**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**
**15 July 2019**

**UNCLASSIFIED**

# SUMMARY of CHANGE

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

This administrative revision, dated 1 November 2022—

- Changes proponency from CIO/G–6 to Deputy Chief of Staff, G–6 (title page).

This major revision, dated 15 July 2019—

- Updates governance forums to include the Information Technology Oversight Council (table 2–1).
- Updates guidance contained in DODI 5000.02 (table 2–2).
- Establishes the requirement to obtain a Statement of Non-Availability for information technology procurements outside the Computer Hardware, Enterprise Software and Solutions process (para 2–6*c*(2)).
- Updates the information technology systems acquisition and delivery systems procurement strategies and procurement contracting organizations and removes references to legacy contracting organizations and centers (para 2–8).
- Updates Army guidance related to the redistribution and disposal of information technology assets to incorporate policies contained in cybersecurity regulations and pamphlets regarding the reuse of Army computer hard drives and sanitization of media (para 2–9).
- Introduces the Department of Defense information network and Department of Defense information network–Army terminology, processes, and services and replaces the previous legacy Global Information Grid references, terms, and processes (para 2–11).
- Replaces the legacy Global Information Grid waiver process with the new Department of Defense temporary exception to policy process for requesting connection exceptions for non-Defense Information System Network connections (para 2–26).
- Incorporates and updates previous content into new chapter 5 (formerly chap 3).
- Realigns, updates, and consolidates processes and procedures into new chapter 3 (formerly chap 5).
- Removes previous content about telecommunications and unified capabilities and refers all Army users to follow the policies, procedures, and guidance provided AR 25–13 (formerly chap 7).
- Updates telework program instructions (app B).
- Provides a new Army standard for life cycle replacement of information technology assets (app H).
- Incorporates detailed governance and network implementation guidance, processes, and procedures previously contained in AR 25–1 to this pamphlet and other Army regulations and pamphlets, as cited (throughout).
- Incorporates Army Directive 2016–18, Divesting Legacy Information Technology Hardware, Software, and Services in Support of the Army Network (throughout).

**Headquarters**
**Department of the Army**
**Washington, DC**
**15 July 2019**

# *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:

MARK A. MILLEY
*General, United States Army*
*Chief of Staff*

Official:

KATHLEEN S. MILLER
*Administrative Assistant*
*to the Secretary of the Army*

**History.** This publication is a major revision.

**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 the Army. It establishes procedures for the administration of information resources and the supporting technology requirements. This pamphlet supports AR 25–1 in implementing Public Law 104–106 and Section 2223, Title 10, United States Code. Chief information officer functions and those of corresponding information management and/or information technology official and management processes are delineated in 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 Regular 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. This pamphlet applies to platform information technology/industrial control systems; appropriated-funded morale, welfare, and recreation support systems; nonappropriated fund morale, welfare, and recreation support systems; and contractor-owned, contractor operated systems operated on behalf of the Army. During mobilization, this publication can be modified to support policy changes as necessary.

**Proponent and exception authority.** The proponent of this publication is the Deputy Chief of Staff, 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, its direct reporting unit, or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this publication 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 on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil.

**Distribution.** This pamphlet is available in electronic media only and is intended for the Regular 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 publication supersedes DA Pam 25–1-1 dated 26 September 2014.



**UNCLASSIFIED**

**Contents—Continued**

## Appendixes



## Table List



## Figure List

## Contents—Continued

# Chapter 1
# Introduction

## 1–1. Purpose
This pamphlet provides operational procedures and practical guidance to Army organizations furnishing and receiving Department of Defense information network–Army (DODIN–A) information technology (IT) services, products, and support. The Department of Defense information network (DODIN) includes DOD IT (for example, DOD owned or DOD controlled information systems (IS), platform IT systems, and IT products and services) that are operated by or on behalf of DOD components as defined in DODI 8500.01 and control systems and industrial control systems (ICS) as defined in National Institute of Standards and Technology (NIST) Special Publication 800–82. This pamphlet implements policies mandated by AR 25–1. It identifies and describes procedures, explicit and implied, stemming from DOD policies and federal authorities, to include Section 2223, Title 10, United States Code (10 USC 2223); 40 USC Subtitle III (known as the Clinger-Cohen Act (CCA)); 44 USC Chapter 35 (known as the Paperwork Reduction Act); and Office of Management and Budget (OMB) Circular A–130.

## 1–2. References and forms
See appendix A.

## 1–3. Explanation of abbreviations and terms
See the glossary.

## 1–4. Exceptions
This pamphlet does not address telecommunications services (see AR 25–13). AR 25–1 contains the overarching Army policy for records management, printing device management, 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 DA Pam 25–40. For visual information, see DA Pam 25–91. This pamphlet does not address procedural or practical guidance for cybersecurity (see AR 25–2). This pamphlet does not apply to embedded, real–time, or safety-critical vetronics and avionics systems (see AR 70–1).

## 1–5. Overview
*a.* The Army network is one of the key technological focus areas described in TRADOC Pamphlet 525–3–1. As an enabler of situational understanding across the Joint force, the network must, according to the Vice Chief of Staff, "empower leaders at the lowest levels with relevant combat information, situational understanding, and access to Joint and Army capabilities." TRADOC Pamphlet 525–3–1 calls for developing and modernizing "capabilities, such as cloud-enabled networks for mobile operations in austere environments and across wide areas," that are "simple and resilient, anticipating enemy efforts to disrupt communications." The world is evolving into an increasingly interconnected environment. The Army of 2020 and beyond will operate in a complex world where cloud-based computers receive data from tens of billions of devices. These computers will have the capacity to digest, correlate, contextualize, process, and then present data back to humans in a way that assists our decision-making process.

*b.* The Army is following industry best practices to transition to the cloud. Cloud-based networking requires assured and sufficient bandwidth. The Army is employing Multi-Protocol Label Switching (MPLS) and other transport upgrades designed to increase exponentially the throughput of our global "backbone" and the connectivity to posts, camps, and stations. With joint regional security stacks, the Army is transitioning from legacy security that protected data locally and required hundreds of security stacks to regionalized security that protects data in the cloud. The Army's application rationalization project will help reduce the number of applications the Army maintains (currently more than 25,000) and will modernize and move the remaining applications to the cloud. Once bandwidth is sufficient, security is applied, and data/applications reside in the cloud, the Army will then provide secure access to data from mobile devices. The end state is a global cloud-based network designed to provide Soldiers access to tailored and timely information at the point of need. As the network aggregates, processes, secures, and presents data in a way that is easily understood, Soldiers will be able to make more informed, effective decisions as they perform the missions of the future.

*c.* The Army is modernizing its network to prepare for the emerging data-driven, cloud-based world. While legacy networking architectures stored and protected data locally, cloud-based architectures will store and protect data in a

centralized yet distributed repository that enables global access. The Army's strategy for end-to-end network modernization is outlined in the Army Network Campaign Plan 2020 and Beyond and has five high-level lines of effort:

(1) *Provide signal capabilities to the force.* The Army's goal is to optimize the signal force to synchronize delivery of future capabilities and ensure effective operation and defense of a single end-to-end network by continually assessing and shaping doctrine, force structure, and equipping and training concepts across the operating and generating forces. In the end, signal forces will be structured, trained, and equipped to enable decisive action across the full range of military operations, business, and manufacturing with Joint force and unified action partners.

(2) *Enhance cybersecurity capabilities.* The Army's goal is to optimize defensive cyberspace operations and DODIN operations by continually assessing and shaping cybersecurity strategy, policy, doctrine, and resourcing to enhance the security of the network and information environment. The result will be a resilient network and information environment that assures survivability against highly sophisticated cyber adversaries.

(3) *Increase network throughput and ensure sufficient computing infrastructure.* The Army's goal is to lead and integrate Army strategy, policy, and resourcing to deliver a robust and secure transport and computing infrastructure that will enable assured warfighting and business operations. The Army sees an end state with a secure, resilient, and versatile global network infrastructure that gives the Army, including regionally aligned forces and unified action partners, the full range of military and business operational advantages across all Joint operational phases.

(4) *Deliver information technology services to the edge.* The Army's goal is to provide a consistent, end-to-end user experience by developing strategy, policy, resources, and change management for the transition of IT services from local implementations to enterprise capabilities. This will result in a global environment that offers integrated and timely access to relevant information, services, and applications at the point of need.

(5) *Strengthen Department of Defense information network–Army network operations.* The Army's goal is to optimize end-to-end network operations by leading the development of data and resource strategies and policies and an integrated architecture to establish common processes and standards, and to simplify and standardize capabilities in support of and integrated with DODIN operations. In the end, the Army will have a resilient, protected, multi-tiered, and rapidly configurable network that enables an information advantage for Army and Joint missions in cyberspace, supports Soldier requirements, and is responsive to the commander throughout all phases of operations and in all environments.

### 1–6. Pamphlet structure

The scope of this pamphlet includes all organizational levels. This pamphlet is structured into four disciplines: IT investment management, enterprise architecture, data management (DM), and IT solutions implementation:

*a. Information technology investment management.* (See chap 2.) This chapter addresses Army IT governance and the requirements for IT reporting, accountability, and compliance throughout the life cycle. It outlines the procedural information for IT planning, control, implementation and fielding, and evaluation of IT. Highlights of the chapter include IT governance, portfolio management, budgeting, resource management, acquisition delivery strategies, Army information technology service management (ITSM), IT career management, and IT performance management.

*b. Enterprise architecture.* (See chap 3.) This chapter provides guidance governing the composition and use of IT architecture documentation in the Army, including components of the architecture and governance.

*c. Data management.* (See chap 4.) This chapter covers Army information/DM policies and procedures and the Army's DM governance structure and operation.

*d. Information technology solutions implementation.* (See chap 5.) This chapter addresses network capacity regarding information transport and computing infrastructure; user facing services, including website management and procedural information for conducting privacy impact assessments (PIAs); and information on electromagnetic spectrum operations in accordance with AR 5–12.

## Chapter 2
## Information Technology Investment Management

### Section I

### Planning

### 2–1. Governance forums

*a.* The purpose of IT governance is to specify the authorities and decision-making mechanisms necessary to guide activities in carrying out the Chief Information Officer (CIO)/G–6 strategies and vision to manage IT. Mature processes are essential to ensure IT is aligned with the Army's strategic vision and operational direction. CIO/G–6 hosts

eight primary governance forums that support the enterprise information environment mission area (EIEMA): Chief Information Officer Executive Board (CIO EB), Migration Implementation and Review Council (MIRC), Army Enterprise Network Council (AENC), Information Technology Oversight Council (ITOC), Resource Integration Group (RIG), Army Data Board (ADB), Army Data Council (ADC), and the Army Standards Council (ASC) (see table 2–1). For more information and board charters, visit the CIO/G–6 governance web page at https://www.milsuite.mil/wiki/armycio/g-6_governance.

*b.* Other governance forums exist at the Headquarters, Department of the Army (HQDA) level to manage IT investments in the business mission area (BMA) (the Army Business Council (ABC), led by the Under Secretary of the Army; the warfighting mission area (WMA), the Mission Command (MC) General Officer Steering Committee (GOSC), and Army Warfighting Integration Council, led by Deputy Chief of Staff (DCS), G–3/5/7; the Department of Defense intelligence mission area (DIMA) (the Intelligence Senior Initiative Group) led by DCS, G–2; and the Army Cyber Council led by DCS, G–3/5/7, Cyber Director). These forums, as well as the AENC, validate IT requirements for resourcing and must be in line with CIO/G–6 priorities to be effective. CIO/G–6 staff participates as voting members and provides subject matter expertise to all of these forums.

**Table 2–1**
**Chief Information Officer/G–6 governance forums**

| Forum Name | Purpose/Scope |
|---|---|
| CIO EB | Purpose. The CIO EB provides strategic guidance and direction to the Army, related to the CIO's authority and duty to take action on all matters related to information resource management (IRM), cybersecurity, and IT architecture. The CIO EB ensures that stakeholders' needs and conditions are evaluated to develop balanced, enterprise-wide IRM, cybersecurity, and IT architecture objectives.<br><br>Scope. The CIO EB sets the strategic direction to achieve enterprise-wide IRM, cybersecurity, and IT architecture objectives through prioritization and decision making, and by monitoring performance and compliance against agreed direction and objectives. |
| AENC | Purpose. The AENC serves as an advisory body for Army-level decisions for strategic direction, policy development, and resource allocation related to the EIEMA within the IT investment portfolio. The AENC provides oversight for the management of the EIEMA to ensure investments deliver the expected benefits so that mission needs are met, solutions and services are delivered cost-efficiently, risk is identified and managed, and compliance with legal and regulatory requirements is achieved.<br><br>Scope. The EIEMA is comprised of the communications, computing infrastructure, core enterprise services, and cybersecurity (formerly information assurance (IA)) domains; management of which are informed by the Joint Capability Area (JCA) for Communications and Computers. |
| MIRC | Purpose. The MIRC serves as an advisory body chartered to advise, validate, and make recommendations on data center closures and application/system portfolio migration to the AENC for implementation of tasks specified within Army Directive 2016–38. The MIRC is a 3-star general officer (GO)/senior executive service (SES) governance forum, chaired by the Deputy CIO/G–6 and the Deputy Chief Management Officer. Using the MIRC as an advisory body, CIO/G–6 has oversight of the directive's implementation plan through the AENC.<br><br>Scope. The MIRC synchronizes the implementation plan across the Army; adjudicates and elevates requests to deviate from the implementation plan, as required; advises and recommends implementation plan changes; validates compliance with the implementation plan and assesses operational impacts of data center closures; and reports Army compliance with the implementation plan to the AENC. Quarterly, the Chair of the AENC reports implementation progress to the Senior Review Group. |
| ITOC | Purpose. The ITOC is a senior leader review group, co-chaired by the Under Secretary of the Army and Vice Chief of Staff of the Army designed to provide Army senior leaders with greater situational understanding of IT programs, investments, and resourcing. The ITOC is designed to integrate activities and assessments across the four IT mission areas: WMA, EIEMA, DIMA, and the BMA in order to provide guidance and direction, prioritize investment, allocate resources, and resolve conflicts.<br><br>Scope. CIO/G–6 serves as the Secretariat for the ITOC. It leads an integrated process team with the mission area leaders to develop a holistic IT strategy that includes commander and operator feedback and defined metrics for measurable outcomes and incorporates periodic outcome-based assessments. |

**Table 2–1**
**Chief Information Officer/G–6 governance forums—Continued**

| Forum Name | Purpose/Scope |
|---|---|
| RIG | Purpose. The RIG is a senior level advisory body co-chaired by CIO/G–6 and DCS, G–8. The RIG is chartered to advise the Program Budget Advisory Committee and the AENC on resourcing strategies; provide in-depth advice on financial aspects of the Army's network, including data flow, storage, and access; and provide input on all IT strategies for hardware (HW) sustainment and refresh policy through the planning, programming, budgeting, and execution (PPBE) process.<br><br>Scope. The RIG provides advice on synchronizing, integrating, and prioritizing the costs and resourcing for the Army's network, to include the WMA, BMA, and EIEMA mission areas, to inform the PPBE Process. |
| ADB | Purpose. The ADB serves as the senior Army data enterprise decision body for development of coordinated Army enterprise positions on data strategy, DM, standards management, and execution in conformance with the Army common operating environment (COE) architecture.<br><br>Scope. The ADB serves as the senior adjudication body across the Army enterprise for IT data and standards issues; acts as the final authority across the Army enterprise for standards, policies, and practices; coordinates data-sharing efforts across the Army enterprise; serves as a certification/waiver approval authority for targeted standards as delegated by the chief data officer (CDO); and collects and disseminates best practices and lessons learned for IT DM and standards communities. |
| ADC | Purpose. The ADC serves as the ADB's initial adjudication forum for data topics. Its membership consists of functional data managers (FDMs) identified by individual Army data stewards (DSs).<br><br>Scope. The ADC will coordinate adjudication of unresolved, internal data issues. If any issue remains unresolved, the Secretariat will escalate that issue to the ADB for resolution. Assists the ADB in the management and implementation the Army Data Management Program (ADMP), Army data strategy, and Army Information Architecture (AIA), ensuring that standardized Army data processes and procedures are consistently used. |
| ASC | Purpose. The ASC serves as the ADB's initial adjudication forum for all Army and Joint standards topics and processes. Its membership consists of standards managers identified by individual Army DSs.<br><br>Scope. The ASC will coordinate adjudication of unresolved and internal IT standards issues. Assists the ADB in coordinating the management and integration of standards–Related architecture and engineering products with Department of Defense Architecture Framework (DODAF) viewpoints; coordinating, integrating, and maintaining other related standards that may be identified as critical to the success of system interoperability; and ensuring that technology strategies are aligned with institutional Army transformation processes and warfighting strategies. |

## 2–2. Information technology planning

*a.* The IT planning strategy advances comply with 10 USC, 40 USC Subtitle III, 44 USC, and other statutes and regulations governing IT. IT planning uses IT resource analysis, including IT–Related management decision package (MDEP) and portfolio based reviews, program evaluation group (PEG) assessments, IT investment reviews (as domain portfolio reviews), 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, Programing, and Budget Committee; the MC GOSC; the ABC; CIO/G–6 governance forums; 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 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 IS investment projects.

(3) Providing for identifying IS 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.

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

(6) Evaluating the activity to ensure that the portfolio is meeting the outcomes described in paragraph 2–2*b*(2). Portfolios are monitored and evaluated against portfolio performance measures to determine whether to recommend continuation, modification, or termination of individual investments within the portfolio. This approach applies to all IT.

*c.* The IT portfolio is the central component of the IRM process and provides the structure for managing all IT–Related investments across the Army. The portfolio structure is aligned to four mission areas: WMA, BMA, EIEMA, and the Army segment of the DIMA. Structuring and aligning the portfolio to the four mission areas enable 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.

(1) The WMA encompasses the following domains: battlespace awareness, force application, focused logistics, force management, MC, protection, and training.

(2) The BMA encompasses the following domains: acquisition; financial management; human resources management; installation, energy and environment; logistics, and training.

(3) The EIEMA encompasses the following domains: communications, computing infrastructure, core enterprise services, and cybersecurity.

(4) The Army segment of the DIMA encompasses the following domains: analysis and production, exploitation, collection, dissemination, enterprise IT, enterprise management, and mission management (all DIMA domains apply specifically to intelligence and information operations).

*d.* The Army is transforming processes to deliver relevant, affordable, and interoperable infrastructure to the generating and operating forces while modernizing net-enabled solutions over time. A domain portfolio is comprised of new and existing doctrine, organization, training, materiel, leadership, personnel, and facilities solutions necessary to accomplish the strategic goals of the domain. This portfolio approach is built to synchronize and integrate all enterprise processes and to deliver improved IT solutions over time.

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

(1) CIO/G–6 reviews and approves the IT prioritization results and recommendations, which are the foundation of the command, control, communications, computers, and information technology (C4IT) investment strategy. As the functional proponent for the Army's C4IT investment strategy, 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 limited IT resources and are aligned with supporting enterprise initiatives for the Army.

(2) The results and recommendations ensure integration among the four mission areas.

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

*f.* CIO/G–6 investment strategy is developed through the collaborative efforts of the Army's multifunctional community of C4IT stakeholders that collectively determine the "best value" investment solutions for the Army's most critical C4IT requirements.

(1) The process incorporates strategic reviews, performance measures, capability gap assessments, risk assessments, and interdependency assessments each year for the four mission areas. To accomplish this task, 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. They have many functions, including:

*(a)* Representing their mission 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. 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.

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

*(d)* Rationalizing all existing and new solutions within their mission area, ensuring they adhere to an integrated architecture.

*(e)* 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 of key players is only a starting point and as required includes:

*(a)* MDEP managers and PEG resource managers/analysts, PEG integration team leads, and CIO/G–6 representatives to each PEG.

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

*(c)* Army warfighting functions and functional representatives.

*(d)* Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)); Deputy Assistant Secretary of the Army for Management and Budget; DCS, G–3/5/7; and DCS, G–8 leadership (as appropriate).

*(e)* Each Army command (ACOM), Army service component command (ASCC), direct reporting unit (DRU), U.S. Army Cyber Command (ARCYBER), U.S. Army Reserve (USAR) command, and Army National Guard (ARNG).

*(f)* Joint and DOD counterparts.

(4) The IT planning process links to the 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 C4IT 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 The Army Plan (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 four mission areas.

*(c)* Once the prioritization list and funding strategy is developed, they are briefed to 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) As part of the PPBE Process, involving the mission area 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 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. PEGs are responsible for prioritizing validated IT requirements within their portfolios for POM resourcing decisions and determining resource trades. The CIO/G–6-developed IT funding prioritization list must be coordinated with the PEGs to ensure synchronization of PEG resourcing decisions with the Army IT resourcing strategy. 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. Planning, programming, budgeting, and execution for information technology requirements and capabilities

Information resources management processes for planning, selecting, controlling, and evaluating IT align with the individual elements of the PPBE Process. 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.

*a. Planning.* Understanding the functional requirement for IT solutions 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.

*b. Information technology budget requirements identification.* IT budget requirements may be identified through the MDEP development process. For proper validation and to ensure appropriate resourcing, each MDEP manager must provide the resource requirements for an MDEP to the relevant PEG for the current POM. ACOM, ASCC, and DRU commanders may also identify urgent IT budget requirements through a narrative assessment of the ACOMs, ASCCs, and DRUs ability to accomplish its mission, identify significant shortfalls and internal resource adjustments, as well as adjustments with other ACOMs, ASCCs, and DRUs as part of the POM process.

*c. Guidance for the installation information infrastructure modernization program.* While the MDEP requirements process is generally implemented as stated in paragraph 2–3*b*, MDEPs contain many different requirements that demand tailoring by CIO/G–6 MDEP managers and DCS, G–8 PEG managers to ensure appropriate stakeholders are consulted for development, review, and requirements validation. The tailored process for capturing requirements for the Army's Installation-Information Infrastructure Modernization Program (I3MP) is as follows:

(1) *Installation functions.* Installations requiring I3MP IT infrastructure improvements generally elevate from the installation, to the Network Enterprise Center (NEC), to ARCYBER and to CIO/G–6 for planning, programming, and prioritization. Senior information management (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 C4IT 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) *Network Enterprise Center 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 (brigade or theater command). The theater commands will gather all I3MP requirements in their respective duty areas and forward to CIO/G–6 via ARCYBER for validation and prioritization.

(3) *U.S. Army Cyber Command functions.*

*(a)* Provides a technical control review and validates all enterprise-level fielding requirements.

*(b)* Validates all I3MP requirements and, in coordination with the theater commanders, develops a prioritized list of I3MP requirements.

*(c)* Reviews and approves the I3MP prioritization list and forwards to CIO/G–6 for final disposition.

(4) *Chief Information Officer/G–6 functions.* Army CIO/G–6 serves as the final approval authority for all requirements and requests for support from the I3MP. It also provides the Program Executive Office, Enterprise Information Systems (PEO EIS) with an integrated requirements list directing the priority in which the requirements are to be executed, along with funding source (MDEP) and Army program element (APE) to execute the material development of the capabilities required. This process is achieved as follows:

*(a) Coordinating program objective memorandum submissions.* In coordination with DCS, G–8; ARCYBER; and Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)), plan, program, and defend the Army I3MP program in the annual POM effort, as well as maintain oversight of resources garnered and ultimately obligated by the program.

*(b) Coordinating annual other procurement–Army prioritization.* In coordination with DCS, G–8; ARCYBER; and ASA (ALT), lead the annual I3MP other procurement–Army (OPA) prioritization staffing process and publish coordinated OPA priorities no later than the second quarter of the current fiscal year for implementation in the following fiscal year. Adjustments to OPA priorities are the exception and will be approved at the three 3-star level.

*(c) Managing Installation-Information Infrastructure Modernization Program requirements.* In coordination with ARCYBER, Assistant Chief of Staff for Installation Management (ACSIM), and ASA (ALT), publish and manage the global Army authoritative installation list aligned to I3MP investment requirements to ensure visibility of network modernization, divestiture, and other requirements in scope of the I3MP.

*(d) Verifying investment priorities.* Verify I3MP investment priorities and ensure requirements are consistent with Army and DOD policy in order to maximize the limited funds available.

*(e) Confirmation of Installation-Information Infrastructure Modernization Program requirements.* CIO/G–6 will confirm the I3MP integrated requirements list for the upcoming year of execution plus one year to product manager I3MP by 30 March annually. After 30 March, year-of-execution changes to the confirmed integrated requirements list will be coordinated with product manager I3MP as soon as feasible.

*d. Reporting.* CIO/G–6 reports the Army IT budget resources to Office of the Secretary of Defense (OSD), OMB, and Congress twice a year. The IT budget includes resources for any fiscal year of the Future Years Defense Program (FYDP). To ensure accurate reporting, Army Portfolio Management Solution (APMS) command administrators, system owners, and resource managers must verify record profile data and resource data by published dates, usually 15 August and 15 November each year. CIO/G–6 will issue specific guidance, but general rules are as follows:

(1) Report all Defense business systems (DBSs) individually. If DBSs share a funding line, users must split the funding and report funding in each individual record.

(2) All data centers must provide funding data in APMS (either directly or indirectly). Direct reporting means that the user will include (within the data center record in APMS) all data center costs required to build, operate, maintain, and close the data center. Indirect reporting means that if the data center hosts an IT asset in APMS, the owner of the IT asset will enter funding under their IT asset and select "Data Center" as the capability function.

(3) Verify and update all funding in the current FYDP.

(4) Update prior year funding to reflect actual obligations (one year appropriations).

(5) Correct all funding warning errors concerning years in the current FYDP. During the Army budget cycle, the funding information in the Army data warehouse may adjust due to funding decrements, transfers, adjustments, realignments, and reprogramming. This may cause previously valid funding lines to become invalid and warning errors will show in APMS.

(6) Avoid entering funding twice. For Non-DBS, if funding is provided via a parent record registered in APMS, do not enter the funding on the child record. Instead, indicate the parent name, acronym, and Army Information Technology Registry (AITR) number in the "Financial Comments" section. The funding cannot cross mission areas. For example, if the parent is registered in EIEMA and the child is registered in WMA, the funding must be split.

(7) Ensure that the IT budget module for all records are complete and accurate; the indicator button must be green. Refer to appendix C of the APMS Desk Side Reference Manual (DSRM) for instructions and definitions. The DSRM is found on the APMS home page https://cprobe.army.mil/enterprise-portal/web/apms.

(8) Ensure the name and descriptions do not contain undefined acronyms. The general rule for acronym use is to spell out the acronym on first use and then use the acronym afterwards.

## 2–4. Information technology resource management

*a.* The efficient and effective use of IT resources has a direct effect 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. CIO/G–6 oversees IT resourcing 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 C4IT MDEPs.

*b.* The management of Army information resources provides an integrated view for managing the entire IT life cycle. Information resource management uses a set of 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 (IEA), system engineering, cybersecurity, and IT acquisition), IRM 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.* C4IT planning is an integral part of 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 C4IT information resource process.

(1) CIO/G–6 is the principal focal point for Army 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) Senior IM/IT officials at ACOMs, ASCCs, DRUs, and installations must be engaged in the development of a similar process that supports both TAP and Army IRM 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 IRM, acquisition, contracting, and security 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.

## Section II

## Control

### 2–5. Army Portfolio Management Solution

*a.* In support of 40 USC Subtitle III (CCA), DOD portfolio management directives, and Public Law 108–375, the 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 allow the Army to manage IT investment spending by aligning IT investments to Army strategy and functional capabilities.

*b.* APMS provides 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, and is the authoritative data source (ADS) for, the Army's inventory of active IT investments and their associated systems and applications, as well as information system and application hosting environments. APMS is used for portfolio data collection, certification of funds in accordance with DBS certification guidelines, and consolidated reporting to OSD and Army requiring offices. APMS is the Army's feeder system to the Department of Defense Information Technology Portfolio Repository (DITPR). APMS includes functionality to register, delete, and transfer IT investment systems from the AITR.

*d.* APMS is used for three primary functions:

(1) Compliance reporting and other DOD directed reporting, including Standard Financial Information Structure/Public Law 104–208, infrastructure, CCA, data center closure, and cloud status reporting, as well as DBSs that require funds certification by the Defense Business Council in compliance with the provisions of the prevailing National Defense Authorization Act.

