion detection systems (WIDS), capable of location detection of both authorized and unauthorized wireless devices. All systems will provide 24/7 continuous scanning and monitoring. Appointed NEC personnel will respond to all WIDS alerts, maintain reports and document actions taken. WIDS logs and documented actions will be maintained for a minimum of one year.

(8) Backdoor Access. All wireless solutions will be acquired and/or configured to preclude backdoor access into the Army's LANs. Systems must meet all information assurance vulnerability message compliance requirements.

7–2. Network operations

a. Network operations (NETOPS) are the operation and management of the LandWarNet. NETOPS supports the broader operational discipline of cyberspace operations which includes the full-spectrum operations required to defend the LandWarNet and ensure freedom of action on the network. LandWarNet is the combination of information 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 LandWarNet as the Army part of the GIG (the organizing and transforming construct for managing IT throughout the DOD). Single-authority operation and management of the LandWarNet 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 ensures information dominance, enables command speed for Warfighters, and establishes a technical framework to create a network common operational picture. Figure 7–1 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.



GCM	GIG content management	GNA	GIG network assurance
GEM	GIG Enterprise management	NETOPS	Network operations
GIG	Global information grid		

Figure 7–1. 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 SSO plug-and-play capability.

(2) Correctly show total and integrated situation awareness of the LandWarNet.

(3) Expect impacts on LandWarNet of varying systems and operational contingencies.

(4) Redirect and reallocate LandWarNet resources in near real-time to support Army response to crisis anywhere in the Army information structure operational area.

(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 area of responsibility, 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 network common operational picture for their part of the GIG.

(1) A network common operational picture 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 network common operational picture is an integrated capability that receives, correlates, and displays a view of voice, video, and data telecommunications networks, systems, and applications at the installation and/or tactical, region, theater, and global levels through the installations and/or 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. The network common operational picture at each level reflects status, performance, and IA. At a minimum, the network common operational picture includes telecommunication, system, and application fault and performance status, as well as significant IA reports, such as network intrusions or attacks.

e. The tactical portion of the LandWarNet 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) Army Cyber Command/2d Army, oversees Army NETOPS and cyberspace operations through NETCOM and subordinate theater signal commands.

(2) NETCOM, through its Army theater signal command, supervises the operation and maintenance of the Army's portion of the GIG in theater.

(3) 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 J6, 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 required to monitor 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 LandWarNet 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/MC GOSC 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 and managed with approved 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 and logon using PKI or CAC.

(6) Single, integrated help desk or "one-stop" problem reporting and resolution.

h. Information infrastructure management focus areas are identified to highlight key concepts needed to achieve the Goal 3 vision and effectively manage the LandWarNet as an enterprise. A high-level description of each area is provided below.

i. The configuration management process covers all aspects of the information infrastructure configuration. The Army controls introduction of new services and functionality to the end-user community, without disrupting existing services by the process. Configuration management is also the process required to ensure compliance with operating and security policy.

(1) The LandWarNet Technical Configuration Control Board is the primary organizational entry point into the

change process. NETCOM, in conjunction with the LandWarNet Technical Configuration Control Board, will manage the change process.

(2) The configuration management process solicits input from the users and allows the supporting organizations to glean the best of these items.

j. The 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.

k. AR 25–1 requires a "networthiness certification" process that identifies and continually refines required support for a C4IM systems and applications, particularly in the areas of supportability, interoperability, sustainability, and security. The process ensures that a C4IM system and/or application does not adversely impact the network and that it is sustainable through its lifecycle. Information on the networthiness certification process and other applicable documents are available on AKO at the networthiness homepage.

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 configuration management 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, IP 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 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 LandWarNet.

(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 7–1 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 7–1.
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, ACOMs, 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. 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 Installation Management Agency 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. Table 7–2 shows the levels used in this document and the organizations identified on that level. Each of the entities are described in detail below:

Table 7–2.
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, ACOM, Army Cyber Operations and Integration Center
Theater	DISA regional network operations and security centers, theater network operations and security centers, regional computer emergency response team, NETCOM (OCONUS)
Regional	Network support center, regional director, NETCOM (OCONUS)
Installation/tactical	NEC, supporting signal unit

7–3. Spectrum operations

a. AR 5–12 governs Armywide spectrum management. 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 DODI 4650.01. The Army is obligated to comply with these policies unless waived by the Army Spectrum Manager. For 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 agreements made with the host nation. Additional spectrum related policies based on combatant command tactical control, operational control, or administrative control command relationships will apply in OCONUS locations.

b. NECs coordinate, plan, program, and fund for the management of the electromagnetic spectrum as outlined in AR 5–12, the C4IM Services List, and this publication. The NEC is responsible for ensuring emitter usage on the installation complies with AR 5–12 and operates within the scope of the specific frequency assignment. The installation NEC 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.

(2) Frequency assignment and utilization as outlined in AR 5–12, relevant Combatant Command guidance, and applicable U.S.-host nation bilateral agreements.

(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 five years. OCONUS, Army records require a similar review under Allied Communications Publication 190(C) or per combatant command directives.

(4) Clearance for electronic attack operations per AR 5–12.

(5) Radio station identification, international call signs, and other non-tactical call signs per AR 5–12.

(6) Coordination with other installation directorates and tenant activities concerning spectrum-dependent equipment per AR 5–12.

(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) Coordination 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.

(11) Ensure that the installation frequency coordinator is trained through a military department spectrum managers course. 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 and/or 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 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 radio frequency emitters are for official Government use.

(l) At a minimum, each antenna tower should have an annual technical inspection per AR 500–3 and AR 750–1.

(m) Register the use of non-licensed wireless devices in accordance with AR 5–12.

7–4. Telecommunication systems

a. Local leased base communications services.

(1) 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, 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.

(2) BASECOM services encompass the following types: centrex service, direct in-dial/ direct out-dial trunking, two-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 and/or 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.

(3) 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 Federal Communications Commission. Services can be acquired using a communication service authorization and commercial communication work order, or other contract format, per the FAR and DFARS, as the contractual vehicle. FAR part 12 is incorporated into solicitations as a preference, in order to streamline the acquisition process.

(4) 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 and DFARS. The ATD works closely and directly with the NECs' appointed telecommunications coordinating officers to facilitate the acquisition of local lease telecommunications services. Mailing address and phone numbers for ATD: Commander, U.S. Army Network Enterprise Technology Command, ATTN: NETC–EST–T, 2133 Cushing Street, Fort Huachuca, AZ 85613- SBU 879–8679/2369/8101 or commercial (520) 538–8679/2369/8101.

(5) Additional information on procedures for acquiring local leased BASECOM services are contained in the ATD's BASECOM letter of instruction. The letter of instruction can be found on the ATD's restricted Web site. Individuals with a need to know can obtain access to the Web site by sending an email to: ato_automation@netcom.army.mil/.

(6) Requests for leased commercial phone service are submitted by memorandum or local service request to the installation NEC (other areas, such as Europe, require DA Form 3953 (Purchase Request and Commitment)). The memorandum or local service request must be reviewed by and have the original signature of the unit's telephone control officer (TCO), before submission. User should submit requirements to the NEC at least 90 days (120 days for 1–800 service) in advance of required service date. This will allow the NEC to deal with such issues as cable availability and workload management. The NEC should be advised as soon as a requirement is identified.

(a) If the user needs service such as Networx, calling cards, 800, and so on, it is ordered via the Defense IT Contracting Office (DITCO). The NEC initiates a request for service on behalf of the customer.

(b) Activities must provide funds for the request.

(c) The following information must be included in the memorandum:

1. A statement that "Funds are available for this request."

2. The fund site 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.

3. The original signature of the initiating activity's fund certifying officer, to include the phone number, email address, complete mailing address, unit name, office symbol, street, building, room, and stop numbers.

4. A thorough justification for the requirement.

5. Point of contact name, phone number, email address, complete mailing address, unit name, office symbol, street, building, room, and stop numbers. Point of contact must be thoroughly familiar with requirement and available to answer any questions.

6. 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.

7. Type of equipment (phone or modem) and any special configuration requirements.

8. 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.

9. The type of service. Types of leased commercial service and additional information required for each are:

a. Provisioning of local leased commercial services with Networx long-distance services required on phones, or local voice, data, or video teleconferencing (VTC) circuits such as toll free dedicated and/or switched, voice on net, calling cards, long distance dialing, (local and international) and/or frame relay.

b. Telephone calling cards. Provide the number of cards required. (See AR 25–1 for authorized usage and management control.)

10. Local leased commercial phone service (voice). Give number of lines, including area code and exchange for the local calling area required.

11. Off-premise extension circuits. Give number required.

12. Local-leased commercial phone service (data). Give type and bandwidth of circuit (56 kbps up to OC192) and number of circuits required. Bandwidth off the Networx contract is 56 kbps up to T3.

13. Integrated services digital network (ISDN) service. Give number of ISDN basic rate interface or ISDN primary rate interface required.

14. 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 six months. Provide the plain language address message addresses for the initiating activity and the initiating activity's ACOM.

15. Cellular phone service activities must provide estimates of usage as follows:

a. 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.

b. Cellular phone equipment and services may be procured through normal procurement procedures.

(7) Coordination is important to successfully installing a local leased service. Information regarding the service should be shared with the NEC. The NEC should be contacted anytime there is any change in the status of a local leased requirement.

(8) 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.

(9) An in-effect report is submitted by the NEC, when service has been installed and is working. The NEC is informed by the point of contact 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.

(10) The TCO performs these functions for leased commercial phone service:

(a) Reviewing and signing requests for leased commercial phone service.

(b) Keeping a current list of leased commercial phone service for their activity.

(c) Completing the biannual review and revalidation of all leased commercial phone service and returning it to the NEC by the suspense date. The review and revalidation requires the following:

1. A current and thorough reason for keeping services. A memo should be sent to the NEC requesting disconnection of services no longer required.

2. Current funding information, including the original signature of the funds certifying officer.

3. The original signature of the TCO.

(d) Picking up and signing for all phone calling cards.

(11) For information on the billing of telecommunications systems use, including cable television (CATV), see AR 25–13.

b. Telephone services.

(1) On-installation telephone services. This paragraph outlines special considerations for phone services provided to activities that reside on an Army installation.

(a) The installation NEC program 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. Appropriate signal command will ensure installation NEC'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 chapter 6 and section II of the glossary 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, ACOMs or other organizations and Government agencies, and procuring contractual services.

2. Class A–2 and C phone service is provided to 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 non-reimbursable 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 NEC may provide support for the requirement. In such a case, a host and/or tenant communications support agreement is executed. This agreement may be between the NEC 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 non-reimbursable 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 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 of 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 non-reimbursable 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 non-appropriated 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 6211. 02D for authorized use of the SBU by contractor personnel.

3. When official phone service is authorized, the NEC 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 NEC, 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. ACOMs 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 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 paragraph C–3).

(2) 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 NEC 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 Cadet Command.

1. The educational institution often provides on-campus phone service supporting the ROTC detachment and Junior ROTC instructors.

2. All U.S. Army Cadet Command (USACC) recruiting elements not on an Army installation will be provided services centrally from the USACC Headquarters.

3. The USACC may work within the NEC, NETCOM, DISA, General Services Administration, or direct with Networx providers for services. These services might include on or off net from a nearby Army installation. All services will be subject to reimbursement by the requesting USACC. All available services, including Networx, are considered before approval of commercial services.

c. Video services.

(1) Defense video services-global. Defense video services-global (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 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.