(2) Portfolio and investment management, to ensure HW, software (SW), or services in direct support of an IT investment are managed for strategic alignment, performance, environmental impact, risk, cost, redundancy, and gaps. All Army IT, including computing infrastructure, HW, SW, services, initiatives, prototypes, and investments, regardless of funding source or amount, must be registered or accounted for as a component of another record in APMS. Types of investments requiring an individual registration can be found in the APMS DSRM on the APMS home page. APMS is not an inventory of end-user computing devices, peripherals, or stand-alone SW. These investments can be accounted for using the "Common User Infrastructure" record. IT service contracts not in direct support of an investment (for example, an IT staff augmentation contract) do not have to be registered or accounted for in APMS. Any system requiring an accreditation, regardless of funding source or amount, must be registered. IT will not be double reported, but relationships can be identified using the "Dependencies" folder.

(3) To assist in the reporting of the Army's IT budget.

*e.* The APMS is the Army's feeder system to the DITPR. Reporting to DITPR is accomplished via an automated web service that pushes updated information from APMS nightly.

*f.* The APMS DSRM 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.

*g.* APMS is composed of the following modules:

(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 pushes updated information to DITPR 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 DBS certification.

(5) *Ad hoc reports.* Ad hoc reports provide the functionality to create and save tailored reports. There are two ad hoc reports, one with financial data elements and one without. The ad hoc with financial and ad hoc without financial

reports are available to all APMS account holders. The ad hoc with financials report is most applicable to administrators and analysts at the command, domain, and mission area levels.

*h.* All Army funded IT, including computing infrastructure, HW, SW, 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, and wireless robotic IT weapons platforms). Note that IT with wireless connectivity capability will need to be tracked through its life cycle but only for cybersecurity requirements.

(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, 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 business rules, see appendix C of this pamphlet.

## 2–6. Procurement of information technology requirements

*a. Requirement to use Computer Hardware, Enterprise Software and Solutions.* The Computer Hardware, Enterprise Software and Solutions (CHESS) system is the mandatory source for establishing commercial IT contracts for HW and SW, and the primary source for services (not applicable to IT HW or SW 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 HW and SW from a non-CHESS vendor requires a waiver from CIO/G–6. All waiver requests must include a rationale explaining the extenuating circumstances or unique configurations required by the mission that are not supported by CHESS. Waiver requests may be submitted through the CIO/G–6 website at https://cprobe.army.mil/enterprise-portal/web/itas/home. If additional assistance is needed, the CHESS helpline is available at 888–232–4405. Anyone may search or browse the CHESS website at https://chess.army.mil/. Users wishing to request a quote or execute a shopping cart must be logged in to the site.

(1) 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.

(2) 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.

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

(4) 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.

(5) Hardware acquired to support unified capabilities (UC) must be listed on the DOD UC approved products list (APL) at https://aplits.disa.mil/.

*b. Use of common hardware systems.* The common hardware systems (CHS) program office is the Army's mandatory source for commercial IT HW for tactical/operational requirements. All programs requiring commercial IT HW to meet an operational need are required to coordinate with CHS prior to entering post-milestone (MS) A activities.

(1) CHS support for commercial IT HW extends to organizations having requirements for:

*(a)* Configuration management (CfM).

*(b)* Transport or ruggedization.

*(c)* End-of-life configuration change support.

*(d)* Systems engineering support for HW modification or not well-defined requirements.

(2) DOD common access card (CAC) holders may browse the current CHS item catalog via the CHS website at https://www.kc.army.mil/chs/.

(3) Organizations having commercial IT HW requirements aligning with the CHS mission area described in paragraphs 2–6*a* and 2–6*b* may contact the CHS program office via email at usarmy.apg.peo-c3t.mbx.pd-chs-helpdesk@mail.mil to coordinate support for technology insertion requirements, HW ordering, or related task order services.

(4) CHS will refer supported organizations to CHESS for commercial IT requirements better aligned to the CHESS mission area.

*c. Information Technology Approval System* (*formerly Goal 1 waivers)*. AR 25–1 establishes Army policy for the procurement and sustainment of all IT HW, SW, and services. Information Technology Approval System (ITAS) waivers support OSD's IT consolidation initiative to achieve greater economies of scale, be more efficient, effective, and cost-consciousness of IT procurements by directing the use of CHESS, CHESS consolidated buys, and enterprise license agreements (ELAs). The ITAS 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 Army organizations requesting IT expenditures through sources other than product lead (PL) CHESS regardless of cost or procurement vehicle or funding source. Commands funding the purchase will request a waiver of this policy by using the ITAS website prior to purchase of all IT HW, SW, or services.

(2) *Procedures.* The Secretary of the Army policy memorandum dated 6 June 2013, subject: Army Waiver Process for Commercial-off-the-Shelf Information Technology (COTS IT) Procurement Outside the Computer Hardware, Enterprise Software and Solutions Program, provides guidance for the submission of requests for CHESS Statement of Non-Availability (SoNA) (available at https://army.deps.mil/army/cmds/hqda_ciog6/memos/forms/allitems.aspx).

(3) *Waivers.* All CHESS SoNA requirements are processed through the ITAS workflow process automation application. ITAS accounts must be requested by visiting https://cprobe.army.mil/urm/user/account/myaccount.

(4) *Operations tempo funding.* To migrate or reprogram Activity Group 11 operations tempo (OPTEMPO) funding (ground and air), Commands must submit an OPTEMPO funding migration request, in addition to an approved ITAS waiver.

*d. Purchase of energy-efficient information technology equipment.* All purchases of IT equipment, including computers, laptops, monitors, and other peripheral equipment (for example, printers, scanners, 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 (additional information is available at https://www.epa.gov/greenerproducts/electronic-product-environmental-assessment-tool-epeat).

*e. Commercial information technology management process.*

(1) The management of enterprise SW licenses and services requires oversight and approval of CIO/G–6 and DCS, G–8 staff in accordance with CIO/G–6 guidance. CIO/G–6 provides direction and guidance to CIO/G–6 and DCS, G–8 staff for the validation of license entitlements on a (monthly or quarterly) basis through vendor sales reports to guarantee license compliance/ownership and the annual SW license inventory audit of command-owned entitlements to assure contractual terms and conditions are met. CIO/G–6 will approve and oversee all license reassignment requests to confirm CIO/G–6 and DCS, G–8 staff agree with the fiscal sustainment obligation of impending maintenance costs.

(2) CIO/G–6 will coordinate with command CIOs to report information critical to managing license inventory and developing IT requirements. All Army command CIOs will receive notice from CIO/G–6, 30 days prior to contract award or renewal, defining the reporting criteria of required information and frequency of subsequent data collection. Reporting parameters are subject to change in accordance with the enterprise agreement contract terms and/or new requirements. Command CIOs are responsible for reporting critical information and responding to follow-up surveys from CIO/G–6 per ELA via the SharePoint site (https://army.deps.mil/army/cmds/hqda_ciog6/pr/prl). CIO/G–6 will maintain this site as a repository of all the collected data. While the data collection will initially be a manual process, CIO/G–6 intends to automate the process as much as possible in the future.

(3) Army commands requesting specific SW or services not offered under an enterprise agreement managed by CIO/G–6 or PL CHESS, must obtain a SoNA from PL CHESS prior to submission of a waiver request through CIO/G–6 ITAS in accordance with paragraph 2–6*c*. CIO/G–6 will analyze data from approved waivers to identify potential future enterprise agreements.

(4) Modified table of organization and equipment (MTOE) unit's mission-essential common COTS IT equipment must be procured in accordance with the COTS information technology management (ITM) 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 ITM process, U.S. Army Training and Doctrine Command (TRADOC) assesses and determines requirements by organization, and DCS, G–8 validates requirements and resources requirements into POM submissions.

(5) MTOE units will use CTA 50–909 to request, purchase, or replace COTS IT HW 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.

## 2–7. Management and accountability of internal use software

CIO/G–6 is co-developing comprehensive guidance with ASA (FM&C); ASA (ALT); and DCS, G–4 in order to provide detailed instructions to commands on how to account for their respective internal use SW assets. This guidance will be published accordingly.

## 2–8. Army information technology service management

*a.* The DOD CIO recognizes that efficient and effective management of IT services is a critical component of the DOD enterprise strategy and roadmap. Central to that principle is the application of a standard ITSM approach across DOD for the quality delivery of IT services to DOD customers. The Defense Enterprise Services Management Framework (DESMF) is a DOD-level ITSM framework that provides a set of standards for managing IT services and establishes clear service management requirements for the acquisition and contracting of IT services and capabilities across DOD based on industry best practices.

*b.* Using DESMF as a guidance, the Army enterprise service management (AESM) is the Army's approach to managing IT enterprise services. It ensures Army investments in services meet user needs by standardizing a holistic and integrated approach to delivering IT services. Through the implementation, management, and continual improvement of ITSM processes, the Army enterprise will benefit with more efficient and effective standards, methods, and practices. The Army ITSM policy, initiated by CIO/G–6, set forth the establishment of the Army Enterprise Service Management Framework (AESMF) to provide the necessary support for the AESM.

*c.* CIO/G–6, as the executive sponsor of the AESMF, will coordinate with ARCYBER and other key stakeholders in developing and executing future revision of the AESMF.

*d.* U.S. Army Network Enterprise Technology Command (NETCOM) will serve as the executive manager and lead for the AESM and report to the AENC on all matters related to ITSM.

(1) The AESMF is the Army's solution for managing IT services. It enhances processes, improves metrics, manages reporting and provides better information on existing IT services, improves quality of communications, clearly defines duties and functions, and clarifies the view of current IT services.

(2) The AESMF uses five IT service life cycle stages to continually identify opportunities to improve IT services that are delivered to the end users. Within each of the five IT service life cycle stages are descriptions of essential IT processes along with comprehensive tasks and procedures to enable commanders to direct and control network resources with situational awareness. There are 32 processes in the AESMF. The 5 life cycle stages and 32 processes are displayed in table 2–2. For further description on each of the life cycle stages or processes and functions, as well as the governance structure, please review the AESM concept of operations (CONOPS) document (available at https://army.deps.mil/army/cmds/hqda_ciog6/pr/pru/hqda-itsm/aesmdocsfinal/aesm%20conops%20v1_0%20final%2016%20dec%202014.pdf.)

**Table 2–2**
**Army Enterprise Service Management Framework life cycle description**

| AESMF Life Cycle Stages | Processes and Functions | Accountable | Responsible | Consulted | Informed |
|---|---|---|---|---|---|
| Service Strategy | Strategy Generation Management | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | IT service owners | Total force |
| | Business Relationship Management | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | IT service owners | Total force |
| | Demand Management | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | IT service owners | Total force |
| | Financial Management for IT Service | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | IT service owners | Total force |
| | Service Portfolio Management | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | IT service owners | Total force |
| | Service Catalog Management | CIO/G–6 | CIO/G–6 | IT service owners | Total force |

**Table 2–2**
**Army Enterprise Service Management Framework life cycle description—Continued**

| AESMF Life Cycle Stages | Processes and Functions | Accountable | Responsible | Consulted | Informed |
|---|---|---|---|---|---|
| | | | ASA (ALT)<br>NETCOM | | |
| Service Design | Design Coordination | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | NETCOM | Total force |
| | Availability Management | CIO/G–6 | ASA (ALT)<br>NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | Capacity Management | CIO/G–6 | ASA (ALT)<br>NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | Information Security Management | CIO/G–6 | ASA (ALT)<br>NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | IT Service Continuity Management | NETCOM | ASA (ALT)<br>NETCOM | CIO/G–6<br>ASA (ALT)<br>NETCOM | Total force |
| | Service Level Management (SLM) | NETCOM | ASA (ALT)<br>NETCOM | CIO/G–6<br>ASA (ALT)<br>NETCOM | Total force |
| | Supplier Management | ASA (ALT) | ASA (ALT) | CIO/G–6<br>NETCOM | Total force |
| | Engineering Function | ASA (ALT) | ASA (ALT)<br>NETCOM | CIO/G–6<br>NETCOM | Total force |
| Service Transition | Transition Planning and Support | ASA (ALT) | ASA (ALT)<br>NETCOM | CIO/G–6<br>NETCOM | Total force |
| | Asset Management | CIO/G–6 | ASA (ALT)<br>NETCOM | NETCOM | Total force |
| | Change Management | CIO/G–6 | ASA (ALT)<br>NETCOM | NETCOM | Total force |
| | Change Evaluation | ASA (ALT) | Project/Program Management | CIO/G–6<br>NETCOM | Total force |
| | CfM | NETCOM | NETCOM | CIO/G–6<br>ASA (ALT)<br>NETCOM | Total force |
| | IT Services Knowledge Management | NETCOM | NETCOM | CIO/G–6<br>ASA (ALT)<br>NETCOM | Total force |
| | Release and Deployment Management | ASA (ALT) | Project/program management | CIO/G–6<br>NETCOM | Total force |
| | Service Validation and Testing | NETCOM | NETCOM | CIO/G–6<br>NETCOM | Total force |
| | Access Management | NETCOM | NETCOM | CIO/G–6<br>NETCOM | Total force |
| | Event Management | NETCOM | NETCOM | CIO/G–6<br>ASA (ALT)<br>NETCOM | Total force |
| | Incident Management | NETCOM | NETCOM | CIO/G–6 | Total force |

**Table 2–2**
**Army Enterprise Service Management Framework life cycle description—Continued**

| AESMF Life Cycle Stages | Processes and Functions | Accountable | Responsible | Consulted | Informed |
|---|---|---|---|---|---|
| | | | | NETCOM | |
| | Problem Management | NETCOM | NETCOM | NETCOM | Total force |
| Service Operations | Request Fulfillment | NETCOM | NETCOM | CIO/G–6<br>NETCOM | Total force |
| | Service Desk Function | CIO/G–6 | NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | Application Management Function | NETCOM | NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | IT Operations Management Function | NETCOM | NETCOM | ASA (ALT)<br>NETCOM | Total force |
| | Technical Management Function | NETCOM | NETCOM | ASA (ALT)<br>NETCOM | Total force |
| Continual Service Improvement | Seven Step Improvement Process | CIO/G–6 | CIO/G–6<br>ASA (ALT)<br>NETCOM | AESM team | Total force |

## 2–9. Information technology systems acquisition and delivery strategies

*a. Clinger-Cohen Act.* On February 10, 1996, the President signed Public Law 104–106 containing the Information Technology Management Reform Act (Division E) and the Federal Acquisition Reform Act (Division D). These acts were subsequently incorporated into 40 USC Subtitle III. CIO/G–6 is responsible for CCA compliance. CCA is a statutory requirement that requires a compliance determination. CCA authority determinations are made by the organizations shown in figure 2–1.

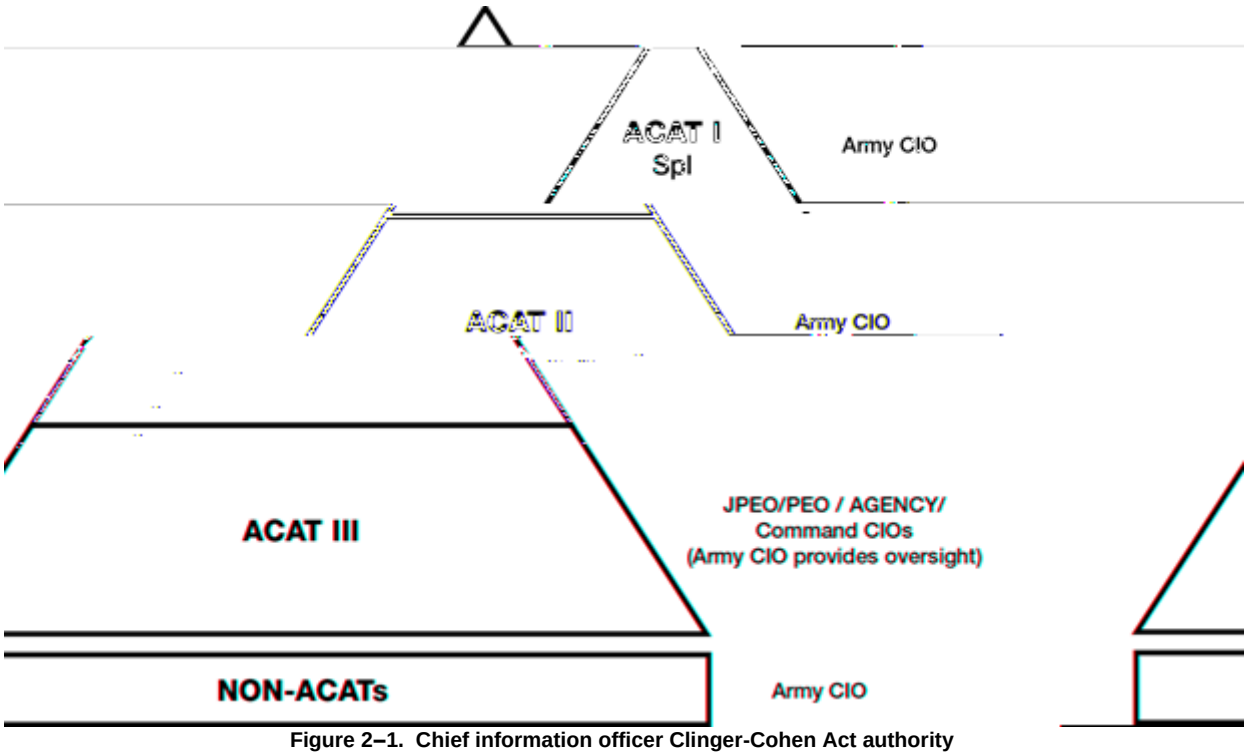


**Figure 2–1. Chief information officer Clinger-Cohen Act authority**

*b. Business process.* The Army acquisition business enterprise portal is CIO/G–6's automated information system (AIS) tool (https://acqdomain.army.mil) operated by PEO EIS and used to assess CCA 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. Review and approve the Army position for acquisition category (ACAT) identification and ACAT sub-category IAM programs at each decision MS before the Defense Acquisition Board or IT Acquisition Board review. This includes the review and approval of acquisition program baselines (APBs) (see DODI 5000.02, DODI 5000.74, and DODI 5000.75).

(1) The CCA assessment determination is made by CIO/G–6 for all ACAT I, II, and special interest programs.

(2) ACAT III assessment determinations are made by the assigned Joint program executive office (PEO), PEO agency, or command CIO (see AR 70–1 and AR 25–1). Upon completion of the compliance determination, the assigned organization CIOs are required to forward a copy of the determination to CIO/G–6. CIO/G–6 reports ACAT III compliance results semi-annually in an oversight role.

(3) Non-ACAT assessment determinations are made by the assigned Joint PEO, PEO agency, or command CIO (see AR 25–1).

(4) The specific CCA procedures and policies for a program can be affected by:

*(a)* Whether the program is designated as a Major Defense Acquisition Program or a Major Weapons System.

*(b)* Determination that the program is an Information System, a DBS, or responds to an urgent need.

(5) The CCA assessment determination is made by CIO/G–6 for all ACAT I, II, and special interest programs, in accordance with DODI 5000.02, Table 10.

(6) Table 2–2 provides an example that identifies the specific requirements for CCA compliance. These CCA requirements will be satisfied to the maximum extent practicable through documentation developed under the Joint Capabilities Integration and Development System (JCIDS) and the Defense Acquisition System. The PM will prepare a table similar to table 2–2 to indicate which documents demonstrate compliance with the CCA requirements. Table 2–3 summarizes the requirements levied on all programs that acquire IT, including National Security Systems (NSS), at any ACAT level.

**Table 2–3**
**Clinger-Cohen Act compliance example**

| Actions Required to Comply with the CCA (40 USC Subtitle III)[1] | Applicable Program Documentation[2] |
|---|---|
| 1. Make a determination that the acquisition supports core, priority functions of the DOD.[3] | Initial capabilities document (ICD), IS ICD, or urgent need requirements documents |
| 2. Establish outcome-based performance measures linked to strategic goals.[3, 4] | ICD, IS ICD, capability development document (CDD), capability production document (CPD), analysis of alternatives (AoA), APB[7] |
| 3. Redesign the processes that the system supports to reduce costs, improve effectiveness, and maximize the use of COTS technology.[3, 4] | ICD, IS ICD, CONOPS, AoA, business process reengineering |
| 4. Determine that no private sector or government source can better support the function.[4, 5] | Acquisition strategy, AoA |
| 5. Conduct an analysis of alternatives.[4, 5] | AoA |
| 6. Conduct an economic analysis that includes a calculation of the return on investment; or for non-AIS programs, conduct a life cycle cost estimate.[4, 5] | Component cost estimate, component cost position, program economic analysis for major automated IS programs |
| 7. Develop clearly established measures and accountability for program progress.[4] | Acquisition strategy, APB[7], test and evaluation master plan (TEMP)[7] |
| 8. Ensure that the acquisition is consistent with the DOD information enterprise policies and architecture, to include relevant standards.[4] | CDD net–Ready key performance parameter (NR–KPP), CPD NR–KPP, information support plan (ISP) |
| 9. Ensure that the program has a cybersecurity strategy that is consistent with DOD policies, standards, and architectures, to include relevant standards.[4] | Cybersecurity strategy, program protection plan, Risk Management Framework (RMF) security plan |
| 10. Ensure, to the maximum extent practicable, modular contracting has been used and the program is being implemented in phased, successive increments, each of which meets part of the mission need and delivers measurable benefit, independent of future increments.[4] | Acquisition strategy |
| 11. Register Mission-Critical and Mission-Essential systems with the DOD CIO.[4, 6] | DITPR |

Notes:

[1] DODI 5000.02, Table 2indicates when the program manager must report CCA compliance.

[2] The system information and documents cited are examples of the most likely, but not the only references for the required information. If other references are more appropriate, they may be used in addition to or instead of those cited. Include page(s) and paragraph(s), where appropriate. Urgent needs may cite the associated urgent needs documentation to demonstrate CCA compliance; for example, the course of action and/or the network connection documentation.

[3] These requirements are presumed to be satisfied for weapons systems with embedded IT and for command and control (C2) systems that are not themselves IT systems.

[4] These actions are also required to comply with Section 811, Public Law 106–398.

[5] For NSS, these requirements apply to the extent practicable (see 40 USC 11103).

[6] Mission-Critical Information System. A system that meets the definitions of "information system" and "national security system" in 40 USC Subtitle III, the loss of which would cause the stoppage of Warfighter operations or direct mission support of Warfighter operations. (The designation of mission-critical will be made by a DOD component head, a combatant commander, or their designee). A financial management IT system will be considered a mission-critical IT system as defined by the Under Secretary of Defense (Comptroller) (USD(C)). A "Mission-Critical Information Technology System" has the same meaning as a "Mission-Critical Information System."

Mission-Essential Information System. A system that meets the definition of "information system" in 44 USC 3502, that the acquiring DOD component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The designation of mission-essential will be made by a DOD component head, a combatant commander, or their designee). A financial management IT system will be considered a mission-essential IT system as defined by the USD(C). A "Mission-Essential Information Technology System" has the same meaning as a "Mission-Essential Information System."

[7] The APB and TEMP may be submitted in draft to expedite program assessment.

*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 IM systems. The engineering and management focus is enterprise resource planning to meet Army's current and future mission requirements. This vision standardizes business IM systems through enterprise resource planning SW

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 07806–5000.

*d. Procurement strategies.* Customers and providers of IS must be aware of the various procurement approaches available for acquiring IT systems and services. As the Army's SW product manager within the DOD enterprise software initiative (ESI) program, PL CHESS has oversight functionality for the DOD ESI and has a duty to evaluate business case analysis for Army and DOD component bulk purchases of enterprise SW licenses from approved ESI agreements in order to obtain additional volume level discounts/cost savings. CHESS is the mandatory source for purchases of COTS IT SW, desktops, notebook computers, and all other IT purchases (regardless of dollar value) and CHESS is the preferred source for acquiring IT services (regardless of dollar value). If a contract vehicle is not available on a CHESS contract, DOD ESI, or the federal supply schedule (FSS) and the requirement is greater than the simplified acquisition threshold, the customer should contact the U.S. Army Contracting Command 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. Nonappropriated fund (NAF) procurement rules will follow these procedures unless additional guidance is promulgated by the U.S. Army Installation Management Command.

(1) IM/IT offices may select from various contract vehicles and techniques to meet their requirements. Multiple approaches may need consideration to meet both short and long-term requirements.

(2) There is no single acquisition strategy that is ideal for every situation. The best acquisition approach for a particular project or program is only determined after examining each requirement's many objectives and environments. The customer must be aware that contract offices may vary in the quality of service and the amount of industrial funding fees charged for clerical costs. Another issue is the variation in the timelines of service in different vehicles. Managers must build a business case for each option and then decide, based on cost, performance, and risk management factors.

*e. 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 Federal Acquisition Regulation (FAR) available at https://www.acquisition.gov/far/. The practice of designating a preferred source for a specific order is prohibited under the FAR, as it denies the U.S. Government (USG) the benefit of continuous, streamlined, commercial-style competition gained from the fair opportunity process.

*f. Micro-purchases.* A micro-purchase is a simplified acquisition procedure for equipment purchases under $5,000 and up to $3,000 for services. 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.

(1) 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 (GPC) 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).

(2) 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.

*g. 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 General Services Administration (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.* USG leases resources for a base period and may have an option for more periods.

*(b) Lease-to-ownership plan.* USG leases items for a period, after which lease payments end and USG takes title.

*(c) Lease with option to purchase.* USG leases items for a period with an option to purchase later. USG 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 HW 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 SW (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. However, 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.

*h. Standard contract vehicles.* 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.

(1) *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.

(2) *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 on.

*i. Other information technology acquisition and delivery options.* CHESS has an array of fully competed contract vehicles to meet Army requirements for purchasing IT of all types (including procurement of commercial cloud service offerings and technical support to transition Army applications to a commercial cloud environment). 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 SoNA, and CIO/G–6 must grant an approved ITAS waiver. A complete list of CHESS contracts, DOD ESI, ELA/enterprise software agreements, information technology enterprise solutions-software, and the SoNA/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 HW and SW maintenance, CfM, 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 (DWCF) 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 HW, executive SW, system administration, personnel, and facility costs; increased standardization and interoperability; and enhanced security.

*(c)* Mainframe information processing is available to the military services and DOD agencies at five Defense Enterprise Computing Centers (DECCs): St. Louis, MO; Mechanicsburg, PA; Columbus, OH; Ogden, UT; and Oklahoma City, OK. Most Army mainframe processing is supported by DECC St. Louis. Non-mainframe information

services are provided at various Defense Information Systems Agency (DISA) regional support activities throughout the continental United States (CONUS).

*(d)* Additional information on DECC services may be obtained from CIO/G–6, Army Data Center Consolidation Plan (ADCCP).

(5) *U.S. Army Communications-Electronics Command/Software Engineering Center.* The Software Engineering Center provides SW support and SW engineering products and services throughout the Army and DOD and may be contacted at U.S. Army Communications-Electronics Command (AMSEL–CG), 6002 Combat Drive, Aberdeen Proving Ground, MD 21005–1845. Their services include integration of battlespace and sustaining base systems; command, control, communications, computers, and information management (C4IM) electronic warfare and sensors; avionics; sustaining base and business systems SW architecture and technology; consulting SW acquisition; postproduction SW support; SW development and prototyping SW; contract administration; and interoperability engineering.

## 2–10. 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 (DLA) is the executive agent of DRMS for DOD. Obtain and follow official disposition instructions from DLA as appropriate (see www.dla.mil/dispositionservices.aspx).

*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 website at www.dla.mil/dispositionservices.aspx.

*c.* Army organizations will divest themselves of legacy equipment as it is replaced by new IT equipment and associated capabilities. Specifically, take appropriate actions to:

(1) Decommission unnecessary switches and routers.

(2) Ensure that the divestiture of IT equipment aligns with the Army's implementation of black core network architecture for MPLS. Decommission post, camp, and station enclaves when MPLS black core architecture is available for use.

(3) Terminate contracts for legacy HW, SW, or IT services that are no longer in use or that have been replaced by updated versions. To prevent unnecessary expenses related to contract terminations, ensure that the cost of early termination does not exceed the cost of continuing the contract through its expiration date.

(4) Make sure contract option years are not exercised for IT HW, SW, or services no longer in use.

(5) Ensure that HW and SW from existing contracts continue to meet current cybersecurity requirements and comply with security technical implementation guides (STIGs) for the duration of their use (STIGs may be viewed at https://iase.disa.mil/stigs/pages/a-z.aspx).

(6) Verify that operation and maintenance costs are not being paid on unused HW or SW, including applications and circuits.

(7) Ensure that divested equipment is removed from corporate databases and contracts that support the equipment.

(8) Delete the divested equipment from the APMS database.

(9) Dispose of unused equipment above the level the command established for contingency stock (inventory held to meet ad hoc requirements or unexpected demand) or transfer the equipment to a location of need, as long as the equipment is deemed necessary and meets security standards established in AR 25–2, this pamphlet, and related IT security documents.

*d.* 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 and associated cybersecurity pamphlets related to the reuse of Army computer hard drives and sanitization of media. All Army GPC IT purchases must be accounted for in APMS and obtain necessary ITAS approvals from CIO/G–6 before acquisition is done.

*e.* 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 and supporting cybersecurity pamphlets related to the reuse of Army computer hard drives and sanitization of media. 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.

*f.* 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 DLA Form 2500 (Certificate of Hard Drive Disposition) or equivalent.

(5) Name, rank/grade, and signature of individual certifying the information.

(6) Remove 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) Remove of the following computer media and cards from all turn-in computer equipment: compact flash cards, secure data cards, optical media, smart card media, micro-drives, multimedia cards, memory sticks, Personal Computer Memory Card International Association cards, backup tapes, floppy diskettes, and zip media.

*g.* Turn-in procedures for computers with hard drives require the following:

(1) Ensure that the hard drive (notebooks, desktops, laptops, and docking stations) has been degaussed or overwritten in accordance with procedures outlined in supporting cybersecurity pamphlets related to the reuse of Army computer hard drives and sanitization of media.

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

(3) Label 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. Labeling the hard drive using DLA Form 2500 or equivalent.

(5) 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, micro-drives, multimedia.

*(c)* Memory cards, memory sticks, Personal Computer Memory Card International Association cards, backup.

*(d)* Tapes, floppy diskettes, and zip media.

(6) A label on chassis using DLA Form 2500 or equivalent.

(7) Name, rank/grade, and signature of individual certifying the information.

(8) Remove memory sticks from other forms of computer equipment, such as handheld computers (palm pilots, organizers, and so on).

*h.* 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 DLA Form 2500 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."

*i.* Turn-in procedures for all other computer–Related devices that do not fall under the category of classified, tempest, or hazardous waste require the following:

(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 are 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 as scrap.

(4) Remove monitors, printers (toner must be removed), keyboards, speakers, modems, mouse, plotters (toner must be removed), and external devices.

*j.* Turn-in procedures include the following:

(1) Hand–Receipt holders will—

*(a)* Turn-in to the unit property book office 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 property book officer will prepare DA Form 3161 (Request for Issue or Turn-In) required for disposal or redistribution.

## 2–11. Use of government purchase cards for purchase of information technology assets

*a. Use of the government purchase card.* The GPC (more formally referred to as the government-wide commercial purchase card) can be used to procure and pay for purchases of COTS IT HW and SW, with CHESS as the mandatory source for these purchases. CHESS contracts are the preferred source for the acquisition of IT services. 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 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 BPA).
(6) Make payments, when the contractor agrees to accept payment by the card.

*b. Government purchase card benefits.* The use of the GPC 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 checks mandatory sources before purchase and ensures 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 information technology purchases.* The senior IM official approves purchases. Written approval must be obtained from the appropriate command authority before purchase. Consumable items such as ribbons, toner cartridges, and so on, are authorized for purchase using the purchase card without senior IM official approval.

## 2–12. Joint capabilities

*a. General.* The biggest challenge that the DOD faces is to improve the speed and quality of decision making by connecting information producers and consumers more effectively through IT and net-centricity. DODIN enterprise services are a suite of information, web, and computing capabilities that will improve user access to mission-critical data. DISA DODIN enterprise services will provide access anytime and anywhere to reliable decision-quality information using cutting-edge, web-based, networked services.

*b. Department of Defense information network enterprise services.* The DISA DODIN enterprise services, consisting of HW, SW, 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. DISA DODIN enterprise services enable DOD information and decision superiority from the command center to the Warfighter.
(5) The DISA DODIN 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 CAC or DOD Public Key Infrastructure (PKI) certificate for access.

*c. Enterprise services management and network operations.* This set of services provides end-to-end DISA DODIN performance monitoring, CfM, 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 911and 411, encompasses general help desk and emergency support to users. Beyond these common core services, the DODIN–A/MC mission areas and domains, and the DOD/Army community of interest (COI) 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 workgroup SW.

(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) *Cybersecurity.* 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 III

## Implementation and Fielding

### 2–13. Army interoperability certification and baseline configuration management

*a. General.* All Army IT or NSS are required to achieve an Army interoperability certification (AIC) to have access to the network authorized. Successful AIC testing demonstrates compliance with DOD and Army policies. CIO/G–6 will issue AIC memorandums that indicate what systems and SW 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. 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 within the WMA is conducted within the Federation of Net-Centric Sites (FaNS) distributed testing environment with the Central Technical Support Facility, the test agent for CIO/G–6, at Fort Hood, TX. BMA systems must coordinate with the CIO/G–6 test agent for their certification event. If the test agent cannot support their request, the system owner must contact the CIO/G–6 action officer for approval of an alternate location that can support the event. CIO/G–6 (SAIS–CB) manages the AIC certification process and ensures Army systems have approved ISPs, meet entrance and exit AIC criteria, have no test incident reports (TIRs) impacting end-to-end system interoperability, and government materiel developers (MATDEVs) or PMs comply with associated CIO/G–6 CfM requirements. Any questions regarding the AIC process should be directed to CIO/G–6 (SAIS–CBC) by email at usarmy.pentagon.hqda-cio-g-6.list.aic-guidance-npe-mgt@mail.mil.

*b. Army interoperability certification approval authorities.* CIO/G–6 is the certification authority for Army interoperability and activities associated with the certification of interoperability. To ensure timely and relevant support for the Soldier, CIO/G–6 has delegated authority for specific certification activities. Below are the signatory authorities for the following interoperability certification activities:

(1) Director, Cybersecurity & Information Assurance (SAIS–CB), is the approval authority for all Army IT NSS AIC determinations.

(2) Director, Cybersecurity & Information Assurance (SAIS–CB), is the approval authority for all Army IT/NSS AIC non-certification determinations.

(3) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for all Army IT/NSS modification to the baseline determinations.

(4) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for all AIC waiver determinations.

(5) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for all AIC exemption determinations.

(6) Director, Cybersecurity & Information Assurance (SAIS–CB), is the approval authority for all Army interoperability capabilities and limitations (IC&L) Assessments of an IT/NSS.

(7) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for AIC fielded baseline approvals.

(8) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for the interoperability verification and validation accreditation (IV&VA).

(9) CIO/G–6 is the approval authority for all FaNS accreditations.

(10) Chief, Interoperability, Certification and Acquisition (SAIS–CBC), is the approval authority for all AIC test plans.

*c. Entrance criteria for an Army interoperability certification testing event.*

*Note.* To facilitate Joint certification, program representatives are requested to contact CIO/G–6 (SAIS–CBC) prior to contacting the Joint Interoperability Test Command for Joint test event coordination. 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.

(1) Government MATDEV, PM, or system owner of any IT or NSS is responsible for meeting all entrance criteria before 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 address the following:

*(a)* Authority to operate (ATO). Include the status of any current RMF authorizations, to include an ATO with plan of action and milestones (POA&M) approved by the system's authorizing official (AO). Attach a copy of existing approvals.

*(b)* Information assurance vulnerability management (IAVM) compliance and POA&M.

*(c)* ISP. Provide the status of the system's ISP.

*(d)* Mission threads. Provide the status of TRADOC developed and approved mission threads. If Combined Arms Service Support Command or TRADOC does not support BMA mission threads, system owners must provide Government Accountability Test test cases to support their AIC event.

*(e)* Configuration Control Board approval.

*(f)* Funding AIC test costs.

(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 SW for the test event so CIO/G–6 approved CfM procedures can be applied to ensure test site configuration control. The MATDEV or PM is required to provide all pertinent SW artifacts. Memorandum from the government MATDEV or PM must be provided that establishes the submitted SW 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)* Scope and content of the AIC test site test plan.

*d. Program executive officer-self-determination.* Program executive officers have been authorized by CIO/G–6 to approve minor SW changes to currently CIO/G–6 AIC certified systems that have no effect on system interoperability. Prior to pursuing a program executive officer-self-determination (PEO–SD), PM will coordinate through CIO/G–6 for an independent test agent position with respect to impact to interoperability. PMs will request approval from their program executive officers in writing and meet criteria established by 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 the request.

*(f)* Description of change.

*(g)* Description of internal testing results and cybersecurity RMF compliance.

*(h)* Coordination with all affected system owners and concurrence on the proposed changes to the certified SW configuration. The request should list titles of the other systems, names of their PMs and the dates of acknowledgment.

*(i)* Assessment of risk.

(2) Self-determination guidance is as follows:

*(a)* PMs need to consider:

1. Risk to interoperability supported by documentation of internal testing.
2. Whether the change can be fielded to entire baseline with reasonable effort and time.

*(b)* If the system changes have an interoperability impact, then the PM must coordinate with the ASA (ALT); DCS, G–3/5/7; and Configuration Control Board for approval to enter AIC testing as a system under test (SUT), and then coordinate with CIO/G–6 for an AIC determination. An AIC determination can result in a certification, non-certification, waiver, exemption, or an IC&L assessment.

*(c)* PM must coordinate and notify all systems with whom they exchange information, obtain written acknowledgment 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–SD.

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

*(e)* Any changes to previously AIC certified SW, 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 SW. PMs must submit self-determination documentation and SW changes to the ACMO, which will coordinate with test sites for integration of the SW changes into test configurations.

*(f)* Upon receipt of a favorable PEO–SD, ACMO will notify CIO/G–6, which will issue a memorandum titled "Modification to the Baseline" to authorize adding the system SW version that identifies the changes to the next CIO/G–6 quarterly baseline release.

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

*e. Configuration management of the Army interoperable certified fielded baseline.*

(1) All SW certified to operate on the Army network must comply with CIO/G–6 approved CfM procedures. SW submitted for interoperability testing is placed under CfM by the ACMO, Fort Hood, TX. Upon certification, SW will be controlled until retired from use. MATDEVs and PMs are responsible for ensuring all changes to certified system SW are coordinated with the ACMO. The ACMO will coordinate with FaNS, or other approved government test sites, to ensure test configurations are up-to-date and the Army has an appropriate record of its baseline SW to support risk mitigation activities and capability decision making. The ACMO effort is in addition to normal CfM performed by developers and maintainers of systems.

(2) The cybersecurity system of systems (SoS) network vulnerability assessment (NVA), performed during an AIC event, is the CIO/G–6 mechanism for SoS risk management through early identification and mitigation of vulnerabilities prior to fielding. Army Research Laboratory Survivability, Lethality Analysis Directorate will perform an SoS NVA on behalf of CIO/G–6 (SAIS–CB). Vulnerabilities that are successfully discovered will be provided to the AO to determine if there is an impact to the current authorization. Any individual system that exposes the SoS to a significant level of cybersecurity risk will not be certified by CIO/G–6 (SAIS–CB). MATDEVs and PMs are responsible for tracking and mitigating or remediating vulnerabilities that are successfully discovered during the SoS NVA.

(3) CIO/G–6 (SAIS–CB) assesses test results and issues appropriate AIC determinations. The AIC determinations result in inclusion of certified SW in the AIC fielded baseline which is the compilation of SW of systems that have AICs approving use in a networked environment. The AIC fielded baseline is composed of multiple SW sets, blocks, or packages, each containing unique integrated SW capabilities that are certified for operations during different time periods. Any questions regarding the CfM 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.

*f. Interoperability capabilities and limitations assessment.* An IC&L assessment is conducted on an IT/NSS product/capability (normally a COTS product) when requested by a combatant commander and validated by DCS, G–3/5/7, the Army Requirements and Resourcing Board via the rapid fielding initiative, quick reaction capability, operational needs statement, or the Joint urgent operational needs processes. IC&L assessments are typically conducted on IT/NSS products not supported by a program of record. IC&L assessments will be conducted in an operationally representative architecture as defined by a TRADOC-approved CONOPS and the assessment will include IT/NSS with which the "to-be" fielded product will be required to exchange information/data/services. The IC&L assessment does not result in an interoperability certification but allows CIO/G–6 to characterize the interoperability performance of the IT/NSS with regards to:

(1) Its ability to operate as defined by the MATDEV/proponent/agency in terms of its interoperability missions, as defined by its CONOPS.

(2) Its ability to operate within the intended network environment without introducing adverse impacts (determination of risk).

(3) The following essential CIO/G–6 IC&L assessment entrance criteria must be met by the MATDEV/proponent/agency before an IC&L assessment execution authorization:

*(a)* Provide a validated rapid fielding initiative, quick reaction capability, operational needs statement, or Joint urgent operational needs.

*(b)* Define how the IT/NSS will operate within its intended network environment, either by a CONOPS, and/or at a minimum, an operational view (OV)–1, system view (SV)–1 and standards view (StdV)–1.

*(c)* Attain AO approval of an ATO and/or an RMF ATO with POA&M for the IT/NSS configuration/version undergoing the IC&L assessment.

*(d)* Ensure and demonstrate compliance with current IAVM requirements and anti-virus patches, as applicable.

*(e)* Submit the IT/NSS on official letterhead and meet the test agent CfM office delivery instructions.

*(f)* Provide concurrence with CIO/G–6 approved IC&L assessment test plan (test plan will be developed by the test agent and concurred with by the MATDEV, proponent, agency, and user).

(4) An IT/NSS fielded under an IC&L assessment may be restricted by CIO/G–6 to specific units/locations for a specified period of time. Prior to the expiration of the IC&L assessment, the MATDEV/proponent/agency must request an extension of the current IC&L assessment. If CIO/G–6 determines that AIC testing is required, the MATDEV/proponent/agency must ensure all AIC entrance criteria are met prior to testing. To request an extension of the current IC&L assessment, the MATDEV/proponent/agency must request an extension via email to CIO/G–6.

*g. Army interoperability certification determinations.* Certification is provided when a specific IT/NSS configuration meets minimum AIC certification criteria and is granted a certification for a time period not to exceed 4 years. IT/NSS are required to undergo the AIC test process prior to the expiration of certification. CIO/G–6 will assess modifications to the certified configuration for impacts to interoperability. If it is determined that interoperability is impacted, the IT/NSS will be required to undergo AIC.

(1) The CIO/G–6 decision to certify the tested IT/NSS and the duration of the certification will be based on the following:

*(a)* Whether the SUT(s) met interoperable and net-centric (NC) capabilities as defined within the respective JCIDS or ISP documentation and other relevant documents.

*(b)* Whether test limitation impacts the ability to execute and assess test cases and required mission threads.

*(c)* Number and type of TIRs identified during testing and adjudicated by the Executive Steering Committee.

*(d)* Test report data on the interoperability and backward capability (BWC) test event.

*(e)* Complexity and impact of technical bulletins and other verified tactics, techniques, and procedures on the information needs of interfacing systems.

*(f)* Whether there are open Level 1 or 2 TIRs scored against the tested IT/NSS.

*(g)* Whether less than 30 percent of the mission threads with a Level 3 TIR scored against the tested IT/NSS.

*(h)* The IT/NSS cybersecurity posture will meet DOD RMF requirements and will not introduce significant risk to the SoS. A POA&M will be developed for cybersecurity vulnerabilities that are discovered during the SoS NVA.

*(i)* BWC certification will evaluate a system's vertical/horizontal interoperability in an SoS environment with the previous certified baseline and is part of all AIC test events starting in COE as a minimum requirement.

*(j)* Whether IT/NSS meets its interoperable and NC capabilities as defined within the respective JCIDS/ISP/test and evaluation management plan documentation.

(2) Criteria for needing an AIC recertification is as follows:

*(a)* Addition of an interoperable capability that previously was not in existence.

*(b)* Hardware/SW/operating system modification that impacts interoperability.

*(c)* IAVM updates that impact interoperability.

*(d)* Modification of the manner in which information is generated, processed, or consumed (such as introduction of a new or modified technical view standard which directly impacts interoperability functionality).

*(e)* Any other modification(s) of the IT/NSS that alters the interoperable performance of the certified configuration.

*h. Not certified.* A SUT cannot receive an AIC determination if it fails to meet the entrance and/or certification criteria. If a MATDEV/proponent desires an AIC for an IT/NSS configuration that received a "not certified" determination, the MATDEV/proponent must correct the deficiencies identified during the previous AIC testing event and demonstrate during regression testing if issue can be fixed during the same AIC test; or if an IA and vulnerability, demonstrate it has been added to the POA&M or mitigated by demonstrating in a FaNS certified lab environment. If this is not possible, then undergo another complete end-to-end test during a future AIC event. IT/NSS must meet the AIC requirements before being granted an AIC.

*i. Exemption.* AIC exemptions are applicable for Army IT/NSS that have no current or planned digital interoperability or NC capabilities or requirements documented in its JCIDS or ISP documents. Exemptions are provided for a specific configuration (that is, HW/SW version) and are permanent. If an IT/NSS is modified after receiving an exemption, then the MATDEV/proponent must submit an AIC request memorandum (for exemption, waiver, or test) to CIO/G–6 based on the modified configuration. If the modification(s) do not produce an interoperable or NC capability change then an AIC exemption will be granted for the modified configuration. However, if the modification(s) provides an interoperable or NC capability, then the IT/NSS will be required to undergo an AIC determination. Joint waivers to policy, approved by the DOD CIO, are provided when an Army IT/NSS has no Joint interoperability capabilities or requirements. Approval of a Joint waiver to policy does not automatically qualify Army IT/NSS for an AIC exemption or waiver. CIO/G–6 must determine Army interoperability testing requirements for the subject IT/NSS.

*j. Waiver.* AIC waivers are applicable for Army IT/NSS that have digital interoperability and NC capabilities and/or requirements that cannot currently meet the JCIDS requirements (in other words, due to technology immaturity, requirements blocking, evolutionary acquisition programs, and so on), but have a requirement for operational employment in its current configuration. AIC waivers are provided for a specific configuration version (HW/SW) and for a specific period of time not to exceed 1 year. If an interoperable or NC capability is not established at the expiration of the waiver, then the MATDEV/proponent must request an AIC waiver extension. AIC waivers will be voided if the IT/NSS is modified within the duration of the AIC waiver. If the modification(s) establishes an interoperable or NC capability, then the IT/NSS must undergo AIC testing. However, if the modification(s) does not provide an interoperable capability, then the MATDEV must request a new AIC waiver for the modified configuration. Approval of a Joint waiver to policy does not automatically qualify Army IT/NSS for AIC waiver. CIO/G–6 will determine interoperability testing requirements.

*k. Surrogate test articles.* CIO/G–6 will allow the utilization of surrogate test articles for AIC testing only after the surrogate test article has demonstrated interoperability characteristics, functionality, and performance identical to the production IT/NSS. To demonstrate that the surrogate test article executes the interoperability requirements identically to the production system, at least one AIC testing event will be conducted with the production system and the system's surrogate test article concurrently.

(1) *Reports for surrogate test articles.* At the conclusion of the event two reports will be generated:

*(a)* An AIC report for the production IT/NSS.

*(b)* A report for the surrogate test article with recommendation for an IV&VA of the surrogate test article for the purpose of future interoperability testing as a cost savings as well as effectiveness. Should the surrogate test article receive an IV&VA, the surrogate test article may be used for AIC evaluation from that point forward against the same technical standards baseline StdV–1 (formerly known as TV–1). The StdV–1 must be identified in the test plan and reported as either the SoS specific StdV–1, the current Department of Defense Information Technology Standards Registry (DISR) standard, or the PM identified StdV–1.

(2) *Criteria for a recertification.* Interoperability verification and validation (IV&V) accredited surrogate test articles may be utilized until a modification of the production IT/NSS changes its interoperability capability posture:

*(a)* Expiration of existing AIC certification.

*(b)* Addition of an interoperable capability that previously was not in existence.

*(c)* Hardware/SW/operating system modification that impacts interoperability.

*(d)* IAVM updates that impact interoperability.

*(e)* Modification in the manner in which information is generated, processed, or consumed (in other words, introduction of a new or modified StdV–1 which directly impacts interoperability functionality).

*(f)* Any other modification(s) of the IT/NSS that alters the interoperable performance of the certified configuration will affect the surrogate IV&V status. Physical configuration auditing will be conducted by the ACMO prior to each AIC test event to ensure the surrogate test article is constructed to CIO/G–6 approved representation of the production IT/NSS.

## 2–14. Information support plan process

*a. General.* The ISP 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 SoS 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 architectural description products of the ISP establish the baseline interoperability requirements critical for interoperability testing. The ISP process provides a method for demonstrating system NC interoperability capabilities and addressing any issues with shortfalls in capabilities. As specified in the Manual for the Operation of JCIDS (available at https://www.dau.mil/acquipedia/pages/articledetails.aspx?aid=12227505-ba29-41c0-88f0-682a219d5bbc), the ISP should include NR–KPP content. The ISP must reference all Army, Joint, and Coalition approved mission threads, which identify time-ordered interaction requirements for the system and SW to be tested. If appropriate mission threads are not available, the submitter must include an SV–10c in their ISP. The SV–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) ISP submission life cycle events are as follows:

*(a)* Initial ISP is submitted at least 90 days prior to the preliminary design review/MS B.

*(b)* Revised ISP is submitted at least 90 days prior to the critical design review.

*(c)* Final ISP is submitted at least 90 days prior to MS C decision and used for the interoperability certification test.

*(d)* The final approved ISP at MS C will be the ISP of record stored on the Global Information Grid Technical Guidance Federation (GTG–F).

*(e)* A post MS C ISP update is submitted at least 180 days prior to interoperability recertification test. The approved updated ISP will be the new ISP of record stored on the GTG–F.

(2) Submitted ISPs must contain the latest technical information on system and SW.

*b. Duties and functions.*

(1) *Army Chief Information Office/G–6.* In accordance with AR 25–1, CIO/G–6, Cybersecurity & Information Assurance Directorate is the approval authority for all Army ISPs and ensures Army compliance to overarching DOD and CJCSI ISP policy. Any questions regarding the ISP 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, CIO/G–6—

*(a)* Defines Army ISP policy and supporting procedures.

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

*(c)* Serves as the Army organization responsible for handling ISP processing and interface with the DOD GTG–F (https://gtg.csd.disa.mil).

*(d)* Serves as the approval authority for Army ISP waivers when appropriate for component unique IT and NSS (that is, no Joint interfaces).

*(e)* Provides to Joint Staff J6 and DOD CIO the Army's statement of concurrence or non-concurrence on all non-Army ISPs as well as all ACAT I and DOD special interest ISPs.

*(f)* Informs MS decision authorities on the status of ISPs during MS reviews.

(2) *Program executive officers.* Program executive officers provide a memorandum endorsing the initial ISP at MS B submission, which states the PM, TRADOC Capability Manager, and other affected Army and Joint organizations have concurred with the ISP and it is ready for release to CIO/G–6.

(3) *System owners.* PMs and government MATDEVs prepare ISPs for their systems in accordance with this pamphlet, Army and Joint policies, and DODI 8330.01. PMs and government MATDEVs should:

*(a)* Use the Enhanced Information Support Plan module within the PM portal on the GTG–F tool to develop all ISPs. Architecture views and mission threads may be hyperlinked to the ISP if the links are readily accessible to all reviewers.

*(b)* Coordinate with CIO/G–6, Data Integration & Architecture (SAIS–AOD), for guidance on Army's approved technical architecture.

*(c)* Ensure the ISP shows compliance with the system NR–KPP as specified in the JCIDS manual; compliance with applicable standards mandated in the DISR, Army technical architectures for COE, and relevant organization unique standards; compliance with DOD cybersecurity directives and policies; identifies any cybersecurity and interoperability certifications; and identifies spectrum issues and whether or not there has been an appropriate submission of a DD Form 1494 (Application for Equipment Frequency Allocation).

*(d)* Show linkage between ISPs, JCIDS-approved capabilities documents, and approved mission threads. The architecture views in an ISP 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 3170.01I). ISPs should reference approved mission threads that identify time-ordered interaction requirements for the system and/or SW. Alternatively, the ISP should include an SV–10c. Table 2–4 shows the required DODAF views for all Army ISPs.

*(e)* Ensure the initial ISP submission at MS B includes a submittal cover memorandum signed by the system's PEO or proponent at the SES or GO level. The memorandum must state the PM, TRADOC Capability Manager, and other affected Army and Joint organizations have concurred with the ISP and it is ready for release to CIO/G–6. Memorandum should state that all PMs and MATDEVs for interfacing systems at test that the ISP 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 ISP for accuracy, completeness, and co-sign the submittal cover memorandum attesting that the ISP is ready for release to CIO/G–6.

**Table 2–4**
**Army required information support plan Department of Defense Architectural Framework views**

| Name | View |
|---|---|
| Overview and Summary Information | All viewpoints (AV) 1 |
| Integrated Dictionary | AV–2 |

**Table 2–4**
**Army required information support plan Department of Defense Architectural Framework views—Continued**

| Name | View |
|---|---|
| High-Level Operational Concept Graphic | OV–1 |
| Operational Resource Flow Description | OV–2 |
| Operational Resource Flow Matrix | OV–3 |
| Operational Activity Model | OV–5B |
| Event-Trace Description | OV–6C |
| Systems Interface Description | SV–1 |
| Systems Resource Flow Description | SV–2 |
| Operational Activity to Systems Function Traceability Matrix | SV–5A |
| Systems Resource Flow Matrix | SV–6 |
| Systems Measures Matrix | SV–7 |
| Systems Event-Trace Description | SV–10C |
| Standards Profile | StdV–1 |
| Standards Forecast | StdV–2 |

*c. Information support plan waivers and exemptions.*

(1) Waiver requests will be provided to CIO/G–6 (SAIS–CBC) for endorsement prior to submission to DOD CIO and Joint Staff J6. PMs and MATDEVs may apply for an ISP waiver on Joint programs if their program satisfies one of the following requirements:

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

*(b)* 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.

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

*(d)* The system has no Joint interoperability requirements.

(2) Exemption requests will be provided to CIO/G–6 (SAIS–CBC) for endorsement and approval if a system does not meet the definition of IT or NSS, or if a system has no external interfaces.

*d. Information support plan submission method and staffing procedures.*

(1) The Army will lead the review of all ISPs regardless of ACAT level. If a program meets the criteria for a Joint review, 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 ISP 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 ISP 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 ISPs 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 an NR–KPP.

*(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) ISPs will be reviewed in the GTG–F for 30 days and will result in a set of comments for the PM to adjudicate. The PM will adjudicate critical and substantive comments within 60 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 CIO/G–6 (SAIS–CBC) for resolution. Critical risks and issues identified through ISP 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 ISP back to CIO/G–6 through the GTG–F.

(5) Upon receipt, CIO/G–6 (SAIS–CBC) will conduct a 14-day review of the ISP and adjudicated comments. If there are no identified issues, CIO/G–6 (SAIS–CBC) will issue an ISP concurrence for MS B and critical design review and an ISP approval memorandum at MS C. All ISP approval memorandums will be posted to the GTG–F with the ISP of record at MS C.

*e. Information support plan submission for test support.* The final ISP is updated to support each AIC and Joint interoperability testing event. Updated ISPs will be submitted to CIO/G–6 at least 180 days prior to a scheduled test. The CIO/G–6 will conduct either an Army only or Joint staffing (if a Joint system) of the updated ISP which will take 30 days. If no critical issues are identified during staffing, CIO/G–6 will issue and updated approval memorandum on the GTG–F, which will in turn authorize the approved test site to use the updated ISP of record for test case development.

## 2–15. Managing information technology at the installation

*a.* ARCYBER provides baseline C4IM services and applications to Army installations 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 primary service categories: Service 700–Automation; Service 701–Communications Systems and Systems Support, and Service 703–Cybersecurity. The IT primary service categories are documented in 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 tenant units and organizations will coordinate with the NEC for C4IM services support requirements above baseline via a service level agreement (SLA). These senior IM officials ensure their unit's or organization's voice, data, and video or visual information needs are provided within available resources and play a key part in ensuring metrics to gauge the effectiveness of NEC support are developed and monitored.

## 2–16. Network Enterprise Center

*a.* An installation NEC provides baseline 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 outside the continental United States (OCONUS) emergency operations centers in accordance with agreed upon SLAs. Installations and/or activities require an array of IT services based on size, location, and a varied customer base. The NEC performs several vital functions in the installation's capital planning and investment management processes, in addition to delivering required services. Most importantly, a NEC can validate new initiatives and ensures they comply with C4IT guidance and Army Enterprise Architecture (AEA). 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 ARCYBER's 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 SLA with this particular customer.