(2) General. 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 service delivery point (SDP). The DISN Switched and/or 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.

(a) Any VTC session that has been cancelled, time has been adjusted, rescheduled, or ends earlier than scheduled will contact DISA to return any unused minutes. DISA will be notified of the release of the minutes.

(b) Use the DISN Video Services Web address, https://dvsops.scott.disa.mil/dvsws, and login to alter your reservation.

(c) Call the DISN Global Support Center – DVS at Commercial (614) 692–4790, Toll Free Commercial (800) 554–DISN (3476), Global SBU (510) 376–3222, SBU (312) 850–4790.

(3) Interoperability with Government video teleconferencing facilities. The DVS–G video services interoperate with Government VTFs with multiple central processing equipment configurations, ranging from desktop and roll about systems, to fully equipped studios.

(4) Video conference reservations. 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.

(5) Other. Connections to other networks (through video hubs) include:

(a) Networx.

(b) Global commercial phone system.

(c) The service provider (global business video service).

(d) Sprint meeting channel.

(e) Tactical and/or deployed users of the DISN transmission system.

(6) Commercial services. 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.

(7) Performance monitoring. Government facilities will monitor the status and performance of the DISN video services and resources through the TNOSC. Video services management includes fault management, accounting management, performance management, and security management.

(8) Video hubs. 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. NECs may also own and operate video hubs and/or bridges at the installation for

both classified and unclassified multipoint VTCs. These devices will be registered with Defense Video Services (DVS) as multipoint control units. This enables VTFs on the installation to participate in both DVS conferences and non-DVS multipoint conferences, without being registered with DVS.

(9) DISN video services support. 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://www.disa.mil/disnvtc//.

(10) NEC-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 International Telecommunications Union-Telecommunication Standards Sector (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. All new DOD procurements for VTC equipment should be purchased through CHESS and conform to industry standards which ensures devices (including video) are interoperable.

(a) The DOD recognizes Federal Telecommunications Recommendation 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.

(b) 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 six frames per second and decoding at a minimum of 7.5 frames per second.

(c) The DVS network is covered by Federal Telecommunications Recommendation 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 and/or collaboration. It should be noted that the other VTFs conducting a conference may not support the advanced capabilities.

(11) Defense Video Services capabilities.

(a) 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 the type(s) of service needed and submit a completed and/or signed access approval document, a copy of your authority to operate or interim authority to operate, 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://www.disa.mil/Services/Network-Services/Video/DVS–G.

(b) 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.

(c) 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, Networx switched service, and SBU Voice. CJCSI 6211.02D provides guidance on use of the SBU Voice, noting that it is the first-choice non-secure DOD inter-installation telephony service (voice, dial-up data, and dial-up video) network and should be the primary communications means for special command and control, command and control, and non-command and control users.

(12) User operated desktop VTC.

(a) All desktop VTC units must comply with Corporation for Open Systems VTC profile standards.

(b) 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.

(c) Along with the basic VTC standards described above, desktop VTC units should also comply with ITU–TSS standard T120 data protocols for multimedia conferencing.

(13) Getting connected to the DVS network.

(a) Submit a request for service (RFS) or telecommunications service request to start your transmission (instructions for completing an RFS may be found in DISA Circular 310–130–1).

(b) Obtain DVS hub service and a site ID by contacting the appropriate theater video operations center (table 7–3).

Table 7–3.
Theater video operations center contacts

Location	Contact numbers
CONUS, DCCC - DVS	Phone: commercial 614–692–4790; toll free 800–554–3476; global SBU 510–376–3222; SBU 312–850–4790.
Europe, DISA EU52	Phone: commercial 011–49–711–68639–5260/5840/5445; SBU 314–434–5260/5840/5445. Email: vtcopseur@disa.mil. Fax: commercial 011–49–711–68639–5312; SBU 314–434–5312.
Pacific, DISA PC22	Phone: commercial 808–472–0223; SBU 315–472–0223. Email: vtcopspac@disa.mil. Fax: commercial 808–472–3838; SBU 315–472–3838.
Southwest Asia, DCCC–DVS	Phone: commercial 614–692–4790; toll free 800–554–3476; global SBU 510–376–3222; SBU 312–850–4790.

(c) For unclassified, complete a site registration as indicated online. Download the "Authority to Connect Request." Download the "Connection Approval Process."

(d) For classified, complete a site registration as indicated on-line. Download the "Access Approval Document." Download annex F.

(e) For tactical users, download the tactical site registration as indicated.

(14) 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 email 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 email 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.

d. Non-tactical radio systems.

(1) Land Mobile Radio Program. Army non-tactical land mobile radio (LMR) systems provide wireless base support 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. The primary users of LMR are emergency response personnel, including installation military police, fire departments, and medical personnel. LMR also enables installations to communicate and work cooperatively with nearby Federal, Defense, State, and local activities supporting homeland security and public safety missions. LMR solutions will be either trunked or conventional.

(a) 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.

(b) 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.

(c) The NEC:

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 user organizations concerning procurement of LMR radios and peripherals.

3. Submits request for frequency assignments and trunking certification from the appropriate DOD Area Frequency Coordinator or Army Frequency Management Office – CONUS (for CONUS NECs) or from the appropriate ASCC G–6 when overseas – in accordance with AR 5–12.

4. Ensures installation POM justification language includes LMR system operations and maintenance requirements, including the need for a system administrator and/or manager.

5. Coordinates, orders, and manages connectivity to repeater sites and dispatch consoles, as necessary.

6. Establishes local policies and procedures for tenant and/or supported organizations that use LMR services that provide – at a minimum –annual inventory reports to the NEC for accountability of radio equipment and maintenance of cryptographic security for all radio COMSEC, see AR 380–40.

7. Ensures that any radios are de-programmed, before being turned in to the DRMO by a tenant and/or supported organization.

8. Provides system documentation to the Product Director, LMR for all LMR infrastructure and equipment acquired outside the Product Director, LMR office. These reports should be submitted to Product Director, Land Mobile Radio (SFAE–PS–TS–LMR), 9350 Hall Road Building 1445, Fort Belvoir, VA 22060.

9. Reports unfunded outstanding LMR requirements to the Signal Brigade or Theater Signal Command. Outstanding LMR requirements include unresolved reports of persistent critical failures, non-compliance with DOD and Army policies regulating LMR, and requirements for compliance with domestic or international laws.

(d) 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 NEC must make every effort to furnish data to support a competitive procurement.

(e) Product Director, LMR is the Army program office responsible for Army acquisition, installation and modernatization of non-tactical LMR systems. This equipment includes LMR infrastructure for trunking and conventional systems that comply with DOD and Army mandated standards, including the Association of Public Safety Communications Officials P25 interoperability standard and Advanced Encryption Standard. The Army LMR Program provides spectrum efficiencies by executing the migration of Army posts, camps, and stations to narrowband frequencies as mandated by the National Telecommunications and Information Administration. Product Director, LMR maintains a repository of LMR infrastructure.

(2) Other Army radio systems.

(a) Coordination with the installation NEC 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 may be authorized only 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 must be assured before procurement action is started, per AR 5–12 and this paragraph.

(c) All U.S. Army installations within CONUS have high frequency radio systems provided specifically by the Army CONUS High Frequency Radio Program. This high frequency 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 NEC supervises:

1. Operation and maintenance of the system.

2. Communications security support for the installation Army CONUS high frequency radio station and equipment.

(d) The Army Military Auxiliary 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 and 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.

7–5. 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 and/or 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 and/or activity commanders may approve emergency calls or system use. (See AR 25–13, 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 25–13, 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; you may obtain legal advice before taking action.

d. The NEC 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 25–13.

7–6. Satellite communication systems

a. INMARSAT service. The policy for INMARSAT is located in AR 25–13.

(1) The INMARSAT satellites network gives users a multiservice satellite capability.

(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, and 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 to 128 kbps. The INMARSAT Broadband Global Area Network (BGAN) service is now available globally, delivered through three INMARSAT–4 satellites. BGAN is based on an IP media sharing construct.

(a) BGAN is accessible via a series of small, lightweight satellite terminals, providing performance options to suit different operational needs.

(b) Standard terminals are highly portable and can be used both indoors and outdoors.

(c) Vehicular systems comprise an interior terminal and a discreet tracking antenna, which is mounted on the vehicle roof.

(d) BGAN service can also be billed on a per minute or per megabyte basis which may result in cost savings.

(4) For the operational need statement (ONS), prepare and submit an ONS for approval per AR 71–9, before attempting to purchase and commission INMARSAT terminals.

(a) The requester receives approval from the ODCS, G–3/5/7 to purchase and commission the specified number and type of INMARSAT terminals. Requesting organizations must prepare a DISA Form 772 (Telecommunications Management System) for entry of their INMARSAT requirement into the satellite database (SDB).

(b) After the owning organization obtains the ONS approval letter from HQDA, the terminals must be commissioned through NETCOM, 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). Submit the ONS approval memo from HQDA, to NETCOM, ATTN: NETC–G34, Greely Hall, Building 61801, Suite 1511, 2133 Cushing Street, Fort Huachuca, AZ 85613–7070, fax: SBU 879–0766.

(c) Once the terminal(s) are commissioned and the phone number(s) or INMARSAT mobile number(s) are assigned and received from NETCOM, the user(s) must coordinate through the local NEC for submission of telecommunications requests 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 through 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. To avoid bills at the full commercial rate, and to minimize the potential for unpaid bills, end users of INMARSAT services must ensure that INMARSAT calls are placed through the appropriate land Earth station as directed by the ISP at service activation, and subsequently, by DISA upon award of the airtime contract. ACOMs and organizations must ensure that their terminals are properly enrolled through DISA, before anyone is allowed to use the terminal. For more information on this step of the process, contact NETCOM.

(5) When an organization no longer needs INMARSAT service, that organization must terminate its financial and legal responsibilities 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 telecommunications request to change DITCO enrollment information, or submit a discontinue telecommunications request 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 telecommunications request or the discontinue telecommunications request becomes effective. For more information on this step of the process, contact NETCOM.

(6) INMARSAT can be contacted by telephone at 011–44–207–728–1777.

b. Enhanced Mobile Satellite Service (Iridium). For policy on the use and acquisition of Iridium, refer to AR 25–13.

(1) Enhanced Mobile Satellite Service (EMSS) or Iridium provides users with a handheld satellite terminal. The terminal can be used both inside and outside; inside with the fixed mast antenna installed; and outside with the antenna pointing towards the sky without obstructions. The terminal accesses one of 66 satellites. DISA administers the EMSS program. Iridium is the only DOD-approved handheld satellite system.

(2) Terminals are purchased through DISA or DITCO via NETCOM and are spectrum certified by a completed (stage 4) DD Form 1494. Iridium users must purchase the handset with the secure module and/or sleeve. Organizations requesting Iridium terminals should follow the ONS procedures outlined in AR 25–13 and AR 71–9. Requesting organizations should prepare a DISA Form 772 for entry of their EMSS requirement into the SDB.

c. Validated satellite communication requirements and the satellite database. Prior to submitting a SAR for military or commercial SATCOM access, units must have a validated SATCOM requirement in the SATCOM Database. The requesting unit completes DISA Form 772 for their 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 ODCS, G–8. The ODCS, G–8 submits the form to the Joint SATCOM panel administrator who checks the form for completeness and enters the submission as a SDB requirement candidate. The Joint SATCOM panel administrator then presents the requirement to the Joint SATCOM panel for approval. In conjunction with the submission of the DISA Form 772, the requesting unit completes DISA commercial satellite team's circuit switched service (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 telecommunications request through proper channels. Telecommunications request 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 point of contact is SBU 879–8024 or commercial (520) 538–8024.

d. Global Positioning Service and Precise Positioning Service. The procedures to prepare and submit an ONS for approval in AR 71–9 are to be followed by U.S. Army units that have candidate special requirements to acquire Global Positioning Service (GPS) or Precise Positioning Service special-application or common user equipment for which the using unit does not have authorization in an approved table of organization and equipment (TOE) or table of distribution and allowances (TDA). These procedures are necessary to satisfy the policies of AR 70–1, and AR 25–1 and ensure that any spectrum dependent equipment requested has the appropriate J/F 12 number in order to operate in both CONUS and OCONUS.