*c.* The NEC provides a standard set (baseline) of C4IM services at a delivery level and resourcing methodology designated in the C4IM Services List for automation, communication systems support, and cybersecurity. Tenants requiring services above the baseline set of service will establish an SLA and reimburse the NEC for the furnished services. ARCYBER and NETCOM oversee SLA development and performance through their subordinate commands.

## 2–17. 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 to include ACOMs, ASCCs, and DRUs 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 CIO/G–6. The command senior IM official directly supervises the IM/IT staff, related programs, and activities and executes DODIN–A global network enterprise activities, as prescribed by ARCYBER. 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 include oversight, guidance, and governance, plus short and long range planning activities. Refer to AR 25–1 for specific duties and functions.

*c.* Senior IMs ensure information management office/officer (IMO) personnel are required to use the service desk ticketing system to accurately track and account for IT workforce labor hours.

*d.* Senior IMs oversee the tracking of IT workforce training and certification requirements in accordance with Army policies and regulations to ensure minimum standards for IMOs are sustained.

### 2–18. Information management office/officer concept and functions

The 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, and provides guidance to the organization's users on IT policy. General duties and functions of an IMO are to:

*a.* Monitor all common user C4IM baseline service delivery and support provided by the NEC or signal battalion.

*b.* Identify, validate, and negotiate C4IM above baseline service delivery and support requirements with the NEC or signal battalion.

*c.* Implement and enforce IM/IT policies and procedures within their organization.

*d.* Develop requirements for operational instructions for applications and systems to include:

(1) Cybersecurity, including supporting cybersecurity personnel in the administration of and compliance with cybersecurity policy, procedures, training, and certification requirements (see AR 25–2).

(2) ITM, including:

*(a)* C4IT resource management, to include:

1. Developing C4IT plans, requirements, and strategic investment strategies in coordination with CIO/G–6, ACOMs, ASCCs, DRUs, and other Army organizations as appropriate.

2. Reimbursing NEC or signal battalion for services above the baseline.

*(b)* Requirements validation, to include:

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

2. Programming functional unique C4IT requirements through ACOM, ASCC, and DRU.

3. Programming all requirements for services above the baseline.

*(c)* C4IM performance management, to include:

1. Assessing the effectiveness and efficiency of C4IT support.

2. Reporting effectiveness and efficiency of C4IT support to ACOM.

*e.* Support implementation of the Installation Status Report (ISR) process, to include reporting on C4IM services in Installation Status Report–Services (ISR–S) Program, completing metrics related to radio frequency in the ISR–Mission Capacity Program, and completing ISR-Infrastructure Inspections of IS facilities.

*f.* Participate in the development of the SLAs, as required by mission, and coordinate with ACOM, ASCC, and DRU on agreement and funding of baseline services.

*g.* Develop supporting architecture by performing the following tasks:

(1) Operational architecture, to include:

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

*(b)* Submitting C4IT requirements to NEC or signal battalion.

*(c)* Recommending functional applications to ACOM, ASCC, and DRU for their mission requirement.

(2) Systems architecture, to include:

*(a)* Recommending applications to ACOM, ASCC, and DRU for their mission requirement.

*(b)* Providing configuration layout and connectivity of C4IT systems to NEC or signal battalion.

(3) C4IT 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, IM goals, and support to the Soldier. This includes interoperability, scalability, and standardization.

*(b)* Acting as liaison to the NEC, signal battalion, and service desk on behalf of the customer population.

*h.* Manage, protect, deliver, and enhance data and information assets (see chap 4).

*i.* Acquire and manage C4IT and services for functional applications, to include the acquisition and resource management processes, which begin when an organization's C4IT 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 C4IT investment strategy, to include:

(1) Facilitating business process reengineering and/or business case analysis for new or modified functional applications.

(2) Assisting system owners with generating options for improvements to functional applications.

(3) Acquiring and resourcing management of C4IT and services for office automation, which includes desktop PCs, laptop computers, notebook computers, hand-held computers, personal digital assistants (PDAs), site licenses, SW control, and leasing of C4IT. 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 SW includes SW required for PCs operations; for example, operating systems and PC office automation applications, including word processing, spreadsheets, electronic mail, task management, graphics, and databases.

(4) Purchasing of office automation via Army enterprise contract vehicles.

(5) Obtaining (and providing) a RMF assessment and accreditation if office automation requires network connectivity and/or web-based application.

(6) Inputting requirements to ACOM, ASCC, and DRU for input to the planning, programming, budgeting, and executing system for the life cycle replacement of office automation equipment and SW upgrades at the desktop level.

(7) Identify requirements for contracting support for short-haul communications and/or post, camp, station, and base communications (BASECOM). Short-haul communications consist of local telephone systems and associated trunking to the nearest serving commercial central office.

(8) Managing C4IT.

*j.* Update and maintain installation-level technical support and service, to include testing equipment and evaluating SW and/or HW. Coordinate with the NEC for installation-level technical support and service, to include testing equipment and evaluating SW and/or HW.

*k.* Manage enterprise C4 systems, to include supporting SW products that enable a desktop COE and enforcing desktop CfM, including:

(1) Enforcing established C4/IT policies.

(2) Providing mission unique application and/or DM.

(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.

*l.* Document change, migration of modernization, to include:

(1) Updating and maintaining system artifacts via Enterprise Mission Assurance Support Service (eMASS).

(2) Ensuring capabilities are authorized (ATO/interim ATO) and/or approved assess only authority as identified in the RMF process (see AR 25–2).

*m.* Provide C4IT support services, which include:

(1) *Server management.* The IMO task is to identify tenant servers 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 command, control, communications, computers, and information technology assets.* The IMO provides for C4IT 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.* Perform NEC support services tasks, including:

(1) Establishing SLAs with NEC or signal battalion to provide funding for services above the baseline.

(2) Identifying a primary organizational point of contact for problem identification and resolution.

(3) Providing requests for customer support service to NEC or signal battalion.

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

*o.* Publish procedural guidance on reutilization and disposal of HW, to include:

(1) Identifying potential excess equipment.

(2) Following procedures to determine excess equipment, removal from property books, and opportunities for reutilization and/or disposal.

(3) Accounting for property. For organizational control for HW and SW, the IMO publishes procedural guidance for proper accountability controls (including hand receipts, property books, and so on) and telecommunications and base services (including overall support of an installation and/or facility or assigned area's networks, to include those supporting DOD; Department of the Army (DA); and ACOM, ASCC. and DRU initiatives). The IMO task is to assist the information system security officer or NEC tasks.

*p.* Request long-haul services from NEC or signal battalion, to include long-haul and deployable communications (review, approval, and funding of all requests for long-haul services).

## 2–19. 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 toll-free (1–800 and 1–888) numbers (for purpose and traffic volume), calling cards (originating and terminating calls), and cellular phones 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 (TCOs) are appointed at installation level, typically in the NEC, and will also be appointed within ACOMs, ASCCs, and DRUs in accordance with organizational policies. TCOs review and validate bills for toll-free (1–800 and 1–888) service, pager service, cellular phone service, collect calls, and calling card usage; long-distance, sensitive but unclassified (SBU) voice, Federal Telecommunications System, and international direct distance dialing; commercial calls; local-leased commercial service; and other services associated with mobile devices in accordance with the requirements of AR 25–13. Additionally, TCOs are the only official other than the commander authorized to approve mobile device service initializations and all service level changes.

(2) Website managers and maintainers install access control mechanisms for websites 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 websites).

(3) Website 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 websites.

*c.* Privacy and security provisions include the following:

(1) 5 USC 552a (known as the Privacy Act of 1974) and 5 USC 552 (known as the Freedom of Information Act (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 (SOR) 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 informing the user there is no right to privacy on the systems. Use of government telecommunications and computing systems are 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 is limited in 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 transmission of large non-operational content over networks may have adverse 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 C2 for the influx of troops into active duty. This may require a surge in IS 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) Inter-Service agreements.

(4) Support to non-DOD federal agencies.

(5) Customer service guide(s).

## 2–20. Information technology support for telework or telecommuting

*a. General.* Telework is defined as an arrangement in which a civilian employee and/or Servicemember 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).

*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 app B). The AO and an O–6 or GS–15 must approve the use of employee-owned computers. The employee-owned computer must meet cybersecurity requirements. However, remote access SW 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).

(1) The 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. The 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 USG is liable under 28 USC 1346 (known as the Federal Tort Claims Act) or 31 USC 3721 (known as the Military Personnel and Civilian Employees Claims Act).

(2) Remote access to the Army portion of the DISN for telework purpose must be by a remote access server or approved virtual private network (VPN) connection and requires 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 AO, a teleworking employee may use employee-owned equipment, SW, 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 SW, such as Citrix, and does not retain copies or derivatives of such data on any part of the employee-owned system. Employee-owned IS will be used in accordance with AR 25–2. Additionally, employee-owned systems must be firewall-enabled and contain antivirus and anti-malware SW. Employees are responsible for the installation, use, and maintenance of all employee-owned equipment.

(4) Whether an employee uses a government-furnished or an employee-owned computer, the CAC will be used to enable cryptographic log-on 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 PKI.

(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 log-on, 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, SW, and communications devices) to the organization's property book officer or designated representative on the termination of the employment relationship with an HQDA organization, upon 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, as amended, 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 DOD 5500.07–R, the general principles of federal employment, and all other federal agency standards of conduct, while working at the alternative worksite.

*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 must comply with the appropriate provisions of AR 25–2. All DD Forms 2946 will address mandatory cybersecurity requirements and be approved by the AO prior to implementation.

*e. Local procedures.* Local procedures address issues such as federal and/or local laws, workplace requirements (safety, HW and/or SW 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.

(1) Computer/Electronic Accommodations Program (CAP) provides assistive technology as a form of reasonable program management.

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

*f. Employee-furnished equipment.* Where approved by the AO, the use of employee-owned computers and equipment for telework is authorized. All DD Forms 2946 will address mandatory cybersecurity requirements and be approved by the AO 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.)

*g. 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, SW, and communications, with appropriate cybersecurity 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 VPN or remote access server. The employee must agree to comply with the terms of any computer SW 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.

## 2–21. 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 ITM; 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 SW applications included in the list serve 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 organizational messaging service email package in use, operating systems, as well as other applications such as web authoring tools. Training for supported SW 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. DODD 8140.01 requires heads of DOD components to establish and maintain a cybersecurity training and awareness program for all DOD military, civilian, and contractor personnel needing access to IS. Information on cybersecurity 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 ITM specialists need technical training above that of standard user and Army enterprise service desk (AESD) agents who perform Tier 0 self-help and Tier 1 functions. Training the IMO and local IT staff to ensure that they can perform more complex customer service support tasks (Tier 2 and above) allows the Army to shift the more expensive IMO and local IT touch labor to more complex tasks while allowing the user and AESD agents to perform the lower level tasks. 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. The Army Training and Certification Tracking System is the primary source for tracking IA baseline training and certifications accomplished. For more information, see the Army e-Learning portal at https://usarmy.skillport.com/and see the Army Training and Certification Tracking System registration site at https://atc.us.army.mil/iastar/. In addition, IT civilians may access training through the Army Civilian Training, Education, and Development System which funds 31 career programs across the Army. Career program 34 (CP–34) provides career development opportunities for the ITM civilian community. View the CP–34 website at http://go.usa.gov/capzb. In addition to the standard career program offerings, CP–34 provides a course-based certification program that addresses the high-impact skills required in today's IT workforce. Additional information is available on the certification website http://go.usa.gov/x97ky.

(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 offsite training.

(2) The Army provides an array of programs for personnel to get technical training. In addition to the Army's e-Learning portal at https://usarmy.skillport.com/, CP–34 provides education and training programs to the civilian ITM workforce on a competitive basis. The CP–34 website is http://go.usa.gov/capzb.

(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.

(4) AESD agents may also need training on the new technologies as part of a new system or service in order to be integrated into the service desk functions to ensure quality customer support.

## 2–22. Information processing services

*a.* 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.

*b.* 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, ASCCs, DRUs, 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 SW, HW, and services. Users are required to procure, maintain, and fully support such products within their own resources, subject to all requirements to register SW, prevent SW piracy, maintain security, and so on.

## 2–23. Technical documentation

*a.* Documentation is the process of recording information produced by a SW and/or information system life cycle process or activity. Documentation should be tailored according to the complexity of the system or SW. (For availability of COTS documentation, check the license or contact the SW 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 SW 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 SW 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. SW and system documentation are maintained for as long as the related information is retained.

*d.* Preparation considerations include the following elements:

(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.* International Standardization Organization (ISO)/International Electro-technical Commission (IEC) 12207 is an international standard adopted for use by DOD. It is the DOD standard for SW documentation. ISO/IEC 12207 establishes a common framework for SW life cycle processes, with well-defined terminology, that can be referenced by the SW industry. It contains processes, activities, and tasks to be applied during the acquisition of systems containing SW, a standalone SW product, and SW services. It applies to the supply, development, operation, and maintenance of SW products. SW includes the SW portion of firmware. This standard provides a process for defining, controlling, and improving SW life cycle processes. The Institute of Electrical and Electronic Engineers (IEEE) and the Electronic Industries Alliance (EIA) 12207: 2008 is the U.S. implementation of ISO/IEC 12207. IEEE/EIA 12207: 2008 applies to the acquisition of systems and SW products and services, to the supply, development, operation, maintenance, and disposal of SW products and the SW portion of a system, whether performed internally or externally to an organization. Those aspects of system definition needed to provide the context for SW products and services are included. SW includes the SW portion of firmware. IEEE/EIA 12207: 2008 consists of two parts:

(1) 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 SW product information.

(2) IEEE/EIA 12207.2 summarizes the best practices of the SW industry in the context of the process structure provided by ISO/IEC 12207.

## 2–24. 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 offsite facility. For more information on document security, 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).

## 2–25. 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 nonrepudiation, 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, Extensible Markup Language (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, USG acknowledged the importance of electronic signatures with 44 USC 3504 (known as the Government Paperwork Elimination Act). This act requires agencies to provide for the use and acceptance of electronic signatures. CAC 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 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 documents 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 (PIN) or password for the CAC, identification key, and soft certificates).

(12) The solution provides an application programming interface and SW 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 CIO/G–6, Cyber & Information Assurance Directorate, Communication Security Division (SAIS–CB), 5850 23rd Street, Building 220, Fort Belvoir, VA 22060.

## 2–26. Non-Department of Defense information network connection exceptions

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. CJCSI 6211.02D serves as the basis for Army policy in which the DOD temporary exception to policy (TEP) process replaces the legacy Global Information Grid/DODIN waiver panel and associated processes and will now use the TEP process to 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 commercial internet service provider and network TEP waiver. This includes, but is not limited to, compliance with DOD networks, computing infrastructure, internet connectivity, satellite, cloud services, and cross-domain management, as well as the oversight of the migration of legacy networks into the DISN. Additional information including a commercial internet service provider and network TEP template, may be obtained at https://snap.dod.mil.

*a. Authority to operate.* An ATO and/or an ATO with POA&M must be completed in conjunction with submitting the TEP request. The TEP panel will not provide an exception authorization without an ATO or an ATO with POA&M. Army personnel should work in the Army non-secure internet protocol router network (NIPRNET) eMASS tracking database at https://emass-army.csd.disa.mil/ to acquire an ATO and/or an ATO with POA&M via the RMF. The Army

secret internet protocol router network (SIPRNET) eMASS instance is located at https://emass-army.csd.disa.smil.mil/. Contact iacora@us.army.mil with questions.

*b. Computer network defense service provider.*

(1) If the organization will be passing DOD data, a cybersecurity 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 items:

*(a)* How often is the connection monitored (for example, daily, weekly, or bi-monthly)?

*(b)* If there is a discrepancy, threat, or hacking event, who does the organization report that event to?

*c. Temporary exception to policy process.* The exception process for cloud computing, network, cross-component computing issues, satellite, and commercial internet service providers is as follows:

(1) The requesting organization will contact ARCYBER/Army Telecommunications Directorate (ATD), NETCOM, or CIO/G–6 (SAIS–CBA) for confirmation if a TEP is required. If a TEP is required, the requester will need to apply for a systems/network approval process (SNAP) account at the SNAP portal (https://snap.dod.mil) where a request template can be downloaded. TEP request identifications are assigned by the SNAP website and do not change.

(2) Once the TEP request is complete it is uploaded into SNAP. Additional information regarding the request is also entered into SNAP, including points of contact, topology diagrams, and other artifacts. The DISN Connection Process Guide at http://disa.mil/connect helps with navigating the process. The CIO/G–6 validating official will then review for content, clarity, and accuracy. If CIO/G–6 validates and supports the TEP, it will be finalized and sent for DISA review and approval. If CIO/G–6 denies the request, a justification will be provided.

(3) All new or renewal requests follow the same processes as new requests and use the same TEP identification associated with the original request.

*d. Temporary exception to policy period.* All approved TEPs are valid for a 12-month period and must be renewed every 12 months.

*e. Combatant commands.* Combatant command packages are handled by the Joint Staff.

*f. Compliance.* If a commercial internet service provider is discovered (either by DISA or Army personnel) at an Army installation that does not have an approved TEP for that connection, a CIO/G–6 validating official, as well as DOD CIO officials, will be notified. The connection will either be discontinued or the customer must begin the TEP process. If a TEP approval is not received, the connection must be discontinued.

### 2–27. Self-service printing device management procedures

*a. Acquisition of equipment.* Submit an administrative request memorandum, along with a completed DA Form 4951 (Lease/Purchase Analysis for Copying/Duplicating Machines), to the functional manager for validation (technical review) prior to procurement, as required by agency, ACOM, ASCC, DRU, USAR, ARNG, or installation guidance. The functional manager will use these forms to validate the printing device requirements. At a minimum, one alternate proposal from a different vendor is to be submitted to the functional manager.

*b. Cost-per-copy/site plan service contracts.* A cost benefit analysis using DA Form 4951, which clearly documents that this service option is more cost effective than purchasing the printing device, must be conducted prior to entering into a service contractual agreement. The functional manager must consider existing ELAs, BPAs, the condition of existing printing device equipment available, the cost of exercising any buyout options on existing equipment, and the useful life of owned equipment.

*c. Approval authority.* Do not acquire printing devices, or a service contract for printing devices, before the technical review (validation) process is completed. A copy of the documentation (administrative request memorandum and DA Form 4951) must be attached to each procurement action. Levels of validation authority for printing devices are as follows:

(1) Functional managers have technical review duties for printing devices.

(2) Table of organization and equipment (TOE) units normally obtain their printing devices while in garrison through the supporting logistics activity. Such equipment, whether rented or bought, will become station property. An exception is the acquisition and use of tactical document copiers for MTOE units, activities, or major elements. The authority for the acquisition of these copiers is in CTA 50–909.

*d. Evaluating requests.* In evaluating requests for printing devices, the main concern is whether the proposal is cost effective and if a valid need exists. The functional manager must also determine if currently available printing devices can satisfy these requirements.

(1) The functional manager, upon completion of the validation process must—

*(a)* Record the requirement statement authorization control number. Refer to this number in all future correspondence relating to the printing device requirements.

*(b)* Coordinate with the requesting activity before recommending a substitute printing device to ensure that it will meet user needs.

(2) The functional manager must retain a copy DA Form 4951 until the printing device is replaced or disposed of.

*e. Replacing printing devices.* The functional manager may replace printing devices when operation is determined unreliable and repair is not cost effective. Printing devices should not be replaced solely based on being fully depreciated (see para 2–27*f*.). Many machines have a serviceable life of more than five years and remain cost effective to operate.

*f. Depreciation of printing devices.* The following guidelines will help determine the depreciation of printing devices to use on DA Form 4951 or to prepare other cost figures:

(1) To determine the monthly depreciation of a newly purchased printing device, divide the original cost (including accessories) by 60 months. This figure will be the monthly depreciation cost.

(2) To determine the monthly depreciation of a printing device that is purchased after having been leased, use the following formula:

*(a)* First, subtract the number of months rented from 60 months.

*(b)* Second, subtract the manufacturer's rental credits from the original purchase price of the device. This figure will be the reduced purchase price of the device.

*(c)* Third, divide the reduced purchase price by the adjusted number of months (the number in the first part of this formula). This figure will be the monthly depreciation for the newly purchased device.

(3) To determine the annual total depreciation cost for originally leased printing devices that are later purchased during the reporting period, multiply the monthly depreciation by the number of months that the equipment was utilized during the reporting period.

(4) To report a printing device that is more than 60 months old, use zero depreciation. These devices are 100 percent depreciated.

*g. Disposal of printing devices.* Every effort should be made to make excess government-owned printing devices available to other organizations prior to turn-in to property disposal officials. When equipment has been declared excess or is no longer serviceable, disposal must be initiated in accordance with established property disposal and security procedures.

## 2–28. Information technology management career program 34

The primary asset of today's organization is its human capital. The Army must recruit, retain, and develop the talent to create an agile and resilient future force that overcomes emerging ITM challenges. CIO/G–6 oversees CP–34, one of the Army's largest civilian career programs. CP–34 identifies and develops training requirements based on the strategic environment, workforce and demographic diversity trends, competency assessments, and gap analysis. All CP–34 training programs are listed in the Army Civilian Training, Education, and Development System Plan, available on the CP–34 Community Page in Army Career Tracker at https://actnow.army.mil/communities/community/civilian-cp34. In 2017, CP–34 established a new course-based certification program to proactively address the requirements necessary to maintain readiness within the highly dynamic IT environment. The CP–34 certification program includes a robust catalog of training resources to develop high-impact skills. Information on CP–34 certification is available on the CP–34 Certification website (http://go.usa.gov/x97ky). CP–34 also manages a robust intern program with over 100 annual hires, in support of the Army's IT workforce recruitment strategy.

*a.* All programs—

(1) Are awarded by a competitive application process.

(2) Require endorsements by the chain of command through the command career PM.

(3) Are available to ITM professionals at GS–09 and above.

*b.* All CP–34 sponsored programs and services are published on the ITM careers website at http://go.usa.gov/capzb.

## 2–29. Performance-based strategic management

The Army performance management construct enables senior leaders to effectively manage their organization's processes using periodic assessments and resource informed decision making toward defined outcomes and objectives. A consistent PM construct is required in order to effectively perform ITM capabilities assessments. Conducting assessments is a recurring duty for all Army commands, and is critical, but not limited to, those commands that develop, support, maintain, and manage the Army's network capabilities. In turn, the assessments provided support Army mandates and strategic aims in support of current readiness and future Army network needs. The requirement to conduct Armywide performance management across Army operations is found in Public Law, DOD policies, Army regulations, directives, and orders.

*a. Performance management definition.* Performance management is the process whereby organizational goals are consistently met in an effective and efficient manner and resources, systems, and personnel are aligned to maximize attainment of strategic objectives and priorities. Performance management combines the organization's plans, activities, measure development, assessments and analyses, and improvement priorities to enhance organizational effectiveness and efficiency. It provides focus across the organization to include individual employees, teams, and processes to create or sustain an effective, results-oriented culture. Performance management is a continuous and iterative process that promotes best practices to achieve strategic goals. Performance management is a top-down driven process that aligns resources and assessment with decision making to achieve organizational outcomes or objectives.

*b. Key process components.* Performance management is continuous and starts with the senior leader's vision that outlines how the organization's existing plan and mission should evolve in response to the changing environment. The leader defines processes critical to organizational success with identified metrics that will validate mission accomplishment and assist in determining whether key processes are being accomplished in an effective and efficient manner. The need to conduct performance management may also arise from regulation, directives, orders, or other sources making the need to conduct performance management steps outside the complete performance management construct. Periodic assessment of performance validates whether the organization is progressing toward intended outcomes and objectives, and identifies those processes that require action to improve effectiveness and/or efficiency. As this action is taken, the assessment process verifies whether the intended improvement has been achieved and whether further steps are necessary. This measurement/assessment/improvement action cycle continues until the senior leader's vision has been realized and outcomes are achieved. As the operating environment for Army organizations is continuously evolving, so must the performance management cycle. It needs to be used to continuously measure/assess/improve organizational performance against its stated goals. The performance management cycle is continuous. New goals are added as others are completed and new strategic initiatives are determined by the senior leader.

*c. Performance framework.* Several steps in a performance framework address performance management as applied to a whole organizational assessment. The complete cycle is shown in figure 2–2. The complete PM guide is addressed in the Department of the Army's Performance Management: Improving Organizational Performance User's Guide, published by the Office of Business Transformation (OBT). The following steps are the critical IT capabilities assessments steps necessary to provide input on a recurring basis as directed by order or regulation:

(1) *Process execution and measure performance over time.* As the organization executes its critical processes overtime, it must measure those outputs based on cost, performance, and/or schedule metrics that validate whether those outputs are consistent with expected outcomes. Organizations should measure performance as frequently as necessary to support the requirements cycle. The data needs to be sufficient to provide enough data points to confirm whether a process is performing consistently before asking leaders to change how it is being executed or resourced. Today, collected data can and should be archived and readily available in real time to leaders using automated data visualization tools. The Army's current official enterprise capability is the Strategic Management System (SMS).

(2) *Specific, measurable, actionable, relevant, and timely guidelines for key performance indicators and measures.* Specific, measurable, actionable, relevant, and timely (SMART) key performance indicators and measures are used by organizations to develop useful measures that will provide consistent information for recurring assessments.

*(a)* Specific measurement is embedded in the activity and is not a compounded set of concepts.

*(b)* Measurable performance indicator has a quantifiable value or the activity is indexed on a specified scale for consistent performance assessments.

*(c)* Actionable performance indicator provides useful knowledge that enables action or decisions. It is not a period ending statement of accomplishment, or non-accomplishment, nor is it a MS or decision point.

*(d)* Relevant performance indicator is aligned to a strategy, campaign plan, or objective and is important to the expected outcome.

*(e)* Timely performance indicator is a recurring measurement that should show some variance against the targets or allowable performance parameters to enable appropriate action in support of risk management activity.

*(f)* Measures with flat trend lines over time are a statistical impossibility when using SMART measures. Measures without variation over time indicate that the wrong metric is being tracked and a flat line measure, good or bad, will skew the measurement value and will obscure actual performance from assessment, particularly when the measures are aggregated to a strategic level.

*(g)* Performance indices are an acceptable form of SMART measurement. A performance index is created by placing three to five measures concerning a common activity, setting the desired performance against a standard scale and tracking the resultant index value over time, rather than individual metric scores. There are several advantages to this approach which include minimizing the reported number of measures to leaders, grouping of dissimilar value types

(percentage, dollars, numbers) into a single scale for rolling up, less likelihood that a single metric will violently skew indicators, and the Army's SMS is setup to do this type of indexing.

(3) *Results/outcomes.* The organization collects and compiles information on the results that were achieved during process execution. These measurements provide insight as to whether the organization is successfully executing the critical processes in support of its business plan, campaign plan, or strategic imperatives. The results/outcomes should also verify whether customers and stakeholders are equally satisfied with the measurable outcomes.

(4) *Assessments and analysis.* In this phase, leadership focuses on identifying changes, commensurate with the duty level of the leader concerned, to the processes they are responsible for executing. In a complex organization, leaders measure (by metrics) and assess the outcomes of critical processes (also known as tasks) and initiatives (groups of functionally related tasks) whose successful accomplishment are essential to the organization's business or strategic plan. This assessment provides an indication of whether resource allocation for a particular process (or task) is sufficient and consistent with organizational priorities and to what degree the process outcome met or exceeded leader expectations for its accomplishment. The assessments and analysis phase starts to identify effectiveness and efficiency as well as opportunities for risk mitigation. Senior leaders should focus their assessments to make data informed resourcing decisions rather than a review of outcome metrics.

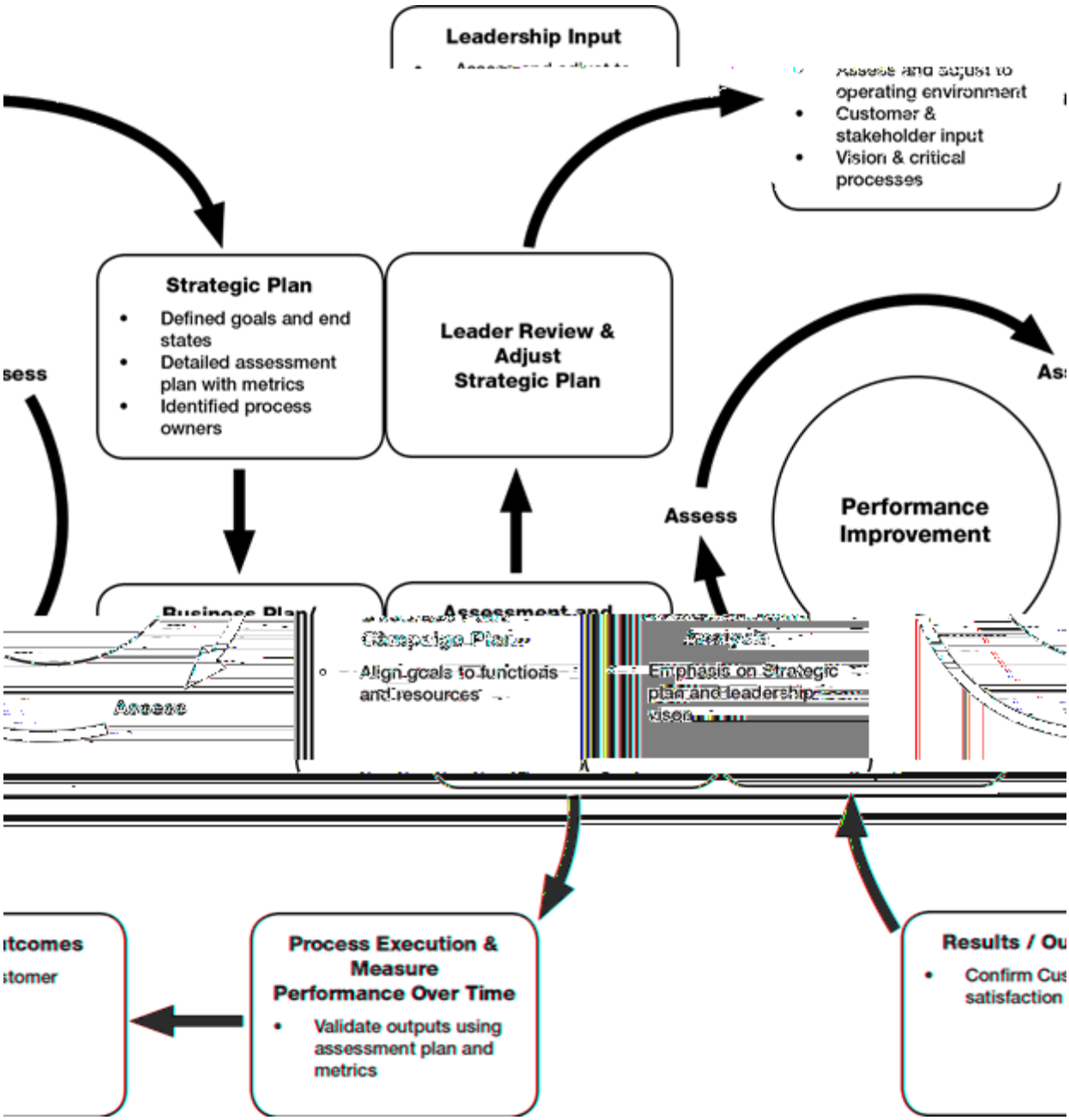


**Figure 2–2. The performance management construct**

*d. Performance assessment.* Performance assessment is a critical aspect of the construct whereby the organization's outputs and outcomes are periodically assessed and reviewed to determine whether goals are being met in an effective and efficient manner. Figure 2–1 depicts the periodic strategic-level assessment in relation to the other steps. Accordingly, leaders make strategic decisions, ensuring resources (personnel, money, and time) are properly aligned and prioritized to achieve organizational objectives. All organizational elements should continue to use internal assessments to evaluate and improve their progress.

(1) In this deliberate process step, outcomes of the processes (tasks) and initiatives (functionally related tasks) whose successful accomplishment are essential to the organization's business or strategic plan are measured (by metrics) and assessed. The performance assessment phase answers four primary questions for leaders:

*(a)* Did results achieved meet the intended outcome (where they effective)?

*(b)* Did results achieved meet the intended outcome at the lowest possible commitment of resources (where they efficient)?

*(c)* Are results achieved over time consistent in their performance, or did the results suggest that a process requires further examination as to how it is executed (application of business process re-engineering/or continuous process improvement)?

*(d)* Did results achieved by the current allocation of resources suggest that certain outcomes exceeded required expectations, and that a reallocation of resources might improve overall performance of the enterprise without compromising successful accomplishment of the original outcomes (mitigating risk by resource reallocation from those outcomes that exceeded expectations to those that are potentially under–Resourced)?

(2) While effectiveness assesses whether the results met requirements, efficiency requires that the resource implications of achieving the outcome, such as cost-per-outcome achieved, have been integrated. An organization can compare the cost-per-outcome achieved against similar organizations who are measuring the same results with the same criteria, a technique known as benchmarking. Organizations can use benchmarking to determine areas that may be ripe for continued improvements in effectiveness and efficiency.

(3) With the answers to the four questions provided in paragraph 2–29*d*, leaders have the opportunity to review and adjust their strategic plan and adjust their line of business. Leaders can continue to sustain the execution of successful processes. They can eliminate those processes whose continued execution has no apparent impact on the overall strategic plan. Senior leaders should mitigate risk by examining outcomes and shifting resources to critical underperforming processes as applicable.

(4) Leaders have the legal authority and duty to inspect their subordinates and subordinate organizations. A robust leader inspection program finds performance gaps and improves mission readiness. Part of this effort must be a self-assessment program where individual Soldiers and civilians report their compliance with guidance. An independent verification of those reports provides leaders with additional confidence in their validity. The findings from self-assessments and inspections should drive root-cause analysis.

(5) The Army expects leaders to use data to enhance their decision making. When constraints do not allow, they may be forced to make decisions with limited data, and are expected to use experience, judgment, and all available resources to guide them.

*e. Terms of reference for information technology performance management.* The terms of reference presented here are provided through coordination with OBT and DCS, G–3/5/7 (DAMO–ZT).

*f. 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, 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 ARCYBER's NETCOM. The data collected through the Army IT Metrics Program provides a snapshot view of the IT infrastructure and operations provided by the 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 IM 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, agreed upon service time, 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 Regional Cyber Center (RCC) for components of a base operations service provided. This requires the Army data center or RCC 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 and current OMB guidance.

1. Public Law 103–62 required departments to develop a strategic plan prior to fiscal year 1998, to establish annual performance goals by FY1999, and to report on actual performance compared to goals in FY2000.

2. CCA, effective August 1996, mandated a process to select, manage, and evaluate the results of IT investments.

3. Office of Business Transformation publication, Performance Management Users' Guide, 2 August 2016 (available at https://www.army.mil/e2/c/downloads/446641.pdf).

(3) *Structure.* The structure of the Army IT Metrics Program is based upon the 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, ARCYBER, and other Army organizations.

*(c)* The IT metrics application produces the Army IT 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 SLM/IT metrics workgroup and approved by 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–Services program.* The collection of individual metrics from each NEC is linked to the 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–S portion of the program captures the ability to provide IT support. The evaluations of these ISR–S metrics 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–S portion of the program. The ISR–S 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 700–Automation.
2. Service 701–Communications and Systems Support.
3. Service 703–Cybersecurity.

*(c)* The quarterly IT metrics data collected correlates the performance data (reflected in the ISR–S green, amber, red, or black service quality ratings) to costs (contained in the ISR–S 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. 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 information technology metrics website.* The IT metrics web-based application, supporting the Army IT Metrics Program, is CAC authenticated using the Enterprise Access Management System–Army (EAMS–A).

*(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 DODIN–A 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 SLAs with installation IT customers.

# Chapter 3
# Enterprise Architecture

## 3–1. Army Information Enterprise Architecture development

*a.* The AEA is the Army's blueprint to transform its operational visions and required capabilities through an integrated and interoperable set of IS and NSS. That blueprint, in turn, informs enterprise-wide network modernization of DODIN–A.

*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 3–1, the Army IEA is a component of the AEA and represents the total architecture for the DODIN–A as it supports the Army's WMA, BMA, and DIMA missions. The IEA consists of operational, systems, and enterprise architecture. This chapter describes the architecture development process that will evolve the Army IEA.

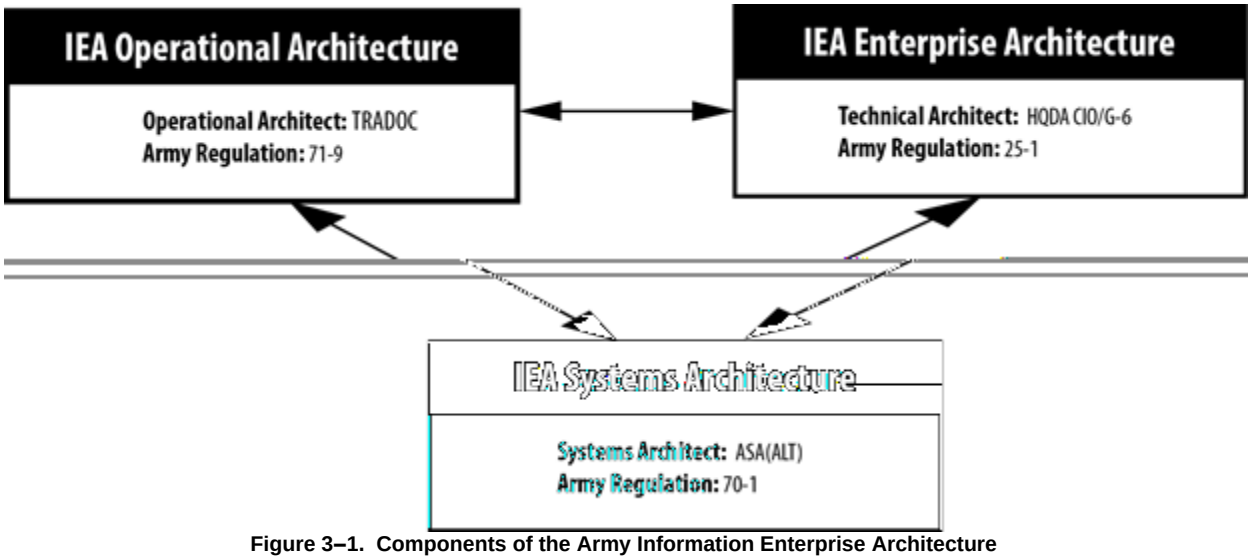


**Figure 3–1. Components of the Army Information Enterprise Architecture**

## 3–2. 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 DODIN–A over time. Each of these architecture views (operational, systems, and enterprise) is critical to understanding the totality of the DODIN–A 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 CJCSI 3170.01I and DOD Reference Architecture Description, available at http://dodcio.defense.gov/. Relevant Army guidance can be found within AR 71–9, AR 70–1, and AR 25–1.

*a. Information Enterprise Architecture—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, 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, and policy solutions). In each instance, the respective mission area lead for the WMA, BMA, DIMA, and 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. Information Enterprise Architecture—systems architecture.*

(1) The IEA systems architecture answers the question "What materiel solutions will reside on the DODIN–A?" It describes the IT materiel solutions that make up the DODIN–A, and identifies the interconnections providing for, or supporting, Army missions 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 ASA (ALT) and represents the individual solutions and services that comprise DODIN–A. 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. Information Enterprise Architecture—enterprise architecture.*

(1) The IEA enterprise architecture answers the question "What are the architectural characteristics and technical standards that DODIN–A 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. Figure 3–1 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.

(2) The IEA enterprise architecture is led by 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 is captured in two architectures, the DODIN–A enterprise architecture and the enterprise reference architectures.

## 3–3. Information Enterprise Architecture overview

*a.* The IEA 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). CIO/G–6's Operations and Architecture Directorate (SAIS–OA), in coordination with OBT; ASA (ALT); DCS, G–3/5/7; DCS, G–2; and TRADOC will oversee execution of the IEA through the AENC, an existing, structured governance and 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 artifacts are developed and published, they will be life cycle and configuration managed by the Architecture Configuration Control Team (ACCT).

*b.* The IEA development process is described in paragraphs 3–3*b*(1) and 3–3*b*(2).

(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 JCIDS and business capability life cycle 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 DODIN–A 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 3–2 identifies the high-level IEA enterprise architecture product development process. The full processes can be found at https://cadie.army.mil/cadie/portal/default.aspx.

*d.* Although not strictly a part of the AEA development process, other documents significantly influence the generation of architecture decisions and products. The documents describe the Army's intended DODIN–A 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 (https://wmaafip.csd.disa.mil/home).
(6) DOD Technical Standards (DOD IT Standards Registry).
(7) Army enterprise reference architectures.
(8) Mission Partner Environment.

*e.* Figure 3–2 identifies the high-level IEA enterprise architecture product development process. The full processes can be found at https://cadie.army.mil/cadie/portal/default.aspx.

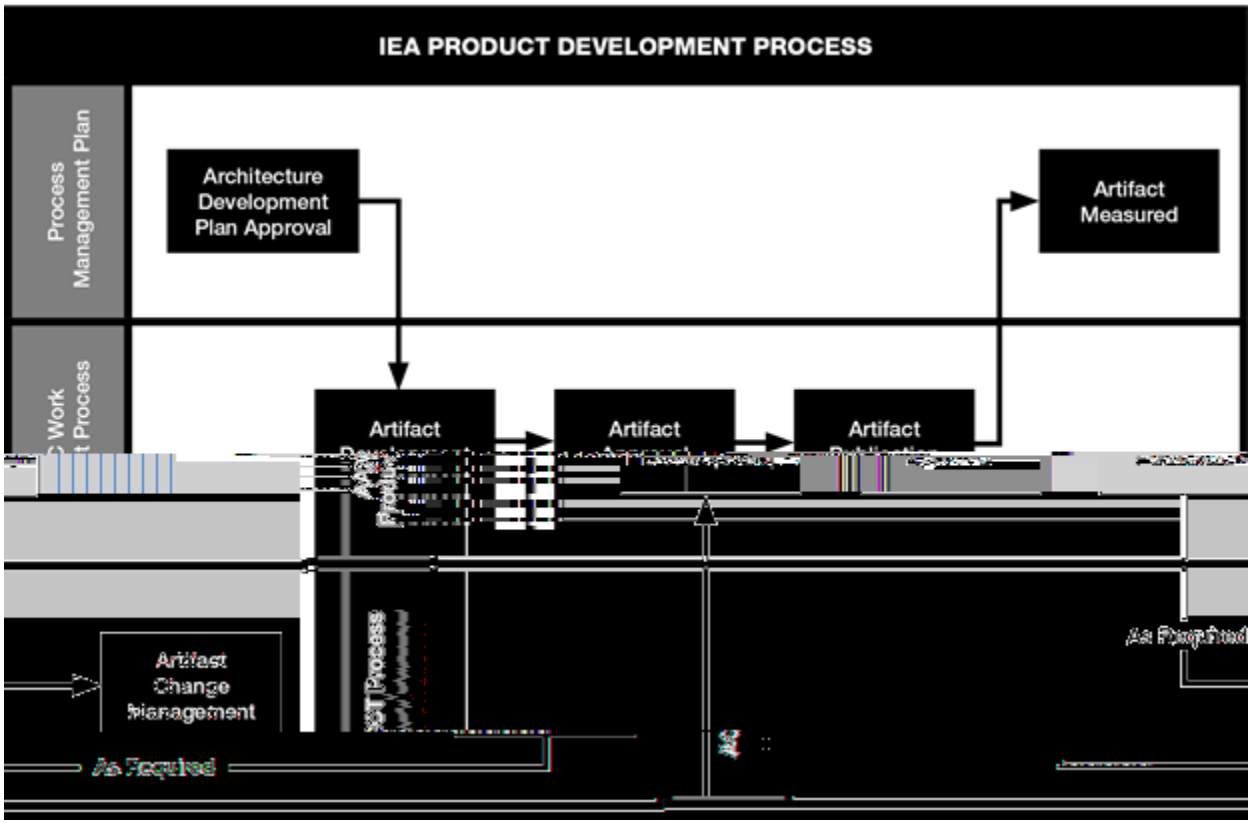


**Figure 3–2. Information Enterprise Architecture product development process**

*f.* IEA enterprise architecture artifacts are a design-focused translation of AENC decisions. As supporting documents to the Army Network Campaign Plan 2020 and Beyond, they provide strategic-level guidance on how the DODIN–A, 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 and mission partner environment.

(1) *Overview.*
*(a)* Scope: DODIN–A as covered by the Army IEA.
*(b)* Level of abstraction: Strategic.
*(c)* Timeframe: Targeted to be realized within 7 to 10 years (document will specify).
(2) *Duties and functions.*
*(a)* Approval: Director, Operations and Architecture Directorate (SAIS–OA).
*(b)* Lead: Operations and Architecture Directorate (SAIS–OA).

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

(3) *Enterprise architecture evaluation criteria.*

*(a)* 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 DODIN–A.

*(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 DODIN–A to stakeholders.

*(f)* Accurately conveys Army and DOD technical standards that are applicable to DODIN–A in the desired timeframe.

*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 organize architecture data around a specific problem set or enable a specific capability. The enterprise reference architectures incrementally provide architecture data with the intent of codifying the DODIN–A strategy and AENC position and intent. The intent of this approach is to guide and synchronize Army investment and acquisition decisions, enable the standardization of DODIN–A materiel solutions, and translate Army Enterprise Network (AEN) decisions that inform, and are informed by, network capability sets (NCSs) for a given timeframe to enable network modernization.

(1) *Overview.*

*(a)* Scope: Includes all architecture development efforts within CIO/G–6. This includes, but is not limited to, all architecture development efforts under the programmatic oversight of the Director, Operations and Architecture Directorate (SAIS–OA).

*(b)* Level of abstraction: Strategic, operational, and tactical.

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

(2) *Duties and functions.*

*(a)* Approval: Director, Operations and Architecture Directorate (SAIS–OA).

*(b)* Lead: Operations and Architecture Directorate (SAIS–OA).

*(c)* Assist(s): Operational Architects–OBT provide guidance, direction, and clarification regarding intended capabilities and capability relationships. System Architects–ASA (ALT) provide guidance, direction, and clarification regarding expected system fielding schedules and represents implementable solutions. DOD and Army partners including, but not limited to, DISA, ARCYBER, ASA (ALT), and Intelligence and Security Command ensure technical and engineering guidance are aligned with current priorities.

(3) *Summary.* CIO/G–6 will continue to adhere to DOD guidance as well as expand the use of architecture rules.

*h.* IEA enterprise architecture products inform Army leaders, architects, and analysts across multiple decision forums. Table 3–1 identifies primary consumers of IEA enterprise architecture products and their anticipated use.

**Table 3–1**
**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.<br>Identification of minimal set of technical requirements.<br>Communicate Army operational requirements. |
| AEN End Users | Communicate CIO/G–6 intent for IT modernization.<br>Inform IT support requirements. |
| Acquisition and IT Solution Developers | Identification of minimal set of technical requirements.<br>Guide acquisition planning and development activities.<br>Support budgetary requests.<br>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.<br>Identify capability-based assessment gaps and relevant consolidation efforts to gain organization, training, materiel, leadership, personnel efficiencies. |
| AEN Domains | Identify IT capability gaps.<br>Inform capability set development. |

**Table 3–1**
**Consumers of Information Enterprise Architecture products and anticipated product use—Continued**

| Groups and Forums | Use of IEA Enterprise Architecture Guidance, Rules, and Data |
|---|---|
| | Provide performance metrics. |
| JIE/DOD | Inform JIE architecture development.<br>Validate JIE architectures.<br>Communicate Army equities and requirements. |

## 3–4. Information Enterprise Architecture governance

*a.* CIO/G–6 is the lead for the Army IEA. 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. Operations and Architecture Directorate (SAIS–OA) is delegated the authority to review, approve, and release IEA enterprise architecture products on behalf of CIO/G–6. They 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 duty to internally integrate the architecture and coordinate architecture activities. The DODIN–A/MC GOSC, the ABC, and the AENC perform this function for the WMA, BMA, DIMA, and EIEMA, respectively. DCS, G–2 will ensure synchronization of the DIMA and will align architecture integration through the DOD intelligence boards.

*c.* ACCT is the Army's chartered organization to maintain configuration control of products addressing the EIEMA. The ACCT, established by CIO/G–6 and chaired by the Operations and Architecture Directorate (SAIS–OA), is comprised of voting members from TRADOC; DCS, G–3/5/7; OBT; ASA (ALT); and ARCYBER. 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.

*d.* AEA certification/compliance policy and architecture compliance assessment (ACA) process CIO/G–6 has published policy guidance and developed the ACA process to ensure that all Army IT solution architectures and resulting systems comply with the rules put forth in the DODIN–A enterprise architecture and associated reference architectures The ACA process is used to assess Army IT solution architectures' and resulting systems' level of compliance with the DODIN–A IT architecture standards. CIO/G–6 (SAIS–OA) maintains the policy guidance and ACA process.

*e.* AIA is based on the DOD's IEA guidance to enable better understanding and interoperability of shared information by providing guidance and compliance requirements to Army stakeholders. The AIA informs and supports the design, development, deployment, and use of IS that are consistent, compatible, and integrated across the Army enterprise. The AIA presents an end-state information-sharing framework that presents the key concepts involved in NC information sharing and their interrelationships.

*f.* The AIA is aligned with the DOD and Army data strategies to make data visible, accessible, understandable, trusted (to include protection, assurance, and security), and interoperable throughout the data life cycle to any authorized consumer or mission partner possessing the appropriate security clearance and need to know.

*g.* The primary component of the AIA is a collection of principles and business rules that support the DODIN–A end-to-end enterprise architecture to ensure compliance in the following areas:

(1) Data asset development management.
(2) Data and service deployment.
(3) Data delivery and use.
(4) Secured availability.

*h.* The AIA provides the foundation to accelerate Army transformation to NC information sharing in two ways:

(1) As design and development guidance for enabling information sharing.

(2) As a set of compliance requirements for assessing the level to which systems meet NC information sharing objectives.

*i.* In addition, the AIA should be used to influence system information requirements definition process and the development of an initial capabilities document.

*j.* The AIA is located at http://ciog6.army.mil/portals/1/architecture/armyinformationarchitecturev4-1dtd2013-06–05.pdf.

## Chapter 4
## Data Management

DM allows the Army to execute and supervise plans, architectures, policies, programs, and practices that properly manage, protect, deliver, and enhance the full life cycle of data and information assets regardless of where they reside. DM minimizes the risks and costs of regulatory noncompliance, legal complications, and security breaches. It also provides access to accurate data when and where it is needed, without ambiguity or conflict, thereby avoiding miscommunication. DM tasks include data quality, master data, metadata and data standards management, information exchange specification (IES), interoperability, and data integration. Implementing enterprise DM and warehousing increases operational performance and reliability, introduces standardization, provides the ability to respond efficiently and effectively to change, enhances security, and allows for economies of scale in terms of operations and maintenance costs. The Army, in its effort to implement enterprise DM, will do this through the ADMP.

### 4–1. Army data strategy

*a.* The Army data strategy adopts, extends, and refines the DOD Net-Centric Data Strategy and implementing instructions DODI 8320.02 and DODI 8320.07. By establishing repeatable and reusable processes and common technical standards for data exchange and DM, the Army will foster improved interoperability and quicker, more cost-efficient fielding of IT solutions, based on the LandWarNet 2020 and Beyond Enterprise Architecture for MC (available on the CIO G–6 portal at https://army.deps.mil/army/cmds/hqda_ciog6/sitepages/home.aspx). The Army data strategy is critical to achieving the COE.

*b.* The Army data strategy includes five goals. These goals, and the enabling objectives that refine and meet these goals, are presented in table 4–1.

(1) *Make data visible.* The goal of making data visible is to enable authorized users to discover authoritative data, information, and IT services.

*(a)* Users and applications migrate from maintaining private data to making data available in community and enterprise shared spaces. These shared spaces will act as repositories, where users and applications can submit or post data assets to the enterprise.

*(b)* To facilitate discovery, users and applications will provide discovery metadata, in accordance with the Department of Defense Discovery Metadata Specification (DDMS), for all data assets, particularly those posted to shared spaces. The DDMS will provide a common set of structured attributes that support discovery of data assets using search tools.

(2) *Make data accessible.* The goal of making data accessible is to provide all credentialed consumers access to authoritative data, information, and IT services via commonly supported access methods in accordance with law, policy, and security controls (for example, classification, need to know, compartmentalized controls, COI, and so on).

*(a)* Shared spaces (virtual and actual, such as enterprise data centers) created to provide a "store and serve" mechanism for data assets. Data access services are any mechanisms that help expose data that are not otherwise available to users and applications.

*(b)* Security–Related metadata, provided for each data asset as defined by the security descriptors element set within the core layer of the DDMS. Systems will control access in accordance with the asset's security–Related metadata.

(3) *Make data understandable.* The goal of making data understandable is to ensure that a data asset is usable by known and unanticipated authorized consumers through development and use of shared vocabularies.

*(a)* Data modeling encompasses procedures, methods, best practices, recommendations, and subject matter expertise that support data model design, development, and implementation. Data model guidance includes standardized, reusable schematic components for ubiquitous concepts (for example, person, location, time).

*(b)* Data integration is the process of combining data from two or more data assets and producing a single unified, consistent, and cohesive view of the combined data. The objective is to create a set of data that represents the same information represented by the input data sets.

*(c)* Information requirements will describe the information needed to drive enterprise processes and capabilities. Information requirement traceability will ensure that the right information is available and can be supplied to the right end users in the Army and among mission partners.

(4) *Make data trusted.* The goal of making data trusted consists of the following: ensure secure access, establish known pedigree and security level of data, and provide information from an approved authoritative source.

*(a)* Identifying ADSs enables commanders, decisions makers, and all Army personnel access to Army-certified (accurate, timely, and high-quality) internal and external data sources containing trusted information. Reuse of

registered ADSs is key to improving mission effectiveness through system interoperability and to reducing the time, effort, and resources required to operationally integrate Army systems.

*(b)* Creating secured availability involves protecting the confidentiality, integrity, and availability of Army information. Secured availability will provide systemic security mechanisms that are an integral part of system design, development, fielding, and operations.

(5) *Make data interoperable.* The goal of making data interoperable is for data providers to utilize non-proprietary, open source, industry, or DOD-designated standards to ensure that data are useable across multiple systems and applications.

*(a)* Complying with IES and reuse of IESs is key to improving the effectiveness of system interoperability and reducing the time, effort, and resources required to operationally integrate Army systems.

*(b)* Establishing master DM and unique identifiers will provide a set of processes and tools that ensure that master data are effectively controlled, updated, and used within and throughout enterprise SW systems. Master data are typically shared and used by different SW applications across the enterprise, often as part of transaction processing. Unique identifiers are a form of master data that enable interoperability and consistency of data assets across the Army enterprise.

*(c)* Establish community-based information sharing through interoperability communities may provide an informal, loosely organized group of members or a formal group that is organized as a community of interest, where a member is a system, service, application, or data asset that is coupled with a human representative. The format and meaning of data exchanged with entities outside the community are the collective duty of the community. This can be best-accomplished using industry standards.

*(d)* Establishing translation and mediation will provide a mechanism where data are translated from their original schematic format to a schematic format more suitable for the receiver through a mediating agent. Mediation involves a third-party neutral mediating format (for example, one governed by an IES) that acts as an intermediary between the sender and receiver. Translations are involved in the exchange of data when a mediating format is used. Mediation may involve a sequence of transformation or translation stages. Use of translation and mediation should be minimized as much as practical; industry standards can be effective in reducing the need for them.

**Table 4–1**
**Army Data Strategic Goals and Enabling Objectives**

| Army Data Strategic Goals | Enabling Objectives |
|---|---|
| Make Data Visible (V) | Post Data to Shared Spaces<br>Register Metadata Related to Structure and Definition |
| Make Data Accessible (A) | Create Shared Spaces and Data Services (also Information and IT Services)<br>Associate Security–Related Metadata |
| Make Data Understandable (U) | Create Data Models<br>Establish Data Integration<br>Identify Information Requirements Traceability |
| Make Data Trusted (T) | Identify ADSs<br>Create Secured Availability (Data Security and Data Access Security) |
| Make Data Interoperable (I) | Comply with IESs<br>Establish Master Data Management/Unique Identifiers<br>Establish Community-Based Information Sharing<br>Establish Translation and Mediation |

*c.* The Army data strategy describes a path forward to realize Army and DOD data, information, and IT service objectives, providing DM planning and implementation guidance to Army DSs, data owners, and data producers to maximize the sharing of Army data, information, and IT services. This will enable commanders, their organizations, and our mission partners to have broad, efficient, and timely access to authoritative data. The strategy also provides the roadmap to increase interoperability among systems and reduce development and sustainment costs. The Army data strategy is being implemented through the COE and numerous ongoing operational data efforts across the Army. The implementation guidance provided via the ADMP is the primary expression of and instrument for executing the Army data strategy.