(1) For additional assistance and product information to refine the requirement and develop the need statement, the requesting unit should contact the Army Product Director for GPS: U.S. Army Project Director, GPS, SMC/CZA, 2435 Vela Way, Suite 1613, Los Angeles AFB, CA 90245–5500. The Army Project Director, GPS Web site is located at https://gps.army.mil/.

(2) Upon receiving the approved ONS, the requesting unit arranges for acquisition of the needed equipment through the Army Project Director, GPS. The requesting unit must identify a valid fund cite and responsible billing addressee in order to initiate the acquisition process. The user submits his request for waiver through the Army acquisition executive to the OSD CIO in accordance with CJCSI 6130.01D.

e. Equipment and services for other commercial satellite communications. The procedures to prepare and submit an ONS for approval in AR 71–9 are provided for U.S. Army units that have candidate new requirements for military or commercial SATCOM services and/or user terminal equipment. These procedures are necessary to satisfy the policies of AR 70–1, AR 5–12, and CJCSI 6250.01D.

(1) For assistance and information to accomplish this assessment, the requesting unit should contact the PM for WIN–T, Commercial SATCOM Terminals Program (CSTP) office, SFAE–C3T–WIN, 6010 Frankford Street, Aberdeen Proving Grounds, MD 21005–1848.

(2) 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 and/or lease of equipment and to lease or enroll for commercial satellite access resources.

(3) 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 to the U.S. Army Spectrum Management Office, to obtain a certification of spectrum supportability of equipment through the National Telecommunications Information Administration. If the commercial SATCOM terminals are used by DOD entities, the acquisition manager must use the J/F 12 number, issued in the Army Satellite Database, to access any DOD SATCOM Service. (J/F 12 numbers are only issued after a completed DD Form 1494 is certified.) Prior to Milestone B in the acquisition process, acquisition managers should allow 12 to 24 months to complete the DD Form 1494 process through Stage 4 (operational) and obtain the appropriate J/F 12 number. 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.

(4) Before the commercial SATCOM terminal equipment is operated to accomplish a required satellite communications mission, the using unit assures registration of a Chairman of the Joint Chiefs of Staff-approved SATCOM access requirement for the mission in the Satellite Database, under the provisions of CJCSI 6250.01D. Upon receiving the approved ONS from DAPR–FDC, the unit may apply for Satellite Database registration by preparing and sending DISA Form 772 (TMS–C), SATCOM Requirement Request through the ACOM level to the Joint Staff's Joint Military Satellite Communications Panel Administrator for approval.

(5) It is OSD policy that all commercial SATCOM will be leased through the DISA using the GSA Future COMSATCOM Service Acquisition vehicle to obtain the lower cost per bit that contract provides. It is Army policy that units and organizations procuring commercial SATCOM will go through NETCOM for visibility purposes when purchasing COMSATCOM from DISA. The voice number for a NETCOM point of contact is SBU 879–8024 or commercial (520) 538–8024. Units or organizations not using DISA to procure their commercial SATCOM must first obtain a GIG waiver (See paragraph 7–9).

7–7. Long haul and deployable communications

a. Long-haul services.

(1) Defense Information Systems Network. 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. This transmission is integrated with military and commercial leased communication satellites, switched voice and data services, bandwidth managers, and teleconferencing services.

(a) Sensitive But Unclassified Network Voice.

1. The SBU Voice (formerly DSN) is the primary information transfer network for DOD and is a major subset of the DISN. The SBU Voice provides the worldwide voice, secure voice, data, facsimile, and video teleconferencing services for DOD command and control elements, their supporting activities engaged in logistics, personnel, engineering, and intelligence, as well as other Federal agencies.

2. SBU Voice is under the operational direction and management control of the DISA.

3. To order SBU Voice usage and precedence service, see the subsequent paragraphs below.

(b) DISN IP router service.

1. The NIPRNET connects several LANs and users through the use of routers and switches, 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, file transfer protocol, secure shell, hypertext transfer protocol (HTTP), and simple mail transfer protocol (SMTP). The NIPRNET provides access to the Internet through the use of gateways. Email can be transferred to Internet users, since the NIPRNET mail addressing system is recognizable to the Internet.

2. Remote NIPRNET access can be accomplished using VPN connections. Communications servers have modem banks that are connected to DISA routers, allowing modem users to access the NIPRNET. For information on how to obtain access, see the network information home page at https://www.nic.mil/.

3. Deployed U.S. forces can access the NIPRNET through the use of the Integrated Tactical-Strategic Data Network.

4. All requirements for NIPRNET must be properly registered, per CJCSI 6211.02D.

(c) 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 internetworking protocols to allow all types of traffic to traverse the network. These protocols include IP, transmission control protocol, file transfer protocol, 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.

1. Remote SIPRNET access can be accomplished using dial-up connections. Communications servers connect to DISA routers using secure devices (for example, STE) to access the SIPRNET. STEs restrict access to only authorized users by use of an access control list, which is loaded into the STE at the node site. Users must have a secret-level SIPRNET user key to be allowed connection to the communications server. For information on how to obtain communications server access, see the network information home page.

2. All SIPRNET requirements must be properly accredited, per DOD policy and procedures. This process can be found in DODI 8510.01.

(2) Networx. Networx 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.

(a) Flexible and efficient service is generally aided when end-to-end service is available. Thus, the majority of telecommunications services for Networx include both access 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 comprise an originating access portion, a transport portion, and a terminating access portion.

(b) Networx includes services necessary for the Government to satisfy many of 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.

(c) Service offerings include CSS, switched data service, and dedicated transmission services.

(3) 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. CSS includes:

(a) Switched voice service (SVS), which supports connections for voice and for analog data up to at least 9.6 kbps using an ITU–TSS V.32 modem and 56 kbps 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 kbps using ITU–TSS V.32 modem and 56 kbps 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).

(b) Circuit Switched Data Service, which provides a synchronous, full duplex, totally digital, SDP-to-POP service at data rates up to digital signal one, including certain integral multiples of digital signal zero 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. Circuit Switched Data Service dedicated access should be delivered directly to user's terminal equipment, including but not limited to, the following types: data terminal equipment (for example, workstation, host computer, PC, video codec, Group 4 FAX, and other communicating office equipment), digital private branch exchange, or intelligent multiplexer.

(c) 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.

(d) 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.

(4) Switched data service provides a synchronous, full duplex, totally digital, SDP-to-POP service at data rates up to digital signal one, including certain integral multiples of digital signal zero 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. Switched data service includes:

(a) 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 digital signal zero. PSS access is delivered directly to the user's terminal equipment. The user's terminal may be either packet-mode data terminal equipment which supports X. 25 protocol or nonpacket-mode data terminal equipment or terminal, which does not support X.25 protocol. User equipment supported should include, but not be limited to, multiplexing or switching devices such as private branch exchanges, channel banks, routers, or multiplexers; data terminal equipment (or packet-mode data terminal equipment); asynchronous American standard code for information interchange (ASCII) terminals; IBM binary synchronous communications protocol terminals; IBM System Network Architecture and synchronous data link control terminals; Unisys poll and/or select terminals. The contractor should provide packet assembly and/or disassembly capability.

(b) Frame relay service provides reliable, high speed, frame-switched, connection-oriented, data transmission services at data rates up to digital signal one between user locations. The flexibility and reliability of the service make it an attractive alternative to private line networks. Frame relay service access is delivered directly to user's terminal equipment, such as intelligent multiplexing or switching devices, or to LAN routers, or to data terminal equipment (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.

(c) IP internetworking service, which supports connectionless service between users (IP hosts) for execution of applications based on protocols, such as file transfer protocol, SMTP, HTTP, and connection to remote hosts (TELNET). IP internetworking service 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.

(5) Dedicated transmission services, which includes 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. Dedicated transmission services 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 dedicated transmission services will be delivered as an analog signal with a nominal bandwidth of 4 kilohertz.

(6) For information on value-added services (optional services) under the Networx program, visit the DOD Networx Web site, http://www.gsa.gov/portal/content/104870 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.

(7) Dedicated services

(a) Army ACOMs 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. Asynchronous transfer mode is being removed from all networks and should not be requested unless no other capability can replace it.

(b) 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.

(c) At the customer access locations, transmission bandwidth interfaces at below T1, T2, and T3 can be provided. The long-distance vendors will team with local access providers as required accomplishing the access area bandwidth requirements.

(d) Services can be obtained through the normal organizational channels via the telecommunications request provisioning process. If further information is required, refer to www.ditco.disa.mil/.

(8) Provisioning long-haul services

(a) DISA direct order entry (DDOE) has been initiated by DISA to facilitate the provisioning process as a means of ordering telecommunication services and equipment. The ATD, NETCOM is the point of contact for administration and maintenance of the Army's portion of DDOE. Customers must register for specific approval roles of the DDOE.

(b) 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 email to netcom.hq.longhaul@mail.mil.

b. Messaging services.

(1) Electronic mail. Official organizational electronic mail is to be migrated to DMS-compliant message products, while commercial email is used for medium grade messaging protected using the CAC card and DOD PKI.

(2) Defense Message System.

(a) The DMS is the DOD official system of record for organizational message capability. DMS is the only authorized electronic medium for the exchange of organizational messaging within the DOD. Other Government agencies and allied nations interface with DMS via the Multi-Function Interpreter, which provides an interface between the legacy Automatic Digital Network and DMS. DMS includes the hardware, software, policy, procedures, standards, facilities, and personnel used to exchange organizational messages electronically between DOD organizations, other government agencies, embassies, North Atlantic Treaty Organization and U.S. Allies. DMS enables command and control functions required to ensure global operational missions are achieved. DMS supports organizational messaging at the unclassified, secret, and top secret collateral levels.

(b) DMS is designed to provide an interoperable, seamless, and secure electronic messaging capability for organizational users within the DOD. DMS relies primarily on the DISN Transmission Control Protocol/Internet protocol (TCP/IP) networks: NIPRNET and the SIPRNET; local area networks; and other wide area networks, such as the Joint Worldwide Intelligence Communication System and other sensitive compartmented information networks.

(c) Organizational message users generally are considered to be those that formally represent the command and have authority to release messages. The Automated Message Handling System allows users to access their organizational

messages, using their CAC and a Web browser by using proxy user agents operated at centralized locations. Users access these mailboxes across a PKI encrypted Web link. Organizational users have the capability to send, receive, decrypt, store, and search messages.

(3) Commercial email. Individual message users will use DMS-compliant commercial electronic mail, which interfaces directly to the DMS messaging.

(4) Record communications (legacy systems).

(a) 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.

(b) DTH is a common-user network that processes traffic for two distinct COIs. 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.

(c) The DTH legacy system will be phased out as organizational users transition from DTH to DMS.

(5) United States Message Text Format.