## 4–2. Army data management program

The ADMP operationalizes the Army data strategy by defining the kind and structure of the functions necessary for Army DM, explaining the duties and functions of governing agents such as the ADB in the execution of Army DM functions, and identifying the major initiatives and long-term timelines for the development and adoption of Army DM guidance.

*a. Authoritative data source.*

(1) The Army is continuing its effort to reduce redundancy, improve development cost of systems and to ensure data is visible, accessible, useable, trusted, and interoperable across the enterprise. The Army has established an enterprise-wide requirement to identify and register user, organization, and system data needs and the ADS that will support those needs (see AR 25–1). DODI 8320.03 defines an ADS as "a recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An ADS may be the functional combination of multiple, separate data sources."

(2) ADSs will be identified and registered in the data services environment (DSE) per DODI 8320.02 and used to the maximum extent possible. This will improve mission effectiveness by enabling the reuse of visible, accessible, understandable, trustworthy, and interoperable data (see DODI 8320.07).

(3) The Army process of identifying, registering, and publishing an ADS consists of four steps. Each step builds upon the previous step to the final approved and published ADS. These steps include:

*(a) Propose and publish a data need.* A data need is a named and defined specification for a particular type of data that supports one or more operational requirements. It may be generic or very specific. This includes defining and describing the data, as well as identifying data attributes that are needed; identifying the authoritative body(s) that owns or maintains the data needed; and the proposed data need being approved by the authoritative body.

*(b) Register and publish a system.* A system is the combination of SW/HW that presents data that supports an identified data need(s). The systems may also identify the data producers. This includes defining and describing the system to include AITR/DITPR number and identifying the program management office/proof of concept (POC), system attributes, system access points, and data feed systems.

*(c) Register and publish a data producer.* The data producer is the person, group, or organization that controls, manufactures, or maintains data assets within the DOD. This includes defining and describing the system; identifying the POCs and producer systems.

*(d) Propose and publish an authoritative data source.* Proposing an ADS includes identifying and relating published data need(s), system, and data producer(s); registering in APMS, including business process documents (suppliers, inputs, processes, outputs, and consumers); data access document (business rules and processes for access to data); and identifying the data elements the ADS is authoritative for. This step includes the ADB review and approval process. Once the approval process is complete and the proposed ADS is approved, it will then be published in the DSE. For complete instructions on the registration and publication of data needs, systems, data producers, and ADSs see https://www.milsuite.mil/wiki/portal:army_data_management_program/ads.

*b. Metadata.*

(1) The ubiquitous definition of metadata is "data about data." Metadata is used to facilitate the understanding, use, and management of data. Metadata is a way of enriching data to preserve its meaning outside of its original context, in part so that SW systems can interact with the data. Governed metadata should be the true focal point of the working knowledge of any organization.

(2) The main purpose of metadata is to facilitate in the discovery of relevant information, more often classified as resource discovery. Metadata also helps organize electronic resources, provide digital identification, and support archiving and preservation of the resource. Metadata assists in resource discovery by "allowing resources to be found by relevant criteria, identifying resources, bringing similar resources together, distinguishing dissimilar resources, and giving location information."

(3) Classification of metadata is by the National Information Standards Organization, which defines three different types of metadata:

*(a)* Cataloging (descriptive) metadata describes a resource for purposes such as discovery and identification. It can include elements such as title, abstract, author, and keywords.

*(b)* Structural/semantic metadata indicates how compound objects are put together; for example, how pages are ordered to form chapters.

*(c)* Administrative metadata provides information to help manage a resource, such as when and how it was created, file type, other technical information, and who can access it.

(4) Data tagging is a tag such as a non-hierarchical keyword or term assigned to a piece of information (such as an internet bookmark, digital image, or computer file). This kind of metadata helps describe an item and allows it to be

found again by browsing or searching. Tags are generally chosen informally and personally by the item's creator or by its viewer, depending on the system.

(5) Tagging is the assignment of descriptive words or categories to content, using terms that mean something to the person doing the tagging. When users add tags to content in SharePoint, they are essentially adding metadata to describe what the content contains, what it does, or what it is about. Tags extend the organizational taxonomy, which improves content findability. Tags help to expand your solution's information architecture over time and, most importantly, they extend the accountability for evolving the information architecture to everyone in the organization. This feature helps to associate content with new and emerging terms, even before these terms are formally added to the organization's taxonomy.

(6) It is the duty of all DOD component heads to register in the DSE all identified ADSs, IT services, and required metadata per DODI 8320.02 and direct and oversee development and visibility of data and services, shared vocabularies and associated metadata (for example, discovery, structural, and semantic), and registration in appropriate registries, catalogs, and repositories.

*c. Army data quality management.*

(1) Data quality is a measurement or assessment of how well data meets or does not meet Army goals based on the evaluation of criteria such as relevance, accuracy, timeliness, precision, coherence, completeness, and understandability.

(2) Data quality management (DQM) is the collection of enterprise processes and governance that ensure that enterprise data "measures up" when data quality criteria are evaluated. The primary objectives of DQM are as follows:

*(a)* Provide data that is fit for use and trustworthy in the eyes of the COI.

*(b)* Reduce the IT and operational inefficiencies within the Army.

(3) The keys to achieving these objectives are not just procedures and tools to perform data quality but the ability to measure and evaluate the level of data quality to identify potential improvements. A partnership between the business and technology groups is essential for any DQM effort to succeed. Business groups are responsible for establishing the business rules that govern the quality of data and are ultimately responsible for verifying it. The IT group is responsible for establishing and managing the overall DQM environment including the architecture, technical facilities, systems, and databases that acquire, maintain, and disseminate data assets. Both groups must be involved in any successful DQM program.

(4) Most organizations react to data quality events instead of determining how to prevent problems from occurring in the first place. Being proactive instead of reactive by:

*(a)* Establishing a DQM program.

*(b)* Determining how data quality issues will be handled during the development of a DQM process.

*(c)* Monitoring data quality at every stage where data is touched.

*(d)* Creating a DQM dashboard to monitor the data quality performance measures.

(5) For more information, guidance, and best practices for DQM and how it can support the Army data quality goals, see the Army Data Management Guide (ADMG)–Data Quality Management located at https://www.milsuite.mil/wiki/portal:army_data_management_program/admg.

*d. Data strategy metrics.*

(1) Data strategy metrics (DSM) are numeric measurements that quantify the performance of DM capabilities. These metrics are used to identify the current level of effectiveness of the DM capabilities and to measure progress towards NC information sharing and other Army data strategy goals.

(2) Measuring Army data strategy effectiveness requires the establishment and monitoring of DSM across multiple dimensions of Army DM capabilities. Many of these capabilities are described in the AIA as sets of principles and rules. Achieving these goals involves successful and widespread adoption of a complex set of interrelated IT skills and standards, as described in the DOD IEA, the AIA, and related Army DM program guidance.

(3) The primary objective of DSM is to identify the important characteristics of DM capabilities needed to meet the Army data strategy goals and objectives, and to establish ways to measure how well the organization is providing these capabilities. 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.

(4) The DSM helps to focus attention on critical DM characteristics and practices, and to provide quantitative measures of the effectiveness of their implementation. The benefits of DSM include being able to baseline how well military systems and organizations are performing critical DM capabilities, and to evaluate their improvement over time. Being able to measure the effectiveness of DM capabilities impacts the ability to manage, control, and improve the quality and value of shared information.

(5) For more information, guidance, and best practices for DSM and how the Army will benefit, see the ADMG–Data Strategy Metrics located at https://www.milsuite.mil/wiki/portal:army_data_management_program/admg.

*e. Information exchange specification.*

(1) When two or more entities need to exchange information, they simply have an information exchange requirement. When a formal specification of that information exchange requirement is created, it represents an IES. When the entities place that IES under CfM and establish that it should not change (for example, other than yearly) then the IES becomes an IES. Stylistically, this is called an Information Exchange Standards Specification.

(2) An IES is a critical product that a COI, functional domain, or mission area within the Army develops to allow for interoperability. When developing their IES, COIs will determine the appropriate focus and data standardization within their community. This decentralized, distributed approach to interoperability ensures that key interfaces and data structures are controlled when tightly engineered interfaces are required.

(3) The IES definitional products document the information exchange. IES is system independent and COI derived. IES-contained products can include; for example, vocabularies, entity relation diagrams, Unified Modeling Language (UML) diagrams, XML schemas, message formats, data dictionaries, taxonomies, and DDMS extensions. Army COIs will register their IES data standard products in the DOD metadata registry.

(4) IES can exist at the COI, domain, and mission area level. It is imperative that COIs coordinate their IES with the domains and mission area IES that they fall under. For example, in the Army, it is the WMA position that, for command and control, whatever data schema a COI develops will conform to the Joint Command, Control, and Consultation Information Exchange Data Model as a starting point. Only then would each COI extend its data specification to cover its functional area.

*f. National information exchange model.*

(1) The national information exchange model (NIEM) technical architecture is a set of reusable XML schema documents. These schema documents contain commonly used data components and are grouped into abstraction layers. Each abstraction layer reuses and extends data components from previous layers. The use of NIEM results in machine–Readable information exchanges.

(2) The NIEM model is defined using World Wide Web Consortium Standard Meta Language schema that is technology and platform independent. For example, you can represent NIEM in UML with tooling that implements the NIEM UML profile, and automatically produces NIEM-conformant XML schema.

(3) Any system can put data into an XML document and transmit it to an exchange partner. Any system can receive and parse an XML document to extract the data. The difficult part is ensuring that the system producing the data creates an XML document that means what the receiving system developer thinks it means, and vice versa. NIEM addresses this problem.

(4) The purpose of NIEM is to provide a standard, extensible format for use in the exchange of information between systems. It is a standard way of defining the contents of messages being exchanged. It is about the data and how it is structured. NIEM is not a system or database, nor does it specify how to transmit or store data. NIEM is a data layer. NIEM is rarely seen by itself. Depending on business requirements, information exchanges might also require access controls, policy automation, and other aspects of implementation.

(5) To implement NIEM a user would build an information exchange package documentation (IEPD). An IEPD defines a recurring message in XML and is built to satisfy information exchange business requirements. A developer builds an IEPD by incorporating the necessary NIEM core and domain model concepts.

(6) For information regarding the NIEM core and the military operations domains refer to https://www.niem.gov/communities/military-operations.

*g. Data engineering resource.*

(1) A data engineering resource (DER) is a "specification that is expressed in a formal syntax that is registered. Examples of DERs are XML schemas, Schematron documents, stylesheets, Web Service Description Language documents, taxonomies, ontologies, and conformant samples." DERs are reusable artifacts that support data modelling efforts and engender consistency and commonality across efforts based on the same DERs. DERs are stored on, and available through, a commonly accessible repository DSE (see DODI 8320.07).

(2) Coordinated development and maintenance with data producers, data providers, data consumers, and system developers of DERs will ensure that data and metadata can be understood and used effectively by COI members and unanticipated authorized users.

(3) There are many DERs available across the Army, such as the schemas registered and available on DSE. There are also many other resources available across the DOD and Army that meet the definition of a DER to include the NIEM Core, Global Force Management Data Initiative or the Joint Command Control and Computing Information Enterprise Data Model, and Ground-Warfighter Geospatial Data Model.

(4) DER Specifications are explicit sets of requirements to be satisfied by a material, design, product, or service.

*(a)* A DER may convey the data structure and validation constraints for an information exchange.

*(b)* A DER has the program logic to translate between different representations.

*(c)* A DER has the controlled vocabulary whose terms will be used in data exchanges or metacards.

*(d)* A DER describes the inputs, outputs, and operations for a web service or an information system.

*h. Unique identification/identifier.*

(1) Unique identification/identifier (UID) is a system of establishing globally ubiquitous unique identifiers within the DOD. UIDs help establish authenticity among a group of like items within the receptacle that contains those like items. The goal of the DOD is to establish a set of rules that unambiguously identify discrete independence amongst entities like force structure units or distinguishable persons, places, things, events, or concepts.

(2) Table 4–2 lists where existing UID guidance may be found.

**Table 4–2**
**Department of Defense level issuances with unique identification/identifier guidance**

| Unique Identifier | DOD-level Issuance |
|---|---|
| Personnel Identification | DODI 1000.30 |
| Real Property and Real Property Sites | DODI 4165.14 |
| Global Force Management | DODI 8260.03, DOD Manual 8260.03 Volume 1, and DOD Manual 8260.03 Volume 2 |
| Tangible Personal Property | DODI 8320.04 |
| External DOD Business Partners | DODI 8320.06 |
| Unit Reference Numbers | CJCSI 3156.01A |
| Transportation Tracking Number | DTR 4500.9–R |

Note. UID guidance for acquisition programs and AIS unique identifiers are being developed.

*i. Information technology standards.*

(1) CIO/G–6 and ASA (ALT) collaboratively develop the Army Annual Standards Profile Guidance (StdV–1) which provides the minimum set of standards as the foundation for building solutions that meet Army strategic guidance and achieve interoperability across the enterprise.

(2) The annual standards development process leverages the DISR process to ensure compliance with DOD guidance and to create the StdV–1 and the StdV–2 (see table 2–4).

(3) The standards management process is comprised of the following standards–Related requirements and timelines:

*(a) Department of Defense Information Technology Standards Registry baseline update cycle (three times annually).* Technical working groups consider change requests. For more details on the DISR governance process, see GTG–F website https://gtg.csd.disa.mil. There are three categories of standards:

1. Mandated (for example, Geopolitical Entity Names and Codes, Global Force Management Data Initiative, Global Force Management XML Schema Definition).
2. Emerging.
3. Retired.

*(b) Common operating environment updates (3-year cycle).* This was formerly known as SW Blocking, the COE SoS implementation is currently based on a 3 year planning cycle.

*(c) Army Annual Standards Profile Guidance.* CIO/G–6, in close coordination with ASA (ALT), develops an annual StdV–1 and StdV–2 (see table 4–2). This annual review enables the consideration of minor changes to Army IT standards between COE SoS 3-year cycles. The approved Army annual StdV–1 and StdV–2 and the StdV–1 and StdV–2 for COE are found in the Army Technical Guidance Repository hosted in the Army Capabilities and Architecture Development and Integration Environment (ArCADIE) at https://cadie.army.mil/cadie/portal/default.aspx.

*j. Army Data Management Guides.*

(1) ADMGs provide common guidance for understanding Army data within the context of Army systems and functions. The ADMGs are a suite of documents that includes an overview and specific data-focused IT topic area guides. Each topic area guide defines the subject topic and presents implementation guidance and the standards and technology that support that guide. The ADMG topic area guides describe specific areas of data use, from data capture to decision support.

(2) The ADMG provides a common starting point for understanding and implementing specific IT data related technologies in the context of the goal of an interoperable, cost effective, scalable, enterprise-wide data architecture.

(3) The ADMGs are considered a set of living documents and will continue to evolve in a coordinated manner in order to keep up with the rapid changes in technology and the policies that govern their implementation. The functional categorization of DM knowledge areas is based on the Data Management Body of Knowledge version 2, from the Data Management Association.

(4) The ADMGs topic areas describe implementation along with standards and governance to, in part, enable bringing together data which currently resides in various technology islands and silos into an integrated environment. This supports more effective information sharing and enhances visibility, accessibility, and security of data to the user community. Although the ADMGs themselves are not an architecture, it provides guidance toward the common enterprise guides in which data is architected, designed, developed, governed, standardized, and exchanged.

(5) The current ADMGs topic areas are:

*(a)* ADMG–Business Intelligence.

*(b)* ADMG–Dashboards and Portals.

*(c)* ADMG–Data Aspects of Cloud Computing.

*(d)* ADMG–Data Aspects of Security.

*(e)* ADMG–Big Data.

*(f)* ADMG–Data Quality Management.

*(g)* ADMG–Data Strategy Metrics.

*(h)* ADMG–Data Warehouse.

*(i)* ADMG–Enterprise Resource Planning.

*(j)* ADMG–Master Data Management.

*(k)* ADMG–Metadata Management.

*(l)* ADMG–Big Data.

(6) More information on each individual guide can be found at the following milWiki link: https://www.milsuite.mil/wiki/portal:army_data_management_program/admg.

### 4–3. Army data governance

*a.* Army DM is the exercise of guidance over the management of data assets and the performance of data functions. Data governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. Sound data governance includes a chartered governing body and council, a defined set of procedures, and a plan to execute those procedures. In practical terms, that means putting personnel, policies, procedures, and organizational structures in place to make data accurate, consistent, secure, and available to accomplish the Army's mission.

*b.* Effective data governance makes the Army more efficient by saving money, allowing re-use of data, and supporting enterprise analytics. However, data governance requires more than just a few members of the IT staff with a project plan. It requires participation and commitment of both IT and business management, as well as senior-level executive sponsorship and active consultation with Army organizations and communities of interest. Data governance enables the Army to effectively manage data assets due to assigned functions and rules of the engagement.

(1) *Army Data Board.*

*(a)* The ADB serves as the senior Army data enterprise decision body for development of coordinated Army enterprise positions on data strategy, DM, standards management, and execution in conformance with the Army COE architecture.

*(b)* This board serves as the senior adjudication body across the Army enterprise for IT data and standards issues; acts as the final authority across the Army enterprise for standards, policies, and practices; coordinates data-sharing efforts across the Army enterprise; serves as a certification/waiver approval authority for targeted standards as delegated by the CDO; and collects and disseminates best practices and lessons learned for IT DM and standards communities. This body's primary focus will be to execute the goals identified by ADB members and approved by the CDO.

*(c)* The ADB is comprised of 1- and 2-star level GO/SES members and is chaired by the CDO. Membership includes Army DSs nominated by the Assistant Secretaries of the Army, DCSs, ACOMs, and other areas as defined by the Army CDO and confirmed by appointment letters from CIO/G–6.

(2) *Chief data officer.* Serves as the senior advisor to the Secretary of the Army and the Chief of Staff of the Army on all data issues and reports directly to the CIO on all issues pertaining to Army data and executes other duties as delegated by the CIO. Develops and implements the ADMP. As required, funds projects to complete the goals and objectives of the ADMP and Army data strategy.

(3) *Data steward.* The DS functions include coordinating the migration; consolidating or retiring data in applications, databases, and systems in their respective domain/area; coordinating related activities through the ADB; recognizing the ADB as the final authority across the Army enterprise for data standards, policies, practices, adjudication,

and management; and adjudicating and approving the recommendations of the FDMs for the identification of Army ADSs and their ultimate registration into the DSE tool for authoritative data element and source registration.

(4) *Army data council.* The ADC will work under the direction of the CDO and the ADB. The ADC will coordinate adjudication of unresolved, internal data issues. If any issue remains unresolved, the Secretariat will escalate that issue to the ADB for resolution.

(5) *Functional data managers.* The FDM functions include establish, manage, or participate in data governance bodies for their duty area that will manage and implement the ADMP, Army data strategy, and AIA; oversee the harmonization and adjudication process, raising any unresolved issues to the ADB; develop success metrics for their functional areas and metrics to assess the value and impact of migrating, consolidating, or retiring applications, databases, and systems; and identify ADSs within their area and recommend approval to their DS so that they can be registered in the DSE and adjudicate any non-concurs or critical comments from other DSs and/or their appointed FDMs regarding an ADS that has been submitted to the DSE ADS registry for formal recognition as the true/valid source of the subject data.

*c.* For more information and guidance on Army Data Governance and the Army Data Board Charter, which includes a complete list of duties and functions of the ADB, CDO, DS, and DMs, see https://www.milsuite.mil/wiki/portal:army_data_management_program/governance.

# Chapter 5
# Information Technology Solutions Implementation

## Section I

## Network Capacity

### 5–1. Information technology requirements in military construction projects

*a. Information technology included in the prime contract.* U.S. Army leadership directs that military construction (MILCON) projects give a complete and usable facility at Soldiers' readiness date and, to meet these goals, directs that all IT requirements be included in the prime contract. IT items are normally user/NEC procured and installed after the beneficial occupancy date when the building contractor turns the facility over to USG and before Soldiers' readiness date when the organization occupying the building moves into the facility. The IT installation is called the "IT fit-out." The incorporation of IT within the prime contract consolidates IT requirements under the U.S. Army Corps of Engineers (USACE) contracting authority. The installation information infrastructure architecture (I3A) technical criteria for SIPRNET is available at 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 OPA capital investment 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.

*c. Assistant Chief of Staff for Installation Management project process for new military construction.* MILCON requesting organizations will comply with AR 420–1 and DA Pam 420–11 that outline the details for timelines and programming for all MILCON projects. MILCON IT requirements are grouped under three categories: MILCON (sometimes referred to as construction or "C costs"), IS (sometimes referred to as "I costs"), and mission unique equipment (MUE) costs (sometimes referred to as proponent or "P costs").

(1) Examples of military construction Army IT costs are IT installation in the building (inside plant) from the wiring closet to the desk wall jacket, video teleconferencing (VTC) wiring, and access system conduits and doors. An IS example is the NIPRNET/SIPRNET or Voice over Internet Protocol phones. The MUE costs are the other IT costs associated with the building occupant's mission or "above standard level of IT service" requirements. For example, knowledge walls which are the center for aggregated information used for monitoring and analyzing to make critical decisions related to military operations. Multiple sources, both secure and public, are used within the command center for making decisions. These sources of information are then displayed on the knowledge wall. This fast-paced and mission-critical environment typically consists of the main command area, offices, meeting rooms, and briefing rooms.

(2) ACSIM's MILCON integrated process team has a subcommittee MUE I team which looks at all MILCON MUE IT requirements to ensure that nothing is left out, that the amount requested for programming is not excessive, and that the MILCON requesting organization submits their project's MUE POM requirements via their command's appropriate MDEP to the PEG. The MDEP manager should identify in their submission that the MUE funds be directed to APE B3150 for IS. ACSIM's MDEP manger will program the MILCON projects "C" and "I" costs based

on the IT requirements in the DD Form 1391 (FY__ Military Construction Project Data), with funds going to APE BB 8650.

*d. Assistant Chief of Staff for Installation Management renovation and modernization military construction process.* Renovation and modernization (R&M) MILCON requesting organizations will also comply with AR 420–1 and DA Pam 420–11 for all R&M projects for IT.

(1) Requesting organizations submit their projects' MUE POM requirements via their command's appropriate MDEP to the PEG. The MDEP manager should identify in their submission that the MUE funds be directed to APE BB 8700 for IS. ACSIM's MDEP manager will program the MILCON's "C" and "I" costs based on the IT requirements in the DD Form 1391, with funds going to APE BB 8650.

(2) Requesting organizations are advised to closely read both AR 420–1 and DA Pam 420–11 where "C" and "I" requirements are less than the threshold amounts and most of the burden is on the requesting organizations to fund the R&M IT costs.

(3) Coordination will be made with the installation NEC for repair and restoration projects that do not require a DD Form 1391 as soon as the project is established. DA Pam 420–11 will be used to establish duties for funding of IT.

*e. Network Enterprise Center functions.*

(1) The NEC documents the project's IT requirements, develops the input to DD Form 1391 information systems cost estimate (ISCE), and provides the 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 the customer's 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 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 tab F if the project scope or building functional requirement or site location is changed. The ACOM; ASCC; DRU; and 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 SW provided by the USACE. The ISCE SW 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.

*f. 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 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 U.S. Army Installation Management Command.

(3) USAISEC FDED exercises oversight of MILCON IT. USAISEC FDED performs the following functions:

*(a)* Provides planning, programming, and budgeting input to the U.S. Army Communications-Electronics Command for procurement of standard level of services equipment and SW such as common user IT instruments and switching equipment in support of IT in MILCON funded construction. The appropriate PM or program executive office provides planning, programming, and budgeting input for mission-oriented IT in MILCON-funded communications facilities construction.

*(b)* Reviews user IT (in functional terms), reviews the user-developed ISCE for each proposed MILCON project submitted, and provides certification to ACSIM (DAIM–FD) prior to the project review board (PRB).

*(c)* Provides the installation; the Theater Signal Command or the ACOM, ASCC, or DRU; 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 IS.

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

*(f)* Participates in ACSIM PRBs for all ACOM, ASCC, and DRU MILCON programs.

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

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

*g. 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 started as early as possible in the project's development cycle and updated throughout the design cycle. In this process, the following agents have major duties:

(1) *Theater Signal Command or Army command functions.* The Theater Signal Command or ACOM, ASCC, or DRU reviews and certifies the NEC's ISCE for the project. The Theater Signal Command or ACOM, ASCC, or DRU may use a variety of methods to complete this task, including the ISCE for Windows SW, internal staff reviews, and assistance from USAISEC FDED.

(2) *U.S. Army Information Systems Engineering Command Fort Detrick Engineering Directorate functions.*

*(a)* The USAISEC FDED plays several parts with respect to the project's ISCE. As an agent of the ACSIM, USAISEC certifies the ISCEs intended for MILCON 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 on MILCON 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, ASCC, or DRU; and the NEC involved with each particular project.

*(b)* USAISEC FDED routinely reviews and updates the ISCEs on MILCON 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, ASCC, or DRU; 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, ASCC, or DRU. 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.

## 5–2. 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 policy addressing energy management for IT equipment within the Army and coordinating with ARCYBER, PL CHESS, and ACSIM to achieve 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 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 distributed in the Army Golden Master operating system image will be set to put the computer to sleep in 30 minutes. A group policy will also be used to push this setting out to ensure consistency using the system center configuration manager facility.

(2) *Monitors.* After 15 minutes of inactivity, monitors and laptop displays will enter into sleep mode. The power options for the Army Golden Master operating system image will be set to put the monitor or display to sleep in five minutes, and a group policy will be used in the system center configuration manager facility to push this setting 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) *Other computers and devices.* Other computers and devices, which are not desktops or laptops normally employed by a single end user at a time, such as servers, storage area network (SAN) devices, kiosk-type displays or

operations center monitors and other network infrastructure are not required to be powered off or in standby during periods of non-use.

### 5–3. Army data center consolidation

*a.* The Data Center Optimization Initiative established by Federal Chief Information Officer Memorandum requires agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure such as cloud services and interagency shared services. The ADCCP is the Army response to the OMB and DOD requirement to develop a plan to consolidate data centers. CIO/G–6 serves as the overall ADCCP project lead on behalf of the Secretary of the Army. The ADCCP establishes standards and assigns duties for the migration of applications and consolidation of data centers. Army organizations must maintain their data center records in APMS at https://cprobe.army.mil/enterprise-portal/web/apms/home, to include all required DOD data center inventory management (DCIM) system data elements. These include, but are not limited to, server counts by operating system, workforce numbers, data center square feet, and virtual operating system number. This information is required to provide the input to the DCIM tool, which is done by members of the ADCCP team to inform DOD CIO of the status of Army inventory and closures. The ADCCP team will review the APMS records for each data center when processing ITAS requests for data center related purchases. The 30 January 2018 APMS Change Control Board authorized the continued use of the ADCCP Tracking Tool at https://service.peoavn.army.mil/ for applications management and continued use of APMS for data center management. Army organizations are required to utilize the ADCCP Tracking Tool to perform all application management functions, including rationalizations, dispositions, and applications reporting. An interface has been established between APMS and the ADCCP Tracking Tool to ensure accuracy and consistency of data center information that is propagated back to the ADCCP Tracking Tool.

*b.* The effort will consolidate data centers, move the Army toward cloud services and provide enterprise hosting as a managed service, and improve the security of Army information assets to reduce costs and use off-premises cloud computing capabilities to the maximum extent possible (see Army Directive 2016–38). As required by the Data Center Optimization Initiative, the 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.

*c.* Army data center owners must maintain their data center records in APMS to include all required DCIM system data elements. These include, but are not limited to, server counts by operating system, workforce numbers, data center square feet, and virtual operating system number. This information is required to provide the input to the DCIM tool, which is done by members of the ADCCP team to inform DOD CIO of the status of Army inventory and closures. The ADCCP team will review the APMS records for each data center when processing ITAS waiver requests for data center related purchases.