(a) 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.

(b) 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://www.us.army.mil/suite/page/441756/.

7–8. Unified capabilities

The DOD CIO defines UC as "The integration of voice, video, and data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the Warfighter and business communities." Voice over Internet Protocol (VoIP) is the DOD preferred means of providing unclassified voice communications, and Voice over Secure Internet Protocol (VoSIP) is the DOD preferred means of providing classified (up to secret) voice communications. The Unified Capabilities Requirements 2008 will be used as policy guidance for implementation of VoIP and VoSIP capabilities. The current Approved Products List for VoIP devices is available at https://aplits.disa.mil/.

7–9. Global information grid waivers

a. General. DISA is the preferred UC transport provider for Internet and commercial satellite connections used for voice, video, and/or data services and DOD components are only permitted to use non-DISA enterprise-level infrastructures by exception. The CJCSI 6211.02D serves as the basis for Army policy in which the GIG Waiver Panel will approve waivers for any DOD use of non-DISA services (that is, DISN), in accordance with DODI 8100.04. Army entities requiring telecommunications services outside of DISA will submit a GIG waiver. This includes, but is not limited to, compliance with DOD networks, computing infrastructure, Internet connectivity, satellite, cloud services, cross domain management, as well as the oversight of the migration of legacy networks into the DISN. Additional information and a waiver template may be obtained at the following Web sites: https://www.intelink.gov/wiki/GIG-_Waiver_Panel_Army/ or http://www.disa.mil/Services/Network-Services/DISN–Connection-Process/Connection-Process-Guide/Service-Appendices/OSD–GIG–Waiver-Process.

b. Authority to operate. An IATO or ATO must be completed in conjunction with submitting the waiver request. The Defense Security and Information Assurance Working Group (DSAWG) will not provide a recommendation without an ATO or IATO. Therefore, it will not be a complete package to be presented to the GIG Waiver Panel. Army personnel should work in the C&A tracking database, https://armydiacaptdb.arl.army.mil/, to acquire an IATO and/or ATO via the accreditation process. Contact iacora@us.army.mil/ with questions.

c. Computer Network Defense Service Provider.

(1) If the organization will be passing DOD data, a Computer Network Defense Service Provider must be identified.

(2) If the organization will only be passing public information or data over the connection, a Computer Network Defense Service Provider is not required. Organizations will be required to identify the following two items: 1) Active Monitoring - How often is the connection monitored (for example, daily, weekly, or bi-monthly); 2) If there is a discrepancy, threat, or hacking event, who does the organization report that event to?

d. Global information grid waiver process. The GIG Waiver process for cloud computing, network, cross component computing issues, satellite, and commercial Internet service provider waivers is as follows:

(1) The requesting organization will contact ATD NETCOM or CIO/G–6 (SAIS–AOI) for confirmation if a GIG waiver is required. If a waiver is required, a briefing template can be downloaded from https://www.intelink.gov/wiki/GIG_Waiver_Panel_Army/ or sent via email. Waiver numbers are assigned by DISA representatives and do not change.

(2) Once the waiver briefing is complete it is forwarded to ATD NETCOM. NETCOM will review and request changes if necessary and then forward to CIO/G–6 (SAIS–AOI) with recommendations. The Army Cyberspace Operations and Integration Center will also review the completed briefing and provide recommendations. CIO/G–6 will review for content, clarity, accuracy, and validation. If CIO/G–6 validates and supports the waiver, it will be finalized and sent for DISA review and recommendation. If CIO/G–6 denies the request, a justification will be provided.

(3) All new or renewal requests must come through the appropriate Army and DISA offices for processing. One DISA office that reviews the packages is the DSAWG. A DSAWG brief is not required for new waiver requests unless requested by the DSAWG or primary responsible DISA office. If the initial review of the brief raises concerns regarding the security of the connection, the new waiver request will be required to go before the DSAWG. DSAWG will inform the Unclassified Connection Approval Office-Waivers if this is the case, DISA will inform both the Service representative and customer.

(4) Upon receipt of all DISA recommendations, the waiver package will progress to the GIG waiver panel. The CIO/G–6 will notify the customer if their waiver is on the monthly agenda. The requesting organization will brief the panel. If they are not in close proximity to the Washington, DC area the requestor can dial in via a teleconference. The requester must be prepared to answer any questions regarding mission, architecture, security, IA, costs, and policies that may be asked by the panel. The GIG Waiver Panel will make a final determination.

e. Waiver period. New GIG waivers can only request approval for 12 months. Renewals can request up to 36 months.

f. Combatant commands. Combatant Command packages are handled by Joint Staff.

g. Compliance. If a commercial ISP is discovered (either by DISA or Army personnel) at an Army installation that does not have a GIG waiver for that connection, Army GIG Waiver Panel representatives will be notified. The connection will either be discontinued or the customer must begin the GIG waiver process. If a GIG waiver approval is not received, the connection must be discontinued.

Appendix A
References

Section I
Required Publications

The following publications are available on the Army Publishing Directorate Web site (http://www.apd.army.mil) unless otherwise stated.

AR 25–1
Army Information Technology (Cited in paras 1–1, 1–4, 1–6a, 2–1a, 2–6e(4), 2–7b, 2–8b(2), 2–8b(3), 3–2d, 3–5b(4)(b), 3–5b(4)(a), 3–8o, 3–8d(12), 3–9b(3), 3–10a, 3–13b, 3–14a(1), 4–1a, 4–1c(1), 4–1c(3), 4–1l, 4–3c(1), 4–3f(2), 4–4, 4–4g(1), 4–7a, 5–3b, 5–6c, 6–5b(2), 6–5c(3), 6–5e, 6–8a, 6–9b, 6–13d, 6–13f(2)(c), 6–13g(1), 6–13h(2), 6–18e(1)(b), 7–2k, 7–3a(6)(c)9b, 7–6d(1).)

AR 25–2
Information Assurance (Cited in paras 1–4, 2–9d, 2–9c, 3–2h(4), 3–2f(1)(e), 3–2f(6), 3–2f(6)(c), 3–2h(1)(a)1, 3–14d(1), 3–14d(2), 3–14d(4)(e)2, 3–14a(1), 3–14a(6), 3–15b(3)(b), 4–1i, 6–4b, 6–5d, 6–9e(3), 6–9d, 6–10a(3), 6–13h(2), 6–13h(5), 7–1e(6).)

AR 70–1
Army Acquisition Policy (Cited in paras 1–4, 2–8d, 2–8b(2), 5–3a(2)(b), 7–6e, 7–6d.)

AR 71–9
Warfighting Capabilities Determination (Cited in paras 5–3a, 6–4b(2)(h), 7–6e, 7–6d, 7–6b(2), 7–6a(4).)

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. Department of Defense publications are available from http://www.dtic.mil/whs/directives. United States Codes, Codes of Federal Regulations, and Public Laws are available at http://www.gpo.gov/fdsys/.

AR 5–12
Army Use of the Electromagnetic Spectrum

AR 25–6
Military Auxiliary Radio System and Amateur Radio Program

AR 25–13
Telecommunications and Unified Capabilities

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 Program

AR 25–400–2
The Army Records Information Management System (ARIMS)

AR 210–7
Personal Commercial Solicitation on Army Installations

AR 215–1
Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities

AR 215–4
Nonappropriated Fund Contracting

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 380–40
Safeguarding and Controlling Communications Security Material

AR 380–53
Communications Security Monitoring

AR 500–3
U.S. Army Continuity of Operations Program Policy and Planning

AR 600–20
Army Command Policy

AR 608–1
Army Community Service

AR 700–142
Type Classification, Materiel Release, Fielding, and Transfer

AR 710–2
Supply Policy Below the National Level

AR 735–5
Property Accountability Policies

AR 750–1
Army Materiel Maintenance Policy

Army Doctrine Publication 3–0
Unified Land Operations

DA Memo 690–8
Headquarters, Department of the Army Telework Program

DA Pam 25–40
Army Publishing: Action Officers Guide

DA Pam 25–91
Visual Information Procedures

DA Pam 70–3
Army Acquisition Procedures

Allied Communications Publication 190(D)
Guide to Electromagnetic Spectrum Management in Military Operations (Available at http://jcs.dtic.mil/j6/cceb/acps/.)

CJCSI 3170.01H
Joint Capabilities Integration and Development System (Available at http://www.dtic.mil/cjcs_directives/.)

CJCSI 6130.01E
2013 CJCS Master Positioning, Navigation, and Timing Plan (MPNTP) (Available at http://www.dtic.mil/cjcs_directives/.)

CJCSI 6211.02D
Defense Information System Network (DISN) Responsibilities (Available at http://www.dtic.mil/cjcs_directives/.)

CJCSI 6212.01F
Net Ready Key Performance Parameter (NR KPP) (Available at http://www.dtic.mil/cjcs_directives/.)

CJCSI 6250.01E
Satellite Communications (Available at http://www.dtic.mil/cjcs_directives/.)

Communications Tasking Order 07–015
Public Key Infrastructure (PKI) Implementation, Phase 2 (Available at https://www.cybercom.mil/J3/orders/Pages/CTOs.aspx.)

Department of Defense Discovery Metadata Standard
(Available at http://metadata.ces.mil.)

Department of Defense Joint Technical Architecture (JTA), Version 6.0
(Available at http://www.acq.osd.mil/.)

DFARS
Defense Federal Acquisition Regulation Supplement (Available at www.acq.osd.mil.)

DFAS–IN Manual 37–100
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.)

DISA Circular 310–130–1
Submission of Telecommunications Service Requests (Available at www.disa.mil.)

DISA Circular 310–D70–30
Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations (Available at www.disa.mil.)

DOD Net–Centric Data Strategy
Memorandum, Chief Information Officer, May 9 2003 (Available from http://dodcio.defense.gov/.)

DOD 7000.14–R
Department of Defense Financial Management Regulations (FMRs)

DOD 8320.02–G
Guidance for Implementing Net-Centric Data Sharing

DODD 3020.26
Department of Defense Continuity Programs

DODD 5000.01
The Defense Acquisition System

DODD 5144.02
DOD Chief Information Officer (DOD CIO)

DODD 5240.01
DOD Intelligence Activities

DODD 5400.11
DOD Privacy Program

DODD 8115.01
Information Technology Portfolio Management

DODD 8570.01
Information Assurance (IA) Training, Certification, and Workforce Management

DODI 1015.12, Enclosure 4
Lodging Program (Category A) APF Support Table of Authorization

DODI 1035.01
Telework Policy

DODI 1100.21
Voluntary Services in the Department of Defense

DODI 4640.07
Telecommunications Services in the National Capital Region (NCR)

DODI 4650.01
Policy and Procedures for Management and Use of the Electromagnetic Spectrum

DODI 5000.02
Operation of the Defense Acquisition System

DODI 5400.13
Public Affairs (PA) Operations

DODI 8100.04
DOD Unified Capabilities (UC)

DODI 8320.02
Sharing Data, Information, and Technology (IT) Services in the Department of Defense

DODI 8330.01
Interoperability of Information Technology (IT), Including National Security Systems (NSS)

DODI 8500.01
Cybersecurity

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT)

DODI 8520.02
Public Key Infrastructure (PKI) and Public Key (PK) Enabling

DODM 5120.20
Management of American Forces Radio and Television Service (AFRTS)

DODM 5200.01 Volume 2
DOD Information Security Program: Marking of Classified Information

Executive Order 13514
Federal Leadership in Environmental, Energy, and Economic Performance (Available at http://www.whitehouse.gov.)

FAR
Federal Acquisition Regulation (Available at https://www.acquisition.gov/far/.)

Federal Telecommunications Recommendation 1080B–2002
Video Teleconferencing Services (Available at www.ncs.gov/library.html.)

Field Manual 6–01.1
Knowledge Management Operations

FIPS 140–2
Security Requirements for Cryptographic Modules (Available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=902003.)

FIPS 199
Standards for Security Categorization of Federal Information and Information Systems (Available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=150439.)

Headquarters, Department of the Army
The Army Resource Formulation Guide (Available at http://www.ppbe.army.mil (subscription and login required).)

IEEE 802
LAN/MAN Standards Committee (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
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 11179–1
Information Technology—Metadata Registries (Available at http://metadata-standards.org.)

ISO/IEC 12207
Systems and Software Engineering – 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.)

Joint Publication 1–02
Department of Defense Dictionary of Military and Associated Terms (Available at http://www.dtic.mil/doctrine/.)

Military Communications–Electronics Board Pub 8
Standard Spectrum Resource Format (SSFR) (Available at http://www.disa.mil/.)

MIL–STD 6040
United States Message Text Format (USMTF) (Available at http://www.disa.mil/.)

NIST Special Publication 800–44 Version 2
Guidelines on Securing Public Web Servers (Available at http://csrc.nist.gov/publications/PubsSPs.html.)

NIST Special Publications 800–100
Information Security Handbook: A Guide for Managers (Available at http://csrc.nist.gov/publications/PubsSPs.html.)

NIST Special Publication 800–125
Guide to Security for Full Virtualization Technologies (Available at http://csrc.nist.gov/publications/PubsSPs.html.)

NIST Special Publication 800–145
The NIST Definition of Cloud Computing (Available at http://csrc.nist.gov/publications/PubsSPs.html.)

OMB Circular A–11
Preparation, Submission and Execution of the Budget (Available at http://www.whitehouse.gov/omb/circulars_default.)

OMB Circular A–76
Performance of Commercial Activities (Available at http://www.whitehouse.gov/ omb/circulars_default.)

OMB Circular A–130
Management of Federal Information Resources (Available at http://www.whitehouse.gov/ omb/circulars_default.)

OMB Memorandum, 30 September 2003
Guidance for Implementing the Privacy Provisions of the E–Government Act of 2002 (Available at www.whitehouse.gov/omb/memoranda_2003.)

Public Law 101–336
Americans with Disabilities Act of 1990

Public Law 103–62
Government Performance and Results Act of 1993

Public Law 104–106
National Defense Authorization Act for Fiscal Year 1996

Public Law 104–191
Health Insurance Portability and Accountability Act of 1996

Public Law 108–375
National Defense Authorization Act for Fiscal Year 2005

Public Law 112–81
National Defense Authorization Act for Fiscal Year 2012

Unified Capabilities Requirement 2008, Change 3
(Available at http://www.disa.mil/Services/Network-Services/UCCO.)

5 USC 552
Freedom of Information Act

5 USC 552a
The Privacy Act

10 USC 1588(f)
Authority to Accept Certain Voluntary Services

10 USC 2223
Information Technology: Additional Responsibilities of Chief Information Officers

17 USC Chapters 1 and 2
Software Copyrights

28 USC 1346(b)
Federal Tort Claims Act

29 USC 794d
Section 508 of the Rehabilitation Act Amendments of 1998, as amended by Section 2405 of the FY 2001 Military Appropriations Act (PL 105–220)

31 USC 3721
Military and Civilian Employees Claims Act

36 CFR 1194
Title 36–Parks, Forests, And Public Property, Electronic and Information Technology Accessibility Standards

36 CFR 1220–1238
Title 36–Parks, Forests, And Public Property, Federal Records

40 USC Subtitle III
Information Technology Management (Clinger-Cohen Act)

42 USC Chapter 55
National Environmental Policy (National Environmental Policy Act)

44 USC Chapter 35
Coordination of Federal Information Policy (Paperwork Reduction Act)

47 USC 153
Definitions

47 USC 255
Access by persons with disabilities

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (http://www.apd.army.mil/); DD forms are available on the Office of the Secretary of Defense (OSD) Web site (http://www.dtic.mil/whs/directives/infomgt/forms/index.htm); Standard forms (SFs) are available on the U.S. General Services Administration (GSA) Web site (http://www.gsa.gov).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2407
Maintenance Request (Available through normal supply channels)

DA Form 3161
Request for Issue or Turn-In

DA Form 3953
Purchase Request and Commitment

DA Form 7222–1
Civilian Evaluation Report Support Form

DA Form 7223–1
Base System Civilian Performance Counseling Checklist/Record

DD Form 428
Communication Service Authorization

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 1367
Commercial Communication Work Order

DD Form 1391
FY__ Military Construction Project Data

DD Form 1494
Application for Equipment Frequency Allocation

DD Form 2930
Privacy Impact Assessment (PIA)

DD Form 2946
Department of Defense Telework Agreement

DISA Form 772
Telecommunications Management System (Available from http://www.disa.mil, then click the "Contact us" button to request form.)

DLIS Form 1867
Certification of Hard Drive Disposition (Available from http://www.dispositionservices.dla.mil/gov/forms/dlis/DLIS1867.pdf.)

SF 1034
Public Voucher for Purchases and Services Other Than Personal

SF 1449
Solicitation/Contract/Order for Commercial Items

Appendix B
Instructions on Telework Program

Telecommuting is designed to benefit employees, managers and the community by decreasing work trip vehicle miles, traffic and/or 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. Instructions for the DD Form 2946

a. Section I (to be completed by the employee).
(1) Employee Name.
(2) Job Title.
(3) Pay Plan/Series/Grade/Pay Band.
(4) Organization.
(5) Traditional Official Worksite.
(6) Alternate Worksite Address.
(7) Alternate Worksite Telephone Number.
(8) Alternate Worksite Email Address.
(9) Telework Arrangement Implementation Dates —
(a) Start (YYYYMMDD).
(b) End (YYYYMMDD).
(10) Tour of duty:
(a) Fixed.
(b) Flexible.
(c) Compressed.
(11) Telework Arrangement.
(a) Regular and recurring telework.
(b) Situational telework.
(12) Continuity of Operation "Emergency Response" Status (select "Is" or "Is Not").
(13) Authorized Management Official Signature and Date.
(14) Employee Signature and Date.

b. 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.

c. Salary and benefits. The supervisor and applicant agree that a telework arrangement is not a basis for changing the applicant's salary or benefits.

d. 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 they will make appropriate arrangements for childcare as necessary to provide for a minimum of interruptions during the workday.

e. 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.

f. Leave. The applicant agrees to follow established office procedures for requesting and obtaining approval for leave.

g. 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.

h. 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.

i. Equipment and/or 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. 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.

j. 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.

k. 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.

l. Liability. The applicant understands that the Government will not be held liable for damages to the applicant's personal or real property while they are 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.

m. 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.

n. Work area. An applicant working at home agrees to provide a designated work area adequate for performance of official duties.

o. Injury compensation. The applicant understands that they are 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 their 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.

p. Work assignments and performance. The employee agrees to complete all assigned work according to guidelines and standards in the employee DA Form 7222–1 (Civilian Evaluation Report Support Form) or DA Form 7223–1 (Base System Civilian Performance Counseling Checklist/Record). 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.

q. 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).

r. Standards of conduct. The applicant agrees that they are bound by official standards of conduct while working at the alternate workplace.

s. Cancellation. The applicant understands that the organization may cancel the telework arrangement and instruct the applicant to resume working at the office. If the applicant elects to voluntarily withdraw from the program, they are expected to give sufficient notice so that arrangements can be made to accommodate their return to a regular work schedule and they must complete the DD Form 2930 and the cancellation section of the form.

t. 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.

u. Term. Unless canceled or terminated earlier by either the employee or the employer, this agreement will expire on (enter date) , unless renewed by agreement of the employee and the employer.

v. Certification. By signing this agreement, the applicant certifies that they have read the terms of this agreement and agree to follow the policies and procedures outlined in them as well as all other applicable policies and procedures.

w. Applicant's signature.

x. Date.

B–2. Telework safety assessment

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 select "Yes or No" to complete the self-certification safety checklist. Upon completion, the checklist should be signed and dated by the applicant.

a. Temperature, ventilation, lighting, and noise levels are adequate to maintain a home office.

b. Electrical equipment is free of recognized hazards that would cause physical harm (frayed, exposed, or loose wires; loose fixtures; bare conductors, and so forth).

c. Electrical system allows for grounding of electrical equipment (three-prong receptacles).

d. Office (including doorways) is free of obstructions to permit visibility and movement.

e. File cabinets and storage closets are arranged so drawers and doors do not enter into walkways.

f. Phone lines, electrical cords, and surge protectors are secured under a desk or alongside a baseboard.

g. If material containing asbestos is present, it is in good condition.

h. Office space is free of excessive amount of combustibles, floors are in good repair, and carpets are well secured.

i. Employee signature and date. 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 the applicant begins to telework.

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 "non-applicable" or "NA". The following information is entered:

a. Employee name.

b. Supervisor's name.

c. Employee and/or supervisor has read AR 25–1, this publication, and reviewed DOD telework policy located at http://www.cpms.osd.mil/telework/telework_index.aspx. Enter date.

d. Employee has been provided with a schedule of work hours. Enter date.

e. The technology and equipment checklist must specify if is a requirement and if ownership is by either the government agency or personal, and whether it is reimbursement by component. Check as applicable:

(1) Computer Equipment:

(a) Laptop (Yes/No).

(b) Desktop (Yes/No).

(c) PDA (Yes/No).

(d) Other (Yes/No).

(2) Access:

(a) IPASS/VPN Account (Yes/No).

(b) Citrix - Web Access (Yes/No).

(c) Other: (Yes/No).

(3) Connectivity:

(a) Dial-In (Yes/No).

(b) Broadband (Yes/No).

(4) Required Access Capabilities:

(a) Shared Drives (for example, H or P Drive) (Yes/No).

(b) Email (Yes/No).

(c) Component Intranet (Yes/No).

(d) Other applications: (Yes/No).

(5) Other Equipment/Supplies:

(a) Copier (Yes/No).

(b) Scanner (Yes/No).

(c) Printer (Yes/No).

(d) Fax Machine (Yes/No).

(e) Cell Phone (Yes/No).

(f) Paper supplies (Yes/No).

(g) Other: (Yes/No).

f. Policies and procedures for care of equipment issued by the agency have been explained and are clearly understood. Enter date.

g. Policies and procedures covering classified, secure, or Privacy Act data have been discussed and are clearly understood. Enter date.

h. Policies and procedures covering information assurance (IA) operations of the equipment and IA functions have been discussed and clearly understood. Enter date.

i. Requirements for an adequate and safe office space and/or area have been discussed, and the employee certifies those requirements are met. Enter date.

j. Performance and conduct expectations have been discussed and are clearly understood. Enter date.

k. Employee understands that the supervisor may terminate employee participation in accordance with established administrative procedures and union-negotiated agreements. Enter date.

l. Employee has participated in training. Enter date.

m. Supervisor has participated in training. Enter date.

n. Supervisor's signature and date.

o. Enter employee's signature and date.