*d.* Army data processing facilities will adhere to facility purpose definitions found in the DOD Data Center Reference Architecture (https://dodcio.defense.gov/inthenews/dodinformationenterprisearchitecture.aspx) and will be identified as the highest-level purpose in the following order: core data center, Army enterprise data center, installation processing node, special purpose processing node, installation service node, geographically separated unit, and tactical processing node (TPN). At this time, Army and DOD do not track geographically separated unit or TPN facilities. To be classified a TPN, a system must be designed to be deployed with a unit and moved and cannot be a fixed facility.

*e.* When completing the initial draft of a data center closure report, commands will ensure the information in the closure report (personnel, servers, applications, floor space, power consumption, SAN storage, and cost savings) matches the information in the data center record in APMS. If the information in the closure report is more current, update the record in the APMS accordingly. Once the draft report is completed, submit to the CIO/G–6 ADCCP office for review. Data center facilities with three or more servers must complete the conventional closure report template. Data center facilities with two or less servers are authorized to complete the Vice Chief of Staff of the Army Small Data Center single-page memorandum. All signed closure reports require a GO/SES signature for final approval. Resources for completing these documents are available at https://cprobe.army.mil/enterprise-portal/group/dco/dco.

*f.* Discovery rationalization of data centers and applications is supported by the PEO EIS Application Management Business Office. When considering cloud service offerings, platform as a service and software as a service offer much better value than infrastructure as a service. Use Application Management Business Office to help develop cost benefit analysis, particularly the to-be hosting costs for a wide variety of enterprise computing environments, including commercial cloud.

(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 APMS 6 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 CIO/G–6: servers, voice switching equipment, racks, SAN storage, matrix switches, optical storage systems, tape drive and storage devices, and mainframe computers. Data centers or server rooms are not to be constructed, renovated, and/or leased without a written waiver, granted in advance by CIO/G–6. Web-based waiver requests can be submitted at https://cprobe.army.mil/enterprise-portal/web/itas/home. 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.

*(c)* Army commands, organizations, and data center owners need to register all data centers in APMS and provide application information in APMS at https://cprobe.army.mil/enterprise-portal/web/apms. Army data center inventory, closure, and application consolidation processes and activities are all inventoried and tracked through APMS.

*(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) *Army command, Army service component command, and direct reporting unit requirements.*

*(a)* Provide quarterly reporting requirements in accordance with the ADCCP reporting schedule to meet DOD CIO, OMB Federal Data Center Consolidation Initiative deliverables, and Army senior leadership reporting in support of the ADCCP quarterly updates. Provide and validate the current list of planned (through the current fiscal year) and completed (with GO or civilian equivalent signed closure report) data center closures. In addition, ACOMs, ASCCs, and DRUs should use APMS 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 the 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 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 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 APMS 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 APMS 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 APMS quarterly. These reports will be reviewed at the CIO/G–6 ADCCP quarterly updates.

*(d)* System/application owners must input cloud–Related data into APMS. Command resource reporting of cloud hosting activity is required to support the Army's IT budget submission process, DOD oversight, and external reporting to both OMB and Congress. The data elements needed to support these requirements are available in APMS. Commands must identify all systems and/or applications that are currently using or are planning to use cloud services. This includes government cloud services acquired through memorandums of understanding or similar agreements, commercial cloud services provided directly through a hosting contract, or commercial cloud services provided through "other direct costs."

*g.* The MIRC serves as an advisory body for implementation for tasks specified within Army Directive 2016–38. Army commands and organizations will report to the MIRC on a regular basis to provide updates on data center consolidation, request deferrals, or re-designations that deviate from the schedule in Army Directive 2016–38.

## 5–4. Network systems

*a. Local area network and wide area network.*

(1) The NEC plans and manages wide area network (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) Wireless networks should be considered whenever a network (re)cabling is called for. Wireless use should be encouraged. This is particularly true for SIPRNET extensions where passive detection system simulators are impractical. Where wireless LANs are to be implemented, the NECs must conduct 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 and certified cybersecurity personnel meeting the standards specified in DODD 8140.01 can successfully determine these risk factors. All wireless local area network (WLAN) installations to include stand-alone and commercially connected networks are subject to the same reviews and RMF requirements as those that are connecting to the NIPRNET/DODIN–A.

(2) WLANs may be used as an extension of the departmental LAN or the common user installation transport network where fixed infrastructure connectivity is unavailable.

(3) Standard interfaces for WLANs are IEEE 802 series. WLANs operate in the 2.4 to 2.484 gigahertz (GHz) and 5.743 to 5.830 GHz range. DOD mandates that all WLAN devices used within CONUS 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 LAN at a remote location using the internet or any unsecure 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 that were not deemed critical mission have been deleted. The CONUS RCC 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 identifications and passwords to prevent non-authorized access to the internet protocol router network. Dial-in service is given through local terminal servers or over remote 1–800 service.

*(a)* Army ACOMs, ASCCs, and DRUs 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 SBU.

*(b)* The installation NEC, or designated official, appoints a service provider who issues Army personnel a valid user identification 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 identification 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.* The supporting NEC will be the focal point for all baseline BASECOM on the installation or the supported area and the initial focal point for tenant organizations and activities to obtain support for BASECOM requirements not provided in the C4IM Services 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.

(1) *Command, Control, Communications, Computers, and Information Management 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 ARCYBER. A lack of NEC support does not negate the requirement to procure devices and service through ARCYBER or the use of the BPAs. For Army organizations located on Joint bases where ARCYBER/NETCOM is not the procurement or service provider for wired telephone service, such as Joint Base San Antonio (where the U.S. Air Force is the proponent for wired telephone service units), organizations will follow the procedures in paragraphs 5–4*d*(2) through 5–4*d*(5).

(2) *Service requests.* NECs will submit BASECOM service requests to ARCYBER G5 with a courtesy copy provided to the respective NETCOM Signal Command Theater office. ARCYBER will obtain BASECOM telecommunications service requests such as local central office trunks, commercial business lines, foreign exchange trunks, and/or lines via consolidated local service contracts that are competed among interested service providers. ARCYBER will satisfy requirements for BASECOM local leased telephone services through BASECOM consolidated contracts and wireless requirements via BPA contracts. NECs will obtain operation and maintenance for installation telephone plants through ARCYBER. Those interested in acquiring local leased telephone and telephone–Related services should email the point of contact at email address usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil. If the existing consolidated contract cannot be used to satisfy the requirement, ARCYBER will competitively award a new contract to satisfy the requirement. ARCYBER 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 ARCYBER 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 ARCYBER contracting officer.

(4) *Wireless.* The ARCYBER G3 is the primary point of contact for procuring wireless (cellular) services and devices in accordance with UC APL multi-function mobile devices at https://aplits.disa.mil/processaplist.do. When procuring wireless (cellular) services and devices, all Army users are required to utilize the ordering procedures established by ARCYBER 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 BPA list, a request for exception to procure from other sources will be submitted to CIO/G–6 for approval through the ITAS waiver application. 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 CIO/G–6. 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, 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 secure telephone equipment. 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, PCs, and unclassified facsimile 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 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 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 non-cleared 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) *Secure communications.* Communications security 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) *Wireless intrusion detection systems.* 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 hour/7 day a week 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 1 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 cybersecurity compliance requirements.

### 5–5. Telecommunication systems and unified capabilities

Guidance related to Army telecommunications and UC (data, video, and voice) previously contained in AR 25–1 is provided in AR 25–13. All Army users will refer to and follow the policies, procedures, and guidance contained in AR 25–13 with respect to telecommunications and UC requirements and operations.

*a. Time-division multiplexing equipment.* Further investment in legacy voice switching (time-division multiplexing (TDM)) equipment is terminated. A majority of Army TDM equipment is beyond useful life. Commands will reduce or eliminate TDM circuits. Commands that have an urgent requirement to purchase (or have already purchased) TDM equipment will submit requirements through the CIO/G–6 ITAS waiver process.

*b. Everything over Internet Protocol migration.* The Army will migrate as soon as practical to an almost Everything over Internet Protocol architecture, to include UC and collaboration, with an end state of end-to-end internet protocol.

*c. Asynchronous Transport Mode.* Further investment in Asynchronous Transport Mode (ATM) equipment or ATM interfaces on customer or provided edge equipment will be terminated and no longer installed within Army networks. All Army organizations that continue to require ATM support are responsible for providing the funding for required levels of support.

*d. Integrated Services Digital Network.* All Army organizations will cease investment in (non-emergency) Integrated Services Digital Network (ISDN) supported technology, equipment, and transport. All Army organizations will transition from ISDN to a compatible IP-supported technology or service including, but not limited to, video, facsimile, voice, and other network capabilities.

## Section II

## User Facing Services

### 5–6. Federal law, regulation, and policy compliance

*a. General.* Army public websites must comply with applicable federal law, regulations, and policies, including DODI 8520.02. 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.shtmlfor additional guidance.

*b. Accessibility.* Army internet services and Army information will be accessible to disabled employees and disabled members of the public, and access will be comparable to that available to non-disabled individuals in compliance with the requirements and alternatives in DODM 8400.01. Information regarding current standards, SW, and equipment are provided at http://www.section508.gov/.

*c. General.* All federal agency acquisitions of electronic and information technology (EIT) should meet the accessibility standards of 29 USC 794d (known by the common name 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 (Section 1194, Title 36, Code of Federal Regulations (36 CFR 1194)) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board) (see AR 25–1).

*d. 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 websites, multimedia, and office equipment (such as copiers and facsimile 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.

*e. Computer/Electronic Accommodations Program.* 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 website at www.tricare.osd.mil/cap/).

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

*g. 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.* Defined in 40 USC 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 Public Law 101–336 (known as 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 electronic and information technology 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 Section 508 standards. Contractor employees in their professional capacity are not considered 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) *Micro-purchases.* Purchases of $5,000 and under are no longer exempted from Section 508. Contracting officers and purchase cardholders are to use the same accessibility standards in micro-purchases as any other EIT purchases.

*h. 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 review.

(4) Contractor-procured EIT that is incidental to the contract, and in spaces frequented only by service personnel does not require documentation under Section 508.

(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.

*i. 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, CIO/G–6 is available to give technical and NSS assistance via email at 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 duties 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.

*j. Collecting information.* Information collection via surveys, forms, Army internet services, internet-based capabilities (IbC), or other means are governed by distinct policies and guidelines.

(1) When collecting information from Army personnel, their families, other federal agency personnel, contractors, or members of the public, comply with AR 335–15.

(2) Consistent with 5 USC 552 and 5 USC 552a, no information will be collected on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, press, and religion, except when—

*(a)* Specifically authorized by statute.

*(b)* Expressly authorized by the individual about whom the record is maintained.

*(c)* The record is pertinent to, and within the scope of, an authorized law enforcement, intelligence collection, or counter intelligence activity.

*(d)* Information collection of personally identifiable information (PII) stored in a Privacy Act SOR provides a Privacy Act Statement (PAS) (see AR 25–22).

*(e)* Electronic collection of information requires the completion of a DD Form 2930 (Privacy Impact Assessment (PIA)).

*k. Copyright.* Any matters pertaining to the creation or use of works of USG must be reviewed by legal counsel before dissemination. For information pertaining to the rights of copyright owners, please refer to DODD 5535.4, DODI 5120.04, and AR 27–60.

*l. Information control, dissemination, and marking.* Policies and guidance governing dissemination and marking of specific categories of information will be complied with when those specific categories of information are disseminated.

(1) PII, as defined in DODD 5400.11, will not be disclosed beyond the allowances described in DOD 5400.11–R. Personal and personnel security must be considered and public disclosure of PII should be limited to pictures, names, biographies, and contact information of Army personnel who, by the nature of their position and duties, frequently interact with the public, such as general or flag officers, public affairs officers, or personnel designated as official spokespersons. Public disclosure of family information will be generic and not include specific information such as names or ages. This includes PII in photographs, videos, captions, and other media.

(2) Social security numbers (SSNs) will not be posted in whole or in part, and release of documentation containing them must follow Director, Administration and Management memorandum dated November 23, 2010, subject: Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites (http://dpcld.defense.gov/portals/49/documents/privacy/osd%2013798–10.pdf). In general, the Army is required to minimize the use of SSNs as a unique identifier for individuals. When an SSN is used on forms and in an IT system, an SSN justification memo must be prepared in accordance with DODI 1000.30 (see AR 25–22).

(3) Potential privacy, operational security (OPSEC), and IA consequences of distributing information must be evaluated before dissemination. Only unclassified information of value (useful) to a given audience (less adversaries) should be disseminated via unclassified Army websites.

(4) A process for information review will be implemented as defined in DODI 8550.01, Enclosure 3.

(5) Army internet service and IbC users who believe that Army information available via an unclassified Army internet service or IbC is classified, sensitive, or would constitute classified or sensitive information when aggregated with other information available via open sources, should report the details through command channels or to their information security or OPSEC office(r) for evaluation and appropriate action (see DODD 5210.50). Once a security determination has been made, appropriate action by the user includes notifying the Army owner(s) or operator(s) of the Army internet service or information in IbC.

*m. Privacy Act Statement.* The Privacy Act of 1974 requires agencies to provide a PAS to all individuals asked to provide personal information about themselves, which will go into a Privacy Act SOR (in other words, the information will be stored and retrieved using the individual's name or other personal identifier). Refer to AR 25–22 for information regarding SORs.

(1) A PAS must include the following elements: authority, principle purpose, routine uses, and disclosure.

(2) All solicitation methods in any format, including but not limited to, forms, paper, website, web portal, and email, must have a PAS if the information will be stored in a Privacy Act SOR. If the personal information is collected and maintained in a Privacy Act SOR, a Privacy Act System of Records Notice (SORN) will be published in the Federal Register. Please refer to AR 25–22 for information regarding a SORN.

(3) The PAS should be placed or provided near or before the collection of information. For example, on a website near the data fields collecting data, or if face-to-face, provided verbally or printed/posted before information is solicited from the individual.

(4) A PAS is also required when individuals are asked to confirm that their data is current and correct.

*n. Privacy Advisory.* An advisory is used when an individual is asked to provide personal information about themselves that will not be stored in a Privacy Act SOR.

(1) The advisory should inform the individual as to why the information is being solicited and how the information will be used. It should include a brief description, if applicable, of the Army's practices with collecting, maintaining, using, or disseminating the PII being requested.

(2) All solicitation methods in any format, including but not limited to, forms, paper, website, web portal, and email, should include a Privacy Advisory.

(3) A Privacy Advisory should be placed or provided near or before the collection of information. For example, on a website near the data fields collecting data, or if face-to-face, provided verbally or printed/posted before information is solicited from the individual.

(4) A Privacy Advisory should be provided when individuals are asked to confirm that their data is current and correct.

*o. Privacy policy on websites.* Clear privacy policies will be posted or linked to on public Army internet services in compliance with OMB Memorandums M–17–06 and M–07–16.

(1) Privacy policy must—

*(a)* Be written in plain language and organized in a way that is easy to understand and navigate.

*(b)* Provide useful information that the public would need to make an informed decision about whether and how to interact with the Army.

*(c)* Be updated whenever the program and or Army makes a substantive change to the practices it describes.

*(d)* Include a time/date stamp to inform users of the last time the program or system had substantive change to the practices the privacy policy describes.

*(e)* Adhere to all other applicable OMB requirements.

*(f)* Include a link to the Army's Privacy Program page.

(2) Privacy policies should be on principal, sub-agency, component, and program websites, mobile applications, and other digital services. For each website, agencies must post a link to that website's privacy policy on any known, major entry points to the website. This requirement does not apply to internal Army activities (such as intranets or online interactions that do not involve the public).

(3) If the website is providing content to children under the age of 13 and collects, maintains, or discloses children's PII, the sponsoring organization may be required to comply with the requirements in 16 CFR 312. Among other things, these requirements include adding a section in the Army's privacy policy that pertains to these activities.

## 5–7. Content propriety and quality

*a. Information of value.* Army public websites should only post information of value to their visitors. These visitors include users from Army organizations, other government agencies, academies, and the private sector.

*b. Content limitations.* Army public website 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 websites may not be directly linked to or refer to websites 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 website 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 website. Home pages will minimize extraneous content to allow visitors to get to the content they need and want most.

*e. Exclusive information.* Websites 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 Army Knowledge Online (AKO) or other approved intranet site.

*f. Public website content.* Webmasters and/or maintainers should provide the following content in each Army public website:

(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).

*(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 emailing foia@rmda.belvoir.army.mil/.

(2) Main entry point websites (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 at 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)* Website 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 website, 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 websites.
2. Security policy.
3. How to request information under FOIA.
4. Accessibility policy.
5. Information quality guidelines.

*g. 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 websites.

## 5–8. Usability criteria

The usability guidelines contained at http://www.usability.gov/ may be a valuable tool for website designers.

*a. Accessibility.* Army public websites must be accessible to all citizens (see AR 25–1).

*b. Public website requirements.* Public websites must be developed according to the following guidelines:

(1) Webmaster 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 website visitors. Army public websites will minimize page download times for their visitors to the maximum extent feasible.

(2) Websites 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 Section 508 of the Rehabilitation Act.

(3) Information should be presented using plain language that considers the knowledge and literacy level of the typical visitor. The text must be gender neutral and be accessible to persons who, because of national origin, are limited in their English proficiency. Understandable language and content criteria should be 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-ins or additional SW 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 the 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 websites 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 SW able to read the format. Raw data files provide the greatest flexibility for the public and are preferred over proprietary formats requiring specific commercial SW. Consistent navigation schemes between and within all Army public websites will be used.

(7) Visitors are more likely to get what they need from a site if changing navigation does not 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) Webmasters and/or maintainers should include either a search box or a link to a search page from every page of the website. 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. Websites 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 websites will answer 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 documents or collections? Will visitors enter phrases or keywords? What other hints can visitors be given?

*(c)* What is the expected search response time? For example, 95 percent of searches get a result set returned within 5 seconds.

*(d)* How can customers use the search engine for more precise searching and browsing (that is, minimum chaff) or for recall (that is, maximum wheat)? For example, if searching for a specific marketing report, include the country name, the year, and the type of report (for example, strategic planning).

(9) Include the following five meta tags on all home pages and major entry points:

*(a)* Page title.

*(b)* Description.

*(c)* Creator and/or sponsor (in most cases, the organizational name).

*(d)* Date created.

*(e)* Date reviewed.

(10) Website visitors will be informed about major proposed and implemented changes to the website. Webmasters 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.

### 5–9. Consistent and nonredundant information

*a. Redundancy.* Content and services provided via Army public websites should not be redundant or in conflict with each other. The requirements paragraphs 5–9*b* through 5–9*d* will be implemented by all Army public websites so that this is achieved.

*b. Links to information.* Websites 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 website.

(2) When an organization website 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 website 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 website'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 websites 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 websites or to portals and specialized websites regularly to ensure they are current and accurate.

*c. Home page link.* To improve website utility, each web page links back to the website 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 (http://www.army.mil/). Subordinate elements of a major command should provide links back to the respective major command and the Army home page.

*d. Home page link.* Major organizational home pages (Army, ACOM, ASCC, DRUs, and HQDA staff elements) should link to the USA.gov home page at https://www.usa.gov/ with the entry "USA.gov: U.S. Government Web Portal."

## 5–10. Training and compliance

*a. Sponsor functions.* Army public website sponsoring organizations must ensure that website 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 webmasters and/or maintainers, reviewers, and content managers must complete required training, 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 via AKO at https://iatraining.us.army.mil. Web content and operations security certification courses are mandatory for all webmasters and/or maintainers.

## 5–11. Website planning and sponsorship

*a. Target audience.* Websites 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, other enterprise portal, or approved private website.

*b. Accurate information.* All Army websites must provide accurate, current, and official information, regardless of whether the site is private, public, or other web-based capability.

*c. Website purpose and plan.* Any Army organization that establishes a public website (or web presence) must have a defined purpose and website plan supporting the organization's mission. The plan should be approved by the organization's parent command or organization. The website plan must at least address:

(1) Website registration (Who? Where? How?).

(2) Identification of webmaster contact information.

(3) Procedures that explain administration of the website 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 website(s) during disasters or emergencies, including important information and services to be provided to the public.

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

(5) Assessing the user's satisfaction. Army public website sponsors should conduct an annual assessment of user satisfaction with the website, 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 websites:

(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 decision-making process that contain opinions and recommendations. This exemption includes draft documents, draft publications, or pre-decisional information of any kind.

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

(9) Lists of names and other PII of personnel assigned within a particular component, unit, organization, or DA office. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties—such as GOs and SESs, public affairs officers, or other personnel designated as official command spokespersons—is permitted. In addition, command websites 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 must be limited. Publishing on an unlimited access website represents global release. Some information appropriate for installation newspapers is not appropriate for public websites. Army organizations may reproduce the content of installation newspapers for the web, if that content meets the restrictions provided in paragraph 5–11 of this pamphlet 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 websites.

*e. Domains.* New Army public websites are established in the army.mil domain to show that they are official sources of Army information. This applies to all websites. Organizations using non-.mil domains should execute plans to transition websites to the army.mil domain in order to comply with federal website policy. For exceptions to the use of the army.mil domain, see paragraph 5–12.

*f. Website listings on the Army home page.* The Army home page (http://www.army.mil/) provides public website locator information for the Army's units and installations (Army A–Z). Organizations and installations with public websites will register on the Army A–Z locator by visiting this site https://www.army.mil/contact/.

*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 RCC. CONUS RCC is part of ARCYBER. ARCYBER supports Army installations needing to apply for internet protocol addresses via the NIPRNET and SIPRNET.

(2) NEC or others with registration duties select the internet registration option on the RCC website 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 via email directly to domain–request@aims7.army.mil/.

*h. Web records administration.* Web records must be managed in accordance with OMB Circular A–130 and guidance from the National Achieves and Records Administration (see 36 CFR Chapter XII and www.archives.gov/records_management/index.html/).

*i. Webmasters and maintainers.* Army organizations assign a webmaster for each public website they sponsor. The webmaster and maintainer have technical control over the registration process, managing the site's content, and ensuring the site conforms to Army website requirements.

*j. Sponsorship display.* Army public websites must clearly display "U.S. Army" on every page, along with the organization's official name and include a statement that the website 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.* Information will be labeled to indicate the status of the content such as draft or copyright or trademark.

*l. Drafts.* Draft policies, regulations, and other pre-decisional information are not posted on public websites.

*m. Copyrights.* Copyrighted information for which releases from the copyright owner have not been obtained will not be posted on public websites.

*n. Website linking.* USA.gov (https://www.usa.gov/linking-policy) provides best practices for creating links from public government sites to content maintained on other sites. Consider leveraging the guidance as a part of your site management.

*o. Date posted data.* Army public websites 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. Webmasters and/or maintainers should include a statement such as "Last updated on" or a date stamp to each page altered or reviewed.

*p. Social media sites.* All social networking sites (SNS) and social media sites must register with http://www.army.mil/socialmedia/. Social media sites are a sub-category of websites and all website 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 (EOPs) 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/.

*q. 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).

## 5–12. Army website domain name exceptions

*a. Waiver requests.* All Army websites must have a .mil domain name unless a waiver is granted by CIO/G–6. To request a non-.mil domain name (for example, .com, .net, .org, .info, .edu, or .gov), the requesting Army organization must compose a waiver request memorandum on the organization's letterhead and address the waiver request memorandum to CIO/G–6.

*b. Addressee.* The waiver request memorandum should be addressed as follows: Memorandum to Army Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

*c. Required waiver request content.* For all non-.mil domain name waiver requests, ensure the following items are addressed in the waiver request memorandum:

(1) State the intended domain name of the website.

(2) State the purpose of the website and the period of time in which the website will be used.

(3) Cite the authority (statute or regulation) to disseminate/exchange the site's information.

(4) Name the Army or DOD sponsor of the website.

(5) State why the organization requires the website to use a domain other than army.mil by selecting one of the reasons provided on the Non-.mil Criteria Checklist (see https://www.milsuite.mil/wiki/non-.mil_domain_waivers).

(6) Is the website for nonpublic access only? If so, explain why AKO or another.mil site cannot be used. Provide confirmation from AKO that other .mil solutions are not achievable for the mission.

(7) If the website operates on the server of a commercial internet service provider, then the requestor is required to either:

*(a)* Obtain a DOD TEP for use of a commercial internet service provider ("internet service provider waiver") prior to applying for use of the non-.mil domain name, or

*(b)* Provide a copy of a signed DOD CIO memorandum approving the use of the commercial internet service provider (as prescribed in CJCSI 6211.02D and DODI 8100.04) to CIO/G–6 (SAIS–CB). The process for acquiring or verifying an internet service provider waiver is found on the SNAP portal at https://snap.dod.mil and the DISN Connection Process Guide at http://disa.mil/connect. If the site is not operating via a commercial internet service provider, then provide the name of the federal, DOD, or military service provider (for example, DISA).

(8) If the requesting organization has not listed the website in the APMS, ensure the website is in APMS. Once the website is listed in APMS, provide the AITR number for the website in the waiver request memorandum.

(9) Confirm that there will be no association with the name of the private provider and that the website contains no commercial advertising, commercial trademarks, or commercial symbols.

(10) Confirm that the domain uses only hypertext transfer protocol secure (HTTPS) rather than hypertext transfer protocol (HTTP) access control.

(11) If the website collects, stores, or processes any FOUO or classified information, then select the option from Section IV of the Non-.mil Criteria Checklist that describes how the website handles FOUO or classified information.

(12) If the website is access controlled (for example, with use of a password or PIN) but does not require access with a CAC or EAMS–A, then:

*(a)* Explain the reason why CAC or EAMS–A is not used, or reference an approved identification and access management CAC/PKI waiver (the identification and access management CAC/PKI waiver is obtained from CIO/G–6 Identity Management).

*(b)* Provide a reference for the site's approved External Certificate Authority (see listings at http://iase.disa.mil/pki/eca/index.html).

*(c)* Provide the access controls used (for example, password protection, PIN, biometrics, and so on).

(13) State any PII concerning a military Servicemember or Family member that will be requested/required and maintained at the site, and state how the PII is safeguarded according to the options provided in Section V of the Non-.mil Criteria Checklist.

(14) State the date of the last OPSEC review (for established websites) or provide confirmation of coordination with the Army web risk assessment cell (AWRAC) for an OPSEC review. AWRAC can be contacted at commercial phone: (703) 323–2072 or via email at usarmy.belvoir.arcyber.mbx.awrac@mail.mil.

(15) Provide your organization's point of contact information for this waiver request.

*d. Memorandum signature.* The waiver request memorandum must be signed by at least the rank of colonel or equivalent position, from the G–6 of the requester's HQDA parent organization.

(1) Scan the signed/dated waiver request memo and forward to usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil.

(2) Along with the waiver request memo, send copies of your organization's authority to connect and ATO.

(3) If your organization requests a ".gov" domain, then also send with the waiver request memo a completed copy of the DODI 8410.01, Enclosure 5.

## 5–13. Internet-based capabilities

IbC are required to follow guidance on the collection, dissemination, storage, and processing of unclassified Army information.

*a. Advertising and endorsement.* For the purpose of advertising, public Army internet services are government publications. In accordance with DOD 5500.07–R, U.S. Congress Senate Publication 101–9, and DODD 5500.07, the credibility of Army information must not be adversely affected by association with nongovernment sponsorships, advertisements, or endorsements.

(1) Any advertisement by or for any private individual, firm, or corporation will not be inserted or allowed on public Army internet services prepared or produced with either appropriated funds or NAFs. Army endorsement will not be implied in any manner for any specific nongovernment service, facility, event, or product.

(2) Stand-alone nongovernment graphics, logos, or aggrandizing statements such as "Powered by," "Serviced by," and "Designed by" will not be inserted or allowed on public Army internet services, or the Army-controlled content area of an IbC prepared or produced with either appropriated funds or NAFs. Proprietary rights notices (including copyright and trademark notices) are not aggrandizing statements. Copyright notices are required as described in DODD 5535.4 and DODI 5120.04. Factual acknowledgment of partners, SW, technology, and services used on a public Army internet service may be included in descriptive information about the service or the organization, such as an "About Us" page. However, such acknowledgment should be carefully considered in the security risk assessment and risk mitigation measures for the service and may not be used in any manner that supports the appearance of endorsement. Factual acknowledgment may include a corresponding nongovernment graphic, logo, or trademark. This graphic, logo, or trademark may be used as a hyperlink to the corresponding nongovernment website or service; however, the link must be disclaimed as described in DODI 5120.04.

(3) Users will not be required or encouraged to choose any specific brand of browser SW or other client applications to access public Army internet services and IbC. Army websites must be designed in accordance with accepted standards of the World Wide Web Consortium (http://www.w3.org/standards/) to ensure browser compatibility.