B–4. Telework arrangement cancellation

Termination from the DD Form 2946 can be either voluntary or involuntary. Either the employee or the supervisor can cancel and/or terminate a DD Form 2946. Management will terminate the DD Form 2946 should the employee's performance not meet the prescribed standard or the teleworking arrangement fail to meet organizational needs. DD Form 2946, Section IV: Notice of Telework Arrangement requires the following information:

a. Cancellation date. (YYYYMMDD)

b. Initiated by (please check one) —

(1) Employee.

(2) Management.

c. Reason(s) for cancellation.

d. Government furnished equipment and/or property returned list property and date of return (please check one) —

(1) Yes.

(2) No.

e. Supervisor's signature and date.

f. Employee'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.

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 NECs or senior IM/IT officials 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 NEC 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, immediate action is taken to recover the cost of unauthorized calls. The phone customer service office and Defense Finance and Accounting Service (DFAS) process cash collection vouchers. If organizations deem disciplinary action appropriate for abuse of Government phone service, the Civilian Personnel Administration Center or Civilian Personnel Operations Center 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 below for information regarding telecommunication bill certification actions).

e. The following are a list of telecommunications 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, and 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 items.

(4) Request a customer service records from the vendor that itemizes the services on the bills. Become familiar with the format of the call detail reports.

(5) Reconcile monthly billings with applicable tariffs, communications service authorizations, and customer service records to make sure bills for services rendered match the contract amount and tariffs.

(6) Ensure that services received are covered by communications service authorizations or local leased consolidated telephone contract.

(7) Investigate differences in bills, customer service records, 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 point of contact, so that unnecessary services can be terminated and the communications service authorizations or contract modified.

(11) Request credits for overpayments when identified, and request payment in kind.

(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 previous month's to see if any major changes occurred.

(14) Discuss disputes immediately with vendors' customer service representatives or your NETCOM G34/G8 long-haul (LH) point of contact, 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 the SF 1034 (Public Voucher For Purchases Services Other Than Personal).

(19) Process bills in a timely manner. Prioritize workload to allow time to prepare SF 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 local and/or long-distance charges, after the bill is paid. If charges are invalid billing items, request a credit from the phone company. If charges are for unofficial calls, request payment from the party making the call.

(21) Request "read only" access to DFAS database to:

(a) Review the status and amounts of telecommunications vendor payments processed by the DFAS.

(b) Aid in resolving payment questions from vendors.

(22) Billing for long-haul services.

(a) Bills for Army long-haul communications services are processed through the G8 LH. Customers must submit a military interdepartmental purchase request and/or funding authorization document issued to the G8 LH on an annual or quarterly basis. Funds can be provided to the central G8 LH email box at netcom.hq.longhaul@mail.mil.

(b) For all Army long-haul accounts, it is required that financial and technical points of contact, and service period of performance be provided on the funding document.

(c) Estimates are derived from the customer cost and obligations report and from new or changed telecommunications requests submitted through the DDOE system (see paragraph 7–7a(8)(a)). The G8 LH produces monthly invoices for each customer account. For any identified discrepancies on the monthly invoice, contact G8 LH at email box netcom.hq.longhaul@mail.mil.

(d) G8 LH is a reimbursable organization, so the G8 LH has no direct funding to cover your account and/or negative un-liquidated obligation while it is being disputed. Your immediate action in providing funds to cover services rendered is requested. If not immediately resolved, the Deputy Assistant Secretary of the Army for Financial Operations may consider this to be a reportable anti-deficiency act violation and may result in an interruption of service. G8 LH cannot hold a monthly bill, until you complete the dispute of your account. If the dispute is justified, then appropriate adjustments will be made to your account.

f. AR 25–1 states that the installation commander establishes local policy for handling incoming official collect calls. Installation NECs 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.

g. AR 25–1 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 NEC in writing. Replacement cards may be issued if necessary. Unissued or returned cards must be kept in a locked and/or secure area. When issuing correspondence regarding calling cards, leave off or cross out the 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.

h. 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 NEC office immediately so service can be canceled to prevent illegal use and/or charges. Cellular phones must not be used when other less costly phone service is available (see AR 25–1 for Army policy on the issuance and use of mobile, portable, and cellular phones).

i. The ATD, NETCOM 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 SBU Voice. Installations and separate reporting activities may institute the measures to reduce telecommunications costs without degrading service.

j. Installations and separate reporting activities may institute the following measures identified below to reduce telecommunications costs without degrading service:

(1) 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.

(2) Review all long distance calls monthly and certify that all calls are Government business.

(3) Know the requirement behind each service, and keep a current database of points of contact on your installation. This will save time when trouble tickets are submitted. Issue calling cards to personnel on temporary duty to make required calls. Cardholders should use cards when access to Networx, SBU Voice or other Government local long distance service is unavailable.

(4) Use official calling cards through commercial phone services, instead of cellular phone service to call long distance.

(5) Make Networx the long distance carrier on Government switches and business lines, as well as official business lines not on Government premises.

(6) 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.

(7) Review the need and use of SBU Voice precedence lines to affirm the requirement is still valid.

(8) Analyze monthly Networx 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 user to transfer calls off post without coordinating through human operators. Identify and report abuse of Government telecommunications systems.

(9) Establish local policy to prohibit the use of 1–800 calls from within the local area vice calling the local numbers.

(10) Ask the local phone company to block all collect and third-party calls and/or if possible on Government switches.

(11) To avoid incurring late charges, date-time stamp bills upon receipt to restart the payment period on commercial phone bills. Payment of phone by use of a Government credit card expedites bill paying and avoids late charges.

(12) Check the requirement for paying state or local taxes. The Federal Government is not required to pay state or local taxes in some states.

(13) 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.

(14) Inventory all phone services and combine them into one requirements package for open competition. This can result in lower prices due to a large volume of services and a commitment to retain the services for a longer period of time rather than month-to-month service.

(15) Reconcile phone numbers billed against the phone numbers actually used. Request that customers inventory their accounts on a regularly basis to ensure that bills correspond to the services required.

(16) TCOs attend G34 BASECOM seminar either annually or biennially.

k. Policy regarding Class B service is found in AR 25–1. Policy and procedures regarding charges for Class B service and distribution of revenues are found in DFAS–IN Manual 37–1, Chapter 13–131802–B (https://dfas4dod.dfas.mil/centers/dfasin/library/regs.htm).

(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 NEC and DFAS.

(2) Rates for Class B service are established by DOD. Because rates normally change annually, NECs 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, Chapter 13–131804–B.

(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. The ATD produces monthly invoices for each customer account. Individuals with a need to know can request billing information by sending an email to netcom.hq.longhaul@mail.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).

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. Appropriated funds may not be used to pay 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, enclosure 4.

f. The installation NEC provides procedural guidance regarding CATV services, payment, and required approvals for official use of CATV to subscribers within their areas of supervision. The NEC 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 DODM 5120.20. 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 ACOM 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.

Appendix D
Element of Resource Codes

D–1. Purpose

The EOR classifies the resource according to the nature of the usage rather than the purpose. The EOR code is a four digit number that identifies the type of resource being employed or consumed (such as military personnel, civilian personnel, travel of personnel, utilities and rents, and communication). The first two numbers are related to an OMB object classification. The 3rd and 4th positions identify the detail needed for management reports, budget exhibits, and general ledger requirements.

D–2. Element of resource categories

EORs have been divided into four categories to facilitate readability and usage: Current - Civilian and Military Pay EORs; Current - Non Pay EORs; Expired - Civilian and Military Pay EORs; and Expired - Non-Pay EORs. The EOR tables and additional information is available in the DFAS–IN Manual 37–100, http://asafm.army.mil/offices/BU/Dfas37100.aspx. The Army proponent for EORs is SAFM–BUC–F.

Appendix E
Army Capability-based Architecture Development and Integration Environment

E–1. Army Capability-based Architecture Development and Integration Environment

AR 71–9 (28 December 2009) directs that all IT and/or NSS products must comply with DODAF and AEA requirements, and be documented in an Army architecture centralized database. Materiel developers and other IM officials requiring IT and/or NSS will ensure compliance with architectures. Directors of IM will review and ensure compliance with architectures. That Army architecture centralized database, implemented in 2006, is the Army Capability-based Architecture Development and Integration Environment (ArCADIE). ArCADIE is the single authoritative source for all Army classified and unclassified architecture data and artifacts. In limited circumstances, the Mission Areas may request approval from HQDA CIO/G–6 to establish supplementary architecture integration tools. When approved, these additional tools must be compatible and interoperable with ArCADIE in order to maintain an enterprise view of the LandWarNet.

E–2. Army Capability-based Architecture Development and Integration Environment Portal access

The ArCADIE Portal is available on NIPR at https://cadie.army.mil and SIPR at https://cadie.army.smil.mil. To access the NIPR portal users must hold an AKO account and a CAC. Note that users accessing ArCADIE must select their "DOD email" certificate when signing in. The portal will continue to evolve and add capabilities and services to leverage technological advances.

E–3. Using Army Capability-based Architecture Development and Integration Environment in support of information technology management

The four primary system functions in ArCADIE are architecture development, architecture management and storage, discovery and search services, and architecture reporting and analysis. The user's requirements will determine the level of interface with the various applications enabling the four primary system functions.

a. Architecture Development.

(1) Architecture tools and licenses are provided. Tools are primarily COTS that enable users to develop architecture from end to end. Many of the COTS tools focus on creating DODAF data and product sets. ArCADIE also provides users with process-specific applications that help to tailor architecture efforts beyond the DODAF (for example, in support of Agile Process Network Integration Evaluations).

(2) Data Extraction, Transformation, and Loading (ETL) Services. ArCADIE provides ETL services transparently to the user, yet they are critical for data management and integration success. The Army leverages Integrated Architecture Data Standards (IADS) developed by the Army architecture and data steward communities and approved by the Architecture Data Steward. The IADS help integrate data from various tools and methodologies into a common format to load into the ArCADIE Data Warehouse. IADS can be found at https://cadie.tradoc.army.mil/IADS/SitePages/Home.aspx.

b. Architecture Management and Storage. Data Integration, Federation, and Storage: The heart of ArCADIE is the data warehouse construct. As data is validated, cleansed, transformed, and aggregated from the ETL process, it is ready to load in the data warehouse. The data warehouse is a centrally managed and integrated database containing authoritative data from the operational sources within each mission area and major command.

c. Discovery and Search Services. To manage architecture, one must be able to organize and find it. For architect and non-architect users, this may be the first step within the ArCADIE process. ArCADIE provides a catalog system that acts as a library "card-catalog" containing metadata about the architectures. This metadata is filled-in and managed by the owner. It follows a standard that is part of a larger DOD-wide federated discovery search capability. ArCADIE enforces this standard and it meets all DOD and Joint regulatory guidance for registration of architecture data.

d. Architecture Reporting and Analysis.

(1) Operational and Systems Visualization. ArCADIE provides the means and applications to use architecture data for analysis across the Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Policy spectrum. ArCADIE provides access to authoritative data to support network design and operational demand analysis for IT material solutions. ArCADIE also provides the ability to create data marts.

(2) Reporting and Analysis. ArCADIE has organic applications native to the system that develop reports and display architecture data. Here again, ArCADIE leverages data marts to be specifically tailored to the user's requirements.

e. Architecture Governance.

(1) Provide and Enforce Data Standards. ArCADIE supports architecture governance through automated auditing and error checking by leveraging IADS. Common architecture development comes through the support of automated data extraction from architecture tools, excel data template imports, and direct input through Web applications.

(2) Verification and Validation Process. This ensures the architecture meets the minimum DODAF guidance. The process routes architecture through appropriate channels for approval and provides users status of architecture validation. The Verification & Validation Guide can be found at https://cadie.army.mil/Cadie/Portal/PolicyInformation.aspx.

E–4. Managed user access

Authentication verifies the identity of users and validates using a CAC through SSO and enterprise collaboration services. Each area of the environment is role-based to ensure segmentation of access and control.

a. Online Support Web based access to a trouble tracking system can be accessed at https://cadie.tradoc.army.mil/Support/SitePages/Home.aspx.

b. Phone Support. Helpdesk analysts can be contacted at 757–501–5922. The end user must have a valid trouble tracking ticket number prior to receiving phone support.

E–5. Federation

ArCADIE is a federated environment. Data federation occurs when data stored in a dissimilar set of autonomous data stores is made accessible to data consumers as single authoritative source by using on-demand data integration. Thus, ArCADIE, as the single authoritative source for Army Architecture data and artifacts refers to the data warehouse as a single integrated data store. Therefore, regardless of how and where data is stored, it is presented as one integrated data set to the user. Data is not necessarily stored in an integrated way or even within a single data warehouse. This is commonly referred to as "on-demand integration" and is transparent to the user.

E–6. Governance

The foundation for sharing and integrating architecture data starts with the governance process. Governance provides the policies, procedures, standards, and rules which developers and users must follow to ensure data is consistent, and in a common format. In order to accomplish the governance process for architecture data the CIO/G–6 has appointed an Architecture Data Steward who is the Army lead responsible for developing, maintaining, and implementing policies, procedures, standards, and rules for Army architecture data. The supporting structure that assists the Data Steward in keeping the Architecture Community of Interest informed falls under the responsibility of the appointed Functional Data Managers of each domain. Further delineation of roles and responsibilities of the Functional Data Managers can be found in the Army Architecture Data Management Plan located at https://cac.cadieview.army.mil/Work%20Collaboration%20Areas/Data_Standards/Documents/Reference/Army_Architecture_Data_Management_Plan.docx. ArCADIE provides the means to support the governance process by enforcing data standards, common architecture development, and Verification and Validation for Army architectures.

Glossary

Section I
Abbreviations

AAFES
Army and Air Force Exchange Service

ACAT
acquisition category

ACOM
Army command

ACP
Army campaign plan

ACSIM
Assistant Chief of Staff for Installation Management

ADS
authoritative data source

AEA
Army Enterprise Architecture

AIA
Army Information Architecture

AIC
Army interoperability certification

AKO
Army Knowledge Online

AKO–S
Army Knowledge Online – SIPRNET

APMS
Army Portfolio Management System

AR
Army regulation

ARFORGEN
Army Force Generation

ARNG
Army National Guard

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ASCC
Army service component command

ASCII
American standard code for information interchange

ATD
Army Telecommunications Directorate

AWRAC
Army web risk assessment cell

BASECOM
base communications

BPA
blanket purchase agreement

C4
command, control, communications, and computers

C4IM
Command, Control, Communications, Computers and Information Management

C&A
certification and accreditation

CAC
common access card

CAP
Computer/Electronic Accommodations Program

CATV
cable television

CECOM
Communications-Electronics Command

CFR
Code of Federal Regulations

CHESS
Computer Hardware, Enterprise Software Solutions

CIO
chief information officer

CIO/G–6
Chief Information Officer,G–6

CJCSI
Chairman of the Joint Chief of Staff Instruction

COE
common operating environment

COI
community of interest

COMSEC
communications security

CONUS
continental United States

COTS
commercial off-the-shelf

DA
Department of the Army

DA Pam
Department of the Army pamphlet

DAA
designated approval authority

DBMS
database management system

DD
Department of Defense

DEERS
Defense Enrollment Eligibility Reporting System

DFARS
Defense Federal Acquisition Regulation Supplement

DFAS
Defense Finance and Accounting Service

DISA
Defense Information Systems Agency

DISN
Defense Information Systems Network

DISR
DOD Information Technology Standards Registry

DLIS
Defense Logistics Information Service

DMS
Defense Message System

DOD
Department of Defense

DODAF
DOD Architecture Framework

DODD
Department of Defense directive

DODI
Department of Defense instruction

DPP
data performance plan

DRMO
Defense Reutilization and Marketing Office

DRMS
Defense Reutilization and Marketing Service

DRU
direct reporting unit

DSN
defense switched network

e-commerce
electronic commerce

EB
Executive Board

EIT
electronic and information technology

ELA
enterprise license agreement

EOR
element of resource

ESA
enterprise software agreement

EXORD
Execution Order

FAR
Federal Acquisition Regulation

FAX
facsimile

FDED
Fort Detrick Engineering Directorate

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Management Act of 2002

FOA
field operating activity

FOIA
Freedom of Information Act

FOUO
for official use only

FSS
Federal supply schedule

FTS
Federal Telecommunications System

FY
fiscal year

GIG
global information grid

GOSC
General Officer Steering Committee

GPS
Global Positioning Service

GSA
General Services Administration

HMW
health, morale, welfare

HQDA
Headquarters, Department of the Army

HTML
hypertext markup language

HTTP
hypertext transfer protocol

HTTPS
hypertext transfer protocol secure

I3MP
Installation-Information Infrastructure Modernization Program

IA
information assurance

ID
identification

IESS
Information Exchange Standard Specifications

IM
information management

IMCOM
U.S. Army Installation Management Command

IMO
information management office/officer

INMARSAT
International maritime satellite

IP
Internet protocol

ISCE
information systems cost estimate

ISDN
integrated services digital network

ISP
Internet service provider

ISR
Installation status report

IT
information technology

ITEC4
Information Technology Electronic-Commerce and Commercial Contracting Center

ITM
information technology management

JCIDS
Joint Capabilities Integration and Development System

JITC
Joint Interoperability Test Command

LAN
local area network

LCM
life-cycle management

MATDEV
materiel developer

MDEP
management decision package

MILCON
military construction

MIL–STD
military standard

MTOE
modified table of organization and equipment

MWR
morale, welfare, and recreation

NAF
nonappropriated fund

NEC
Network Enterprise Center

NETCOM
Network Enterprise Technology Command

NETOPS
network operations

NIPRNET
non-secure Internet protocol router network

NIST
National Institute of Standards and Technology

NSS
National Security System

O&M
operation and maintenance

OCONUS
outside the continental United States

ODCS
Office of the Deputy Chief of Staff

OMB
Office of Management and Budget

ONS
operational needs statement

OPA
other procurement, Army

OSD
Office of the Secretary of Defense

Pam
pamphlet

PBO
property book officer

PBX
private branch exchange

PC
personal computer

PDA
personal digital assistant

PCMCIA
Personal Computer Memory Card International Association

PEG
program evaluation group

PEO
program executive officer

PIA
privacy impact assessment

PII
personally identifiable information

PIN
personal identification number

PKI
Public Key Infrastructure

PM
program manager

POM
program objective memorandum

POR
program of record

PPBE
planning, programming, budgeting, and execution

PRB
Project review board

RFS
request for service

ROTC
Reserve Officers’ Training Corps

SATCOM
satellite communications

SDB
satellite database

SF
standard form

SIPRNET
secret Internet protocol router network

SLA
Service level agreement

SMS
Strategic Management System

SMTP
simple mail transfer protocol

STE
secure telephone equipment

TAP
The Army Plan

TCO
telephone control officer

TCP/IP
transmission control protocol/Internet protocol

TDA
table of distribution and allowances

TNOSC
Theater Network Operations and Security Center

TOE
table of organization and equipment

TRADOC
United States Army Training and Doctrine Command

USACC
United States Army Cadet Command

USACE
United States Army Corps of Engineers

USAR
United States Army Reserve

USAISEC
United States Army Information Systems Engineering Command

USC
United States Code

VPN
virtual private network

VTC
video teleconferencing

WAN
wide area network

WIN–T
Warfighter Information Network-Tactical

WLAN
wireless local area network

WMA
Warfighter Mission Area

XML
eXtensible markup language

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.

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.

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).

Application
A software program or group of programs that acts on behalf of the operating system to perform a limited and specific function for the user. An application does not inherently have an operating system, but relies on an operating system to execute. Application does not include IA or IA enabled products, which would be required to undergo C&A.

Army Continuity of Operations Program
An integrated set of Army policies, plans, and procedures that ensure the continuity of mission essential functions under all circumstances including crisis, attack, recovery, and reconstitution. It encompasses ACOM, ASCC, or DRU, FOAs, and subordinate commands performing continuity of operations functions, including orderly succession, transition of leadership, and performance of essential functions across the spectrum of national security emergency.

Army Cyber Command
Army Cyber Command is an operational level headquarters designated by the Secretary of the Army as the Army Force Component Command of United States Cyber Command. It is the lead for Army missions, actions, and functions related to cyberspace, including responsibility for planning, coordinating, integrating, synchronizing, directing, and conducting Army network operations and defense of all Army networks. When directed, Army Cyber Command conducts full spectrum cyberspace operations to ensure freedom of action in cyberspace, and to deny the same to our adversaries.

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, that provides centralized management of the Army’s worldwide commercial-leased and Government-owned telecommunications; serves as the Army interface with the DISA, DITCO, and GSA on telecommunications certification office related matters.

Army Training and Certification Tracking System
This system provides managers at all levels a capability to report and manage their IA workforce and general user population training and certification statistics and a summary report of certification voucher distribution, available at https://atc.us.army.mil.

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.

Authoritative data source
A recognized or official data production source with a designated mission statement or source and/or product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources.

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 5000.01)

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
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 kbps channels and one clear 16 kbps 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.

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.

Busy hour
The 60-minute period during which the traffic load of a given 24-hour period is at maximum.

Command, Control, Communications, Computers and Information Management (C4IM) Services List
The service list pertains to NEC and NOSC provided services and managed infrastructure. The list's service groups are Communication Systems and Systems Support, Information Assurance, and Automation.

Cable television (CATV) system
A facility consisting of a set of closed transmission paths and associated signal generation, reception, and control equipment that is designated to provide cable service which includes, both audio and video programming and which is provided to multiple subscribers.

Call
A unit of traffic measurement that refers to any demand to set up a connection.

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 dial-up data (DU3); 1,200 bits per second dial-up data (DUl2); or 9,600 bits per second digital data (DI96).

Caller, calling party, call originator
A person, program, or equipment that originates a call.

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.

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 and/or 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 and/or 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 and/or 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, computers, and intelligence (C4I)
One of four domains used to manage architecture configurations in the AEA. C4I includes all systems involved in C4 and intelligence and electronic warfare systems.

Command, control, communications and computer (C4) systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications and computers 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 a Maximum Limits Communications Service Authorization.

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 to provide commercial satellite communications terminals to meet DOD commercial satellite communications requirements.

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.

Communications systems
A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

Communications service authorization
DD Form 428 (Communication Service Authorization) 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 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.

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.

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
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
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
Manages the reporting of automation resources inventory and excess including hardware and software.

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 DOD. 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 U.S. 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.

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.

Electronic access
The ability to access information online (dedicated or dial-up), email, and fax.

Electronic commerce
Army e-Commerce is the 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
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 electronic data interchange is defined by the American National Standards Institute X12 family of standards. Third parties provide electronic data interchange services that allow organizations with different equipment to interoperate.

Electronic mail (email)
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 IT. An enterprise architecture describes the "target" situation that the agency wishes to create and maintain by managing its IT portfolio.

External official presences
Official public affairs activities conducted on non-DOD sites on the Internet (for example, Combatant Commands on Facebook, CIO/G–6 on Twitter). External official presences are established on commercial venues for the purposes of creating a transparent information-sharing environment and gaining feedback from the public.

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
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 file transfer protocol 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 and/or user to a distant telephone exchange and providing the equivalent of local service from that exchange. Rates are established by local tariffs.

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
Functional requirements are those specifically required to support a particular business function.

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 the Defense Information Technology Management System.

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
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 office/officer (IMO)
The office or individual who reports to a senior IM official 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 senior IM official in effectively managing the organization's IM/IT processes and resources that enable the organization's business and mission processes.

Information producers
A person, group, organization, system, or process that creates, updates, distributes, and retires information based on their authorized and/or assigned missions and functions.

Information management support council
An installation implementation work group organized under the direction of the NEC. 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
A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. As part of the set of information resources, an information system includes its own operating system(s), firmware, hardware (or all of the above) to support a single mission or across a range of missions. An information system may include, but is not limited to, the products or deliverables of an acquisition program, such as those described in DODD 5000.01.

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 Subtitle III).

Information Technology Infrastructure Library (ITIL)
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 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-based capabilities
All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as social media, user-generated content, social software, email, instant messaging, and discussion forums (for example, YouTube, Facebook, MySpace, Twitter, Google Apps).

Internet protocol (IP)
A DOD standard protocol designed for use in interconnected systems of packet-switched computer communication networks. Note: The IP provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The IP also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small packet networks.

Internet-working
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 IT and acquiring new IT 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 will 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 process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. The purpose of knowledge management is to create shared understanding through the alignment of people, processes, and tools within the organizational structure and culture in order to increase collaboration and interaction between leaders and subordinates. This results in better decisions and enables improved flexibility, adaptability, integration, and synchronization to achieve a position of relative advantage (see Field Manual 6–01.1).

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
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 allows the Competitive or Certified Local Exchange Carriers to compete for business within the defined service area of the Incumbent Local Exchange Carrier, formerly a monopoly-situated carrier.

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 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 SBU (formerly 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
Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

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 MDR 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
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
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 and frequency-division multiplexing. In optical communications, the analog of frequency-division multiplexing is referred to as wavelength-division multiplexing.

National Security System
As defined in Section 5142 of the CCA (40 USC Subtitle III), 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 decisionmaking cycles. Net-Centric capabilities enable network-centric operations and Network-Centric Warfare.

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 SBU Voice (formerly DSN) via local DOD PBXs and/or private administrative branch exchanges originating from, or extending to, local commercial numbers.

Off-premise extension
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.

Official public affairs activities
Defined in DODI 5400.13.

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 conservation.

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.

Operations and Maintenance, Army funding
Funds providing installation level NEC services and authorized on installation or equivalent The Army Authorization Documents System 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
An internal document, owned by the service management team, that defines the working relationship between different functional areas within an IT organization. The operational level agreement sets out the functions for the support and delivery of C4IM 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.

Outbound
A switched connection made from a domestic location to a nondomestic location.

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.

Personally identifiable information (PII)
Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, and biometric records, and so forth, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so forth.

Planning, programming, budgeting, and execution
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Platform information technology
Refers to computer resources, both hardware and software, which are physically a part of, dedicated to, or essential in real time to the mission performance of special-purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility-distribution systems such as water and electric.

Podcasts and video logs (vlogs)
Online audio and video blogs that can be downloaded to devices such as PCs or handheld devices (wireless phones, mp3 players, digital media players, and so forth). These can be subscription based or free, single-use or repeated use content.

Primary rate interface
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 kbps, and (c) in which the D channel also operates at 64 kbps. Note: The primary rate interface 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 Federal Communications Commission 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, ACOMs, 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 Key Infrastructure (PKI)
An enterprise-wide service (that is, data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption, and digital signature) that supports digital signatures and other public key-based security mechanisms for DOD functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. A PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable certification authority.

Public switched network
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.

Reimbursable basis
When installations have no organic NEC assests they must contract for the services or establish inter-Service support agreements with Army or other Services for NEC 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
A term that includes OPA and research, development, test, and evaluation 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.

Satellite Database
A database, administered by DISA for the Joint Staff, containing all CJCSI 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 Satellite Database authorizations.

Sensitive But Unclassified (SBU) Voice access line
A circuit connecting an SBU Voice (formerly DSN) subscriber (instrument or PBX and/or private administrative branch exchange) directly to a DSN switch.

Sensitive But Unclassified (SBU) Voice subscriber
An individual, station, installation, or location having direct access into an SBU Voice switch.

Sensitive But Unclassified (SBU) Voice user
An individual, station, installation, or location having access into the SBU Voice Network indirectly, that is, either by dialing a designated access code or placing a call through a local private branch exchange or through a console.

School transfer
Excess automation resources for which the Defense Information Technology Management System 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.

Segment
A defined area of obligation with functions and processes that contribute to mission accomplishment.

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
A coordinated set of tactical, Joint, and strategic initiatives to improve C4IM 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 reimbursable services delivered by an IT organization to a customer.

Service level indicators
Service level indicators are the performance metrics to be used to measure the agreed-upon levels of service as documented in SLAs for reimbursable services or service declarations for non-reimbursable services.

Service level management (SLM)
The disciplined, proactive process of envisioning, planning, developing, and deploying appropriate C4IM levels of service to all customers at an affordable cost. SLM is the coordinating process for all service management service delivery and service support processes.

Service management
The practice of overall management of C4IM services and their associated information infrastructure to meet customer requirements. Service management processes are categorized into the IT Service Lifecycle stages of: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. The Army Service Management Program is being developed after the ITIL Service Management concept model.

Service and network management
Service and network management is managing the network and the devices connected to it. Service and network management includes three management areas: Network Management (including network devices, servers, storage devices, and end-user devices like printers, workstations, laptops, and hand-held computers), 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.

Social networking sites (SNS)
Online networking platforms that allow registered users to interact with other users for social or professional purposes. Examples include MySpace, Facebook, and LinkedIn.

Standard data element
A data element that has been coordinated through the standardization process and approved for use in DOD information systems.

Shared database segment
A shared database segment 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.

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.

Sub-Segment
For purposes of IT architecture, sub-segment 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.

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 Network Enterprise Center (NEC)
The NEC is the installation information manager. As the installation NEC, 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
A functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole (Joint Publication 1–02).

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 NEC who has been appointed, in writing, by the 7th Signal Command Office of Acquisition, for the purpose of issuing DD Form 1367s against a Maximum Limits Communications Service Authorization.

Telecommunications device for the deaf/teletypewriter
A device that permits individuals with speech and/or hearing impairments to make and receive telephone calls without assistance from others. A telecommunications device for the deaf or telecommunications device for the deaf-compatible device will be used by the speech- and/or hearing-impaired user community to access the Federal Relay Service. A telecommunications device for the deaf 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 teletypewriter may also be used in referring to this type of device.

Telecommunications service request
A valid, approved, and funded telecommunications requirement submitted to DISA or DISA activities. Telecommunications service requests 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 in writing, by the installation commander supervising management and implementation of the installation telephone system usage control program.

Thin Client Computing
Refers to a computing architecture where computing occurs in the data center (installation processing node), rather than on an end user device (thick client). Thin client computing refers to the entire computing architecture, including: front end user devices, back end server and storage infrastructure, virtualized applications, operating system software, and personnel to implement, provide services, support, and sustain.

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.

Unified Capabilities (UC)
The integration of voice, video, and data services delivered ubiquitously across a secure and highly available infrastructure, independent of the technology, to provide increased mission effectiveness to the Warfighter and business communities**.**

Underpinning contracts
A contract with an external provider covering the delivery of goods and/or services that contribute to the delivery of C4IM 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 and/or TDA command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, and/or

otherwise applying doctrine, training, leader development, organizations, materiel, Soldiers 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.

Visible
Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes.

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
A Web browser, a Web server and their intended interaction. Web browsers and servers may communicate over the Internet and/or intranets.

Web logs (blogs)
A frequently updated, chronologically ordered publication of personal thoughts and opinions with permanent links to other sources, creating a historical archive. This can be published on personal Web sites or institutional Web sites as communication tools.

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 IP 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.

Wiki
Collaborative publishing technology that allows multiple users to work on and publish documents online with

appropriate version control. Wikis allow hypertext links to content in any form, enhancing user experience and interactions.

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.

World Wide Web
An Internet function for sharing of documents with text and graphic content that links documents locally and remotely.

Section III
Special Abbreviations and Terms

AAIC
Army Architecture Integration Center

ACAS
Army Centralized Access System

ACCT
Architecture Configuration Control Team

ACMO
Army Configuration Management Office

ADCCP
Army Data Center Consolidation Plan

ADMP
Army Data Management Program

ADP
Architecture development plan

AENC
Army Enterprise Network Council

ANCS
Army Network Campaign Strategy

ANS
Army Network Strategy

AONS
Architecture, operations, networks, and space

APL
Approved Products List

ArCADIE
Army Capability-based Architecture Development and Integration Environment

ARM
Asset and resource management

ASR
Army Service Request

ATO
Authority to operate

BGAN
Broadband Global Area Network

BMA
Business Mission Area

CDO
Chief Data Officer

CP–34
Career Program-34

CSS
Circuit switched service

CSTP
Commercial SATCOM Terminals Program

DDOE
DISA direct order entry

DIMA
Defense Intelligence Mission Area

DITCO
Defense Information Technology Contracting Office

DITPR
DOD IT Portfolio Registry

DOTMLPF–P
Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities - Policy

DSAWG
Defense Security and Information Assurance Working Group

DTH
DMS Transition Hub

DVS
Defense Video Services

DVS–G
Defense video services-global

EGB
Enterprise Governance Board

EIEMA
Enterprise Information Environment Mission Area

EMSS
Enhanced mobile satellite service

ESI
Enterprise software initiative

ETL
Data Extraction, Transformation, and Loading

FDCCI
Federal Data Center Consolidation Initiative

IADS
Integrated Architecture Data Standards

IASO
Information assurance support officer

IATO
Interim authority to operate

IEA
Information Enterprise Architecture

IEC
International Electrotechnical Commission

IEEE/EIA
Institute of Electrical and Electronic Engineers/Electrical Industries Association

ISO
International Organization for Standardization

ITIL
Information Technology Infrastructure Library

ITU–TSS
International Telecommunications Union-Telecommunications Standard Sector

JIST
Joint Integrated Satellite Communications Technology

LATA
Local Access and Transport Area

LH
long-haul

LMR
land mobile radio

LWN/MC
LandWarNet/Mission Command

MARS
Military Auxiliary Radio System

MDR
Metadata registry

NCS
Network Capability Set

PK
Public Key

POP
Point of presence

PSS
Packet switched service

QI
Quality of information

RHN
Regional hub nodes

SAC
Service access code

SAR
Satellite Access Request

SDP
Service delivery point

SLM
Service level management

SNS
Social networking sites

SOAP
Simple object access protocol

SORN
System of Records Notice

SOSE&I
System of Systems Engineering and Integration

SQL
Structured query language

SSO
Single sign-on

SVS
Switched voice service

TSACS
Terminal Server Access Control System

UC
Unified Capabilities

UDDI
Universal description, discovery, and integration

UID
Unique identifier

UPDM
Unified Profile for DODAF/Ministry of Defence Architecture Framework

VoIP
Voice over Internet protocol

VoSIP
Voice over secure Internet protocol

VTFs
Video teleconferencing facilities

WIDS
Wireless intrusion detection systems

WSDL
Web services description language