(4) Remuneration of any kind (for example, payment, reimbursement, reduced prices, and gifts) will not be accepted in exchange for advertising, acknowledgment, or endorsement without specific statutory authority to do so. Accepting remuneration may constitute an improper augmentation of appropriations in violation of 31 USC Chapter 13 and 31 USC Chapter 15.

(5) Nongovernment advertising in electronic versions of morale, welfare, and recreation (MWR) products is governed by DODI 1015.10, Enclosure 12. Such advertising must only be displayed via private Army internet services that ensure distribution is limited to authorized customers.

(6) Advertising in electronic versions of Army newspapers, magazines, and civilian enterprise publications is governed by DODI 5120.04.

*b. External links disclaimer.* Links to government internet services will not be disclaimed. The quoted disclaimer in Figure 5–1 will be displayed or linked on public Army internet services that have nongovernment links, or through an intermediate "Exit Notice" page generated by the server whenever a request is made for any nongovernment link.

"The appearance of external hyperlinks does not constitute endorsement by the U.S. Army of this website or the information, products, or services contained therein. For other than authorized activities such as military exchanges and MWR sites, the U.S. Army does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this website."

**Figure 5–1. External links disclaimer**

*c. Links to private Army internet services.* Links or references to private Army internet services will not be placed on public Army internet services or IbC; however, under certain circumstances it may be appropriate to establish a link to a log-on page, provided that details about the contents are not revealed.

*d. Site registration.* The internet addresses and contact information for all public Army internet services, EOP, and other official uses of IbC will be registered in the registration system(s) hosted by the Office of the Assistant Secretary of Defense, Public Affairs on https://www.defense.gov/.

*e. General provisions.* Longstanding guidance on personal communication ethics and the handling and dissemination of Army information continues to apply when using IbC. Policies and laws related to the protection, control, and release of Army information, such as OPSEC, information security, and PII apply.

(1) Nonpublic or sensitive information will not be collected, disseminated, stored, or otherwise processed via IbC unless directed to do so in statute, regulation, or Executive Order. IbC are not subject to federal or Army IA standards, controls, or enforcement, and therefore may not consistently provide the protections necessary to prevent disclosure to inappropriate or unintended audiences.

(2) Authorized users are prohibited from installing unapproved SW or applications on Army-furnished equipment. Additionally, some IbC may offer mobile code that is prohibited from being executed on Army furnished equipment in accordance with Public Law 107–198 or third-party applications not covered by the signed Army terms of service (TOS) with the IbC. Such offers should not be used or installed without approval. Third-party applications include, but are not limited to, games, hobbies, photography tools, or mobile code as categorized in DODI 8500.01.

(3) DOD policy prohibits authorized users from using, installing, or configuring peer-to-peer file-sharing applications, unless these actions are approved for mission enhancing functions consistent with DODI 8500.01.

*f. Personal use.* Army employees are not prohibited from establishing IbC accounts for personal use; however, the following provisions apply:

(1) *Contractual obligation or agreements.* Personal accounts with IbC are not covered by TOS agreements implemented by Army. The Army will not be a party to, nor in any way responsible for, individual obligations or agreements established with IbC for personal use.

(2) *Contact information.* Use nonmission–Related contact information, such as personal telephone numbers or postal and email addresses, to establish personal accounts, when such information is required.

(3) *Communication and standards of conduct.*

*(a)* Barring absence of official communication channels, personal accounts will not be used to conduct official Army communication. Personal accounts may be used to participate in activities such as professional networking, development, and collaboration related to, but not directly associated with, official mission activities as an Army employee or Army contractor.

*(b)* Personal communication will be conducted in compliance with DOD 5500.7–R. The dissemination and discussion of nonpublic information will be avoided and opinions will be disclaimed as necessary in accordance with DOD 5500.7–R. Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, will not be disclosed.

(4) *Compliance.* When use of Army systems for authorized purposes is allowed by the DOD and OSD component heads or designees, such communication will be conducted in compliance with DOD 5500.7–R.

*g. Official use.* In addition to approving the establishment of EOP and official use of IbC and consistent with DOD 5500.7–R, the DOD and OSD component heads may approve the establishment of IbC accounts by authorized users for public communication related to assigned duties, such as recruiting, or any other purpose determined necessary in the interest of the Federal Government. The following provisions apply to official use:

(1) DOD and OSD component heads and official-use account users must be prepared to account fully for exercising sound judgment within the authority and scope of official activities.

(2) Liaison will be conducted with public affairs and OPSEC staff to ensure organizational awareness of their authorized, mission–Related public communication and responsibilities.

(3) Written requests (letters or emails) will be submitted to IbC providers to block the display of any commercial advertisements, solicitations, or links on EOP and IbC pages administered with official-use accounts if the IbC provider would otherwise normally display such materials.

*(a)* Establishing an official presence on, or use of, an IbC may require acceptance of a TOS agreement. The "standard" TOS used by the IbC provider may contain legally objectionable terms and conditions, which must be amended or otherwise addressed for Army use. Additionally, IbC providers may agree only to such amended terms and conditions for limited portions of their products and services.

*(b)* Army employees and Army contractors who establish an EOP or other official uses on an IbC will verify whether a TOS for that IbC has been signed and approved by the DOD CIO. Such TOS apply to DOD-wide use and operation of EOP and other official uses. In this case, there is no need for additional TOS at the component level. Signed and approved TOS are listed at http://www.defense.gov/socialmedia/terms-of-service.aspx.

*(c)* If a TOS agreement for an IbC has not been signed by the DOD CIO, establish, in coordination with the DOD CIO, a TOS agreement signed at either the DOD CIO or the DOD component level. The GSA provides TOS templates appropriate for Federal Government use at https://www.apps.gov/ that will be adapted for DOD use if available for the desired IbC. Initiate coordination with the DOD CIO via digitally-signed email to tos-application@osd.mil.

Coordination with the DOD CIO will include determination of appropriate coordination with Commander, U.S. Strategic Command and with component or DOD General Counsel.

*h. Communication.* Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, will not be disclosed.

(1) Official-use accounts will not be used to conduct communication not related to assigned duties, functions, or activities.

(2) IbC will be used as supplemental communication or distribution channels for Army information. Do not establish or represent official-use accounts or pages as primary sources of Army information.

(3) A clear description of the purpose for using the IbC and that Army is the content provider will be posted where possible.

(4) Links to official Army content hosted on Army-owned, Army-operated, or Army-controlled sites will be posted, where applicable and possible, when official use of an IbC references materials originating from an official Army website.

(5) Links will be posted to the organization's official public website.

(6) Specific steps to protect individual privacy whenever third-party websites and applications are used to engage with the public will be implemented in compliance with OMB Memorandum M–10–23.

*i. Disclaimers.*

(1) "For official information from or about the U.S. Department of Defense/(insert name of organization), please visit (insert home page or other official information source) at (insert address)" will be placed in a prominent location on each authorized page as workable.

(2) If the IbC provider is unwilling or unable to block the display of commercial advertisements, the following message will be placed in a prominent location on each authorized page as workable: "The appearance of commercial advertising and hyperlinks inserted by the host of this service does not constitute endorsement by the U.S. Department of Defense/(insert name of organization)."

### 5–14. Public Army internet service on an unclassified network

*a. Domains.* Internet domain names established and approved in compliance with DODI 8410.01 will be used for all Army internet services. The .mil internet domain is established for the exclusive use of the DOD and should be the primary address for Army internet services.

*b. Federal internet services.* Army collection, dissemination, storage, and other processing of information on federally owned, operated, or controlled internet services (for example, Intellipedia, Data.gov) are subject to the same policies and procedures as when such activities are conducted on Army internet services.

*c. Cybersecurity.* The confidentiality, integrity, availability, non–Repudiation, and authenticity of Army information will be ensured through compliance with DODI 8510.01. Army ISs hosting public or private Army internet services must be assessed and authorized. Security and management controls must be in place to:

(1) Prevent inappropriate disclosure of sensitive and other nonpublic information.

(2) Ensure public and nonpublic information are resistant to tampering.

(3) Provide availability to the information or service as intended by the Army component and expected by customers.

*(a)* An approved, legally sufficient notice and consent banner, in accordance with the RMF or appropriate STIG and DODI 8510.01 and available at http://iase.disa.mil/ will be displayed on private Army internet services.

*(b)* Private Army internet services will be public key enabled in accordance with DODI 8520.02.

*(c)* A comprehensive, in-depth IA strategy for the security of web operations will be implemented in alignment with the current version of DISA's web server STIG.

*d. Advertising and endorsement.* For the purpose of advertising, public Army internet services are government publications. In accordance with DOD 5500.07–R, U.S. Congress Senate Publication 101–9, and DODD 5500.07, the credibility of Army information must not be adversely affected by association with nongovernment sponsorships, advertisements, or endorsements.

(1) Any advertisement by or for any private individual, firm, or corporation will not be inserted or allowed on public Army internet services prepared or produced with either appropriated or NAFs. Army endorsement will not be implied in any manner for any specific nongovernment service, facility, event, or product.

(2) Stand-alone nongovernment graphics, logos, or aggrandizing statements such as "Powered by," "Serviced by," and "Designed by" will not be inserted or allowed on public Army internet services, or the Army-controlled content area of an IbC prepared or produced with either appropriated or NAFs. Proprietary rights notices (including copyright and trademark notices) are not aggrandizing statements. Copyright notices are required as described in DODD 5535.4 and DODI 5120.04. Factual acknowledgment of partners, SW, technology, and services used on a public Army internet

service may be included in descriptive information about the service or the organization, such as an "About Us" page. However, such acknowledgment should be carefully considered in the security risk assessment and risk mitigation measures for the service and may not be used in any manner that supports the appearance of endorsement. Factual acknowledgment may include a corresponding nongovernment graphic, logo, or trademark. This graphic, logo, or trademark may be used as a hyperlink to the corresponding nongovernment website or service; however, the link must be disclaimed as described in paragraph 5–14*e* of this pamphlet.

(3) Users will not be required or encouraged to choose any specific brand of browser SW or other client applications to access public Army internet services and IbC. Army websites must be designed in accordance with accepted standards of the World Wide Web Consortium to ensure browser compatibility (see http://www.w3.org/standards/).

(4) Remuneration of any kind (for example, payment, reimbursement, reduced prices, gifts, and so on) will not be accepted in exchange for advertising, acknowledgment, or endorsement without specific statutory authority to do so. Accepting remuneration may constitute an improper augmentation of appropriations in violation of 31 USC Chapter 13 and 31 USC Chapter 15.

(5) Nongovernment advertising in electronic versions of MWR products is governed by DODI 1015.10, Enclosure 12. Such advertising must only be displayed via private Army internet services that ensure distribution is limited to authorized customers. Advertising in electronic versions of Army newspapers, magazines, and civilian enterprise publications is governed by DODI 5120.04.

*e. Links to private Army internet services.* Links or references to private Army internet services will not be placed on public Army internet services or IbC; however, under certain circumstances it may be appropriate to establish a link to a log-on page, provided that details about the contents are not revealed.

*f. Registration.* The internet addresses and contact information for all public Army internet services, EOP, and other official uses of IbC will be registered in the registration system(s) hosted by the Office of the Assistant Secretary of Defense, Public Affairs at https://www.defense.gov/.

*g. Authority, mission, and organization.* A description of the DOD or the DOD component's organizational structure, mission, and statutory authority will be linked from major entry points (including home pages) on the DOD federal agency public website (http://www.defense.gov/) and the principal, public websites of the DOD components consistent with OMB Memorandum M–05–04.

*h. Contact information.* Contact information will be linked from all major entry points on the Army Component's principal public websites consistent with OMB Memorandum M–05–04. Consolidating this information on a single "Contact Us" page is recommended. Contact information must contain:

(1) Organization's postal address.

(2) Street addresses for any regional or local offices that have a function requiring interaction with the public.

(3) Office telephone number(s), including numbers for any regional or local offices or toll-free numbers and telecommunications device for the deaf (TDD) numbers, if available. If TDD lines are not available, use appropriate relay such as the Federal Relay Service as needed.

(4) Means to communicate by electronic mail (for example, email addresses, group mailbox).

(5) The policy, procedures, and time for responding to email inquiries.

(6) Contact information to report data problems as required in the Deputy Secretary of Defense Memorandum dated February 10, 2003 available at http://www.doncio.navy.mil/uploads/1219dxy35343.pdf.

(7) How to request information through 5 USC 552 pursuant to DODD 5400.07 and DOD 5400.7–R, and a link to information made available specifically under FOIA. (DOD FOIA guidance is posted on the DOD federal agency public website.)

(8) Contact information for or link to the DOD or the DOD component's office that promotes small business participation in defense acquisition pursuant to OMB Memorandum M–05–04 and Public Law 107–198.

(9) Contact information to report both technical and information problems regarding the website specifically, including accessibility problems.

(10) A PAS or Privacy Advisory, as appropriate for the method of contact, in accordance with DOD 5400.11–R and DODD 5400.11.

*i. No Fear Act data.* A link specifically labeled "No Fear Act Data" will be placed on home pages of the DOD federal agency public website and the principal public websites of the DOD components. This specific label must link to summary statistical data about equal employment opportunity complaints filed with DOD or with the DOD components, as applicable, and written notification of whistleblower rights and protections pursuant to OMB Memorandum M–05–04 and Public Law 107–174 (known as the No Fear Act).

*j. Privacy policy.* Clear privacy policies will be posted or linked to on public Army internet services in compliance with OMB Memorandums M–05–04 and M–07–16 at major entry points and at those points or pages where personal

information is collected from the public. Use the specific label “Privacy Policy.” The privacy and security notice provided in figure 5–2 may be tailored as shown in the example.

PRIVACY AND SECURITY NOTICE

1. [Name of service (e.g., "Website Title")] is provided as a public service by [name of the Army Component(s)].

2. Information presented on this service not identified as protected by copyright is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.

3. For site management, information is collected [Link "information is collected" to description of specific information. An example is provided after paragraph 8. in this figure] for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond Army websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines. [Agencies subject to DODD 5240.01 shall add the following sentence to this paragraph: "All data collection activities are in strict accordance with DOD Directive 5240.01."]

6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department websites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or agencies. The Department of Defense does not keep a database of information obtained from the use of WMCT. [If the DOD CIO has provided explicit written approval to use Tier III WMCT, cite that approval here.] General instructions for how you may opt out of some of the most commonly used WMCT is available at http://www.usa.gov/optout_instructions.shtml.

7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act (18 U.S.C. § 1030).

8. If you have any questions or comments about the information presented here, please forward them to [contact information to report both technical and information problems with the website specifically, including accessibility problems].

EXAMPLE

Information Collected from [Name of site or "This website"] for Statistical Purposes
xxx.yyy.com -- [28/Jan/2008:00:00:01 -0500] "GET /Defense/news/nr012708.html HTTP/1.0" 200 16704 Mozilla 3.0/www.google.com

**Figure 5–2. Privacy and security notice**

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or Internet protocol (IP) address) associated with the requester (you as the visitor). In this case, the requester is coming from the xxx.yyy.net address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify the user's specific computer. Connections via many Internet Service Providers (ISP) assign different IP addresses for each session, or only connect to the Internet via proxy servers, so the host name may only identify the ISP. The host name (or IP address) may identify a specific computer if that computer has a fixed IP address.

[28/Jan/2008:00:00:01 -0500] -- this is the date and time of the request

"GET /Defense/news/nr012708.html HTTP/1.0" -- this is the location of the requested file

200 -- this is the status code - 200 is OK - the request was filled

16704 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

www.google.com -- this indicates the last site the person visited, which indicates how people find the requested file.

Requests for other types of documents use similar information. Unless otherwise stated, no personally-identifiable information is collected.

**Figure 5–2. Privacy and security notice—Continued**

*k. Privacy format.* Provide privacy policies in a standard machine–Readable format on public websites in addition to the human–Readable text version. Specific guidance is provided in Section IV of OMB Memorandum M–17–06.

## 5–15. Private Army internet services process

This section provides guidance for Army organizations in the establishment, operation, and/or maintenance of a private Army internet service on an unclassified network to collect, disseminate, store, and otherwise process nonpublic information to specific audiences.

*a. Domains.* Internet domain names established and approved in compliance with DODI 8410.01 will be used for all Army internet services. The .mil internet domain is established for the exclusive use of the DOD and should be the primary address for Army internet services.

*b. Federal internet services.* Army collection, dissemination, storage, and other processing of information on federally owned, operated, or controlled internet services (for example, Intellipedia, Data.gov) are subject to the same policies and procedures as when such activities are conducted on Army internet services.

## 5–16. 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 MWR provided NAF communications services.

*b.* DOD members assigned to a CONUS installation, ACOM, ASCC, DRU, 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 when approved by the commander (see CJCSI 6211.02D).

(4) USG 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. USG cannot pay toll charges for extending personal calls. The SBU voice directory at 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:

(1) Family Readiness Group accounts established for each deployed unit and its rear detachment.

(2) Commercial internet email account that the DOD member establishes for personal use at no cost to USG.

(3) Unclassified official email accounts.

*(a)* 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.

*(b)* 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 SW is loaded onto the government system, and USG 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.

*(c)* 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.

### 5–17. Network Enterprise Center website administration

*a. Network Enterprise Center functions.* NECs are required to comply with Section 508 provisions to make information on websites accessible to employees and the public. See federal accessibility standards at http://www.section508.gov for the latest information. At a minimum, these include:

(1) A text equivalent for every nontext element will be provided (for example, via “alt” (alternative text attribute), “longdesk” (long description tag), or in element content).

(2) Web pages designed so that all information conveyed with color is also available without color; for example, from context or markup.

(3) Pages designed to avoid causing the screen to flicker with a frequency greater than 2 hertz and lower than 55 hertz.

(4) Documents organized so they are readable without requiring an associated style sheet.

(5) Web pages updated for equivalents for dynamic content whenever the dynamic content changes.

(6) Redundant text links instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(7) Client-side image maps whenever possible in place of server-side image maps.

(8) Row and column headers identified for data tables.

(9) Markup to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(10) Frames titled with text that facilitates frame identification and navigation.

(11) 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.

(12) A text-only page, with equivalent information of functionality, to make a website 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.

(13) A method that permits users to skip repetitive navigation links.

(14) 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.

(15) When electronic documents are meant to be completed online, guidance to allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the document, including all directions and cues.

(16) When a timed response is required, the user will be alerted and given sufficient time to indicate more time is required.

*b. Army web risk assessment cell.* The AWRAC reviews the content of Army publicly accessible websites (.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 websites to identify security concerns or review website concerns provided by the Joint Web Risk Assessment Cell or Army leadership.

(2) Ensures inappropriate security and personal information is removed from publicly accessible websites.

(3) Ensures that Army sites are compliant with other federal, DOD, and Army website administration policies (for example, Government Information Locator Service registration).

(4) Notifies the website owner with operational authority and the program information system security managers of respective command and/or activity of violations and suspense dates for reporting corrective action.

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

*c. System security considerations.*

(1) Each organization will establish information system security certification and accreditation procedures in accordance with DODI 8510.01, DOD 8570.01–M, 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 website operation and maintenance at all times. It is essential that web server environments be implemented and maintained by personnel trained and certified in accordance with DODI 8510.01, DODD 8140.01, DOD 8570.01–M and AR 25–2. Day-to-day maintenance of the HW and SW, including security patches and configurations, is essential to the system security of web server environments. See also NIST Special Publication 800–44.

(3) A formal risk assessment should be conducted at each organization operating a website 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 800–30.

(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 SW will be compliant with 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 website. Examples of additional measures to be considered include:

*(a)* Disabling internet protocol 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 website 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. Identification and password protection. The internet is an unsecured network where compromise of user identification and password can occur during open transmission. Identifications 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).

## 5–18. Collaboration capabilities

*a.* Collaboration capabilities are necessary to enable two or more individuals who are not co-located to use an electronic 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 AEN, local enclaves, or domain level apply to Regular Army, ARNG, USAR, Army Civilians and applicable Army support contractors, and those organizations operating under contract to the Army.

*b.* The collaboration procedure includes:

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

(2) CIO/G–6 (SAIS–NSE) reviews the requirements and determines if the requirements are met by DOD enterprise services capabilities, AKO, or an existing product on the UC 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 that are not on the UC APL are required to follow the guidance set forth in the RMF Implementation Program (see AR 25–2). They are also required to ensure that the product has been assessed and authorized.

*(a)* The RMF Implementation Program is managed by CIO/G–6 (see AR 25–2).

*(b)* An authorized (ATO/interim authority to test) and/or approved (assess only) by the AO is required before the process can be finalized. Army commands are required to obtain authorization and/or approval per DODI 8500.01, DODI 8510.01, and AR 25–2.

(4) Following approval:

*(a)* The collaboration tool or service is linked to AKO through EAMS–A. EAMS–A 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 authentication using EAMS–A, including forms and technical platform requirements, are available on AKO. Linking to AKO through EAMS–A 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 single sign-on, a waiver, to include a migration plan, must be obtained from CIO/G–6 (SAIS–NSE).

*(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.

## 5–19. Army Centralized Army Service Request System

*a.* The Army Centralized Army Service Request System (ACAS) provides an automated method for enabling units to submit certain satellite access requests (SARs) and to request DISN services (for example, phone numbers, internet protocol addresses for SIPRNET and NIPRNET, and so on). This system is a custom-built website 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 (SATCOM) support centers will use the Joint Integrated Satellite Communications Technology (JIST), https://jist-jsme.disa.smil.mil/jist/pages/framedef.jsp, for SAR and Gateway Access Request input. Army will use ACAS for capabilities not included in JIST. ARCYBER 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 Warfighter Information Network–Tactical 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 will 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 SATCOM bandwidth authorization and connections to the Network Service Center–Training and RHNs. To generate an SAR or ASR, visit the ACAS website at https://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) Log-on 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.

## Section III

## Privacy Impact Assessments/Electromagnetic Spectrum Operations

### 5–20. Privacy impact assessment process

*a.* A PIA is an analysis of how PII is handled in electronic form by information system/electronic collection (ISEC). An ISEC collects, uses, and/or disseminates PII about members of the public, DOD personnel (government civilians, members of the military, and NAF employees), contractors, or foreign nationals employed at U.S. military facilities. A PIA:

(1) Determines the risks and effects of ISEC collecting, maintaining, and disseminating information in identifiable electronic form.

(2) Examines and evaluates protection and alternative processes for handling information to mitigate potential privacy risks.

(3) Ensures conformance to applicable legal, regulatory, and policy requirements regarding privacy.

(4) Addresses who has or will have access to PII in the IT system and/or application or electronic collection and the purpose and use of the information.

(5) Addresses how the PII information will be collected and secured (for example, paper format, facsimile, and email).

(6) Outlines what measures have been put into place or planned to address identified privacy risks.

(7) Will be submitted using DD Form 2930.

(8) Must go through the local command privacy official and PIA (POC).

(9) Will be displayed on the CIO/G–6 website http://ciog6.army.mil/privacyimpactassessments/tabid/71/default.aspx when the ISEC collects PII from members of the general public and federal personnel and/or contractors.

(10) Is not required when the ISEC has been designated an NSS, to include systems that process classified information. 44 USC 3543 states that the head of each agency operating or exercising control of an NSS will be responsible for ensuring that the agency:

*(a)* Provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system.

*(b)* Implements information security policies and practices, as required by standards and guidelines for NSS, issued in accordance with law and as directed by the President and complies with the requirements of 44 USC 4543.

(11) Must be completed in its entirety in accordance with the policy and guidance outlined in AR 25–1 and this pamphlet when ISEC contains PII.

(12) Requires specific sections to be completed if ISEC does not collect, maintain, or disseminate PII. The ISEC owner needs to complete Blocks 1 and 2; Sections 1a, 1b, 3a, 3b; and the signature block at Section 4a of DD Form 2930, with copy of a valid ATO or ARCYBER Certificate of Networthiness (CoN) registration number that is registered in the ARCYBER tracking system.

(13) Must be reviewed and updated as follows:

*(a)* When there are significant system management changes, for example:

1. Significant merging.
2. New public access and/or interagency uses.
3. Commercial sources.

4. Alternation in character or data.

5. Changes in the privacy or security posture.

*(b)* In conjunction with the ISEC assessment and authorization cycle.

*(c)* Within 3 years of PIA approval date in accordance with Public Law 113–283 (known as the Federal Information Security Modernization Act) requirements.

*b.* If an ISEC has the ability to retrieve an individual's name, date of birth, SSN, and contains a personal identifier of an individual, the PIA will require a SORN.

(1) A SORN is a group of records (paper or electronic) from which PII is retrieved using the name of the individual or some other identifying number, symbol, or particular that is unique to the individual. The SORN notifies the general public what personal data is being collected, the purpose of the collection, and the authority for doing so. It also sets the rules to follow in collecting and maintaining the personal data.

(2) The Office of the Administrative Assistant to the Secretary of the Army will review PIA ISECs, confirm compliance with DODD 5400.11, and ensure SORN issues have been properly identified, evaluated, and approved prior to CIO/G–6 approval.

(3) If an ISEC collects information on 10 or more members 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.

*c.* PIAs for Army Medical Command (MEDCOM) ISEC are processed according to their funding source. The ISECs purchased with Defense Health Program funds must follow the Army MEDCOM PIA procedures. Army MEDCOM ISECs purchased with Army funds will follow CIO/G–6 PIA policies and procedures of AR 25–1 and this pamphlet.

*d.* Tenants must identify all PII (personal, financial, medical, military, and so on) residing on NEC's systems and service provider systems, networks and SANs, and stand-alone systems by completing a DD Form 2930 submitted as part of the Tenant Security Plan.

*e.* Army system owners and application owners will—

(1) Conduct an assessment of all IS 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, with the exception of exemptions listed in paragraph 5–20*a*(10).

(2) Document completion of the assessment using the digital signature portable document format (PDF) version of DD Form 2930.

(3) Refer to the Army Publishing Directorate website https://armypubs.army.mil/ for the latest DD Form 2930 template which provides instruction for completing this form.

*f.* APMS is used for compliance reporting, for privacy and PIAs, CCA, and PKI requirements. The ISEC must be registered in the APMS with its own AITR number or be a registered child to a parent ISEC in APMS prior to operation. ISEC need not be separately registered in APMS if the ISEC is an embedded technology component of the APMS parent system.

(1) An AITR and/or DITPR number will be assigned once the system and/or application is registered.

(2) Once an IT system and/or application is registered in APMS, a DD Form 2930 is required.

(3) Complete PIA data fields in APMS, as required, based on the completed assessment.

*g.* Submit completed DD Form 2930s to their command PIA point of contact. The DD Form 2930 must have the first four local digital signatures (military and government civilian only, no contractors) one of which must be the local privacy point of contact.

(1) The command PIA POC will submit the form and attachments to the PIA team collaboration hub at https://army.deps.mil/army/cmds/hqda_ciog6_admin/patch/sitepages/patch.aspx.

(2) The CIO/G–6 PIA team will only accept complete signed packages containing original forms with a copy of the valid ATO or CoN registration number.

(3) The CIO/G–6 PIA team will perform an 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.

(4) The Army Cybersecurity Senior Information Security Officer (CIO/G–6 (SAIS–CB)) will review DD Form 2930s to ensure compliance with policies prior to CIO/G–6 approval. Once approved, the CIO/G–6 PIA team will post all completed PIAs which collect PII from the general public and/or both the general public and federal employees or contractors on the CIO/G–6 website at https://www.rmda.belvoir.army.mil/privacy/docs/da_pia_guide_final_2017.pdf.

## 5–21. Electromagnetic spectrum operations

*a.* AR 5–12 governs Armywide spectrum management. The United States and its possessions-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 pamphlet. 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 (see 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 the United States and its possessions, government policy requires Army users to revalidate each permanent frequency assignment to delete or modify the record, normally every 5 years. OCONUS, Army records require a similar review under ACP 190(D) or per combatant command directives.

(4) Clearance for electronic attack operations (see AR 5–12).

(5) Radio station identification, international call signs, and other non-tactical call signs (see AR 5–12).

(6) Coordination with other installation directorates and tenant activities concerning spectrum-dependent equipment (see AR 5–12).

(7) Assistance in resolving incidents of harmful radio interference (see AR 5–12).

(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.

# Appendix A

# References

## Section I

### Required Publications

The following publications are available on the Army Publishing Directorate website (https://armypubs.army.mil/) unless otherwise stated.

**AR 25–1**
Army Information Technology (Cited on title page.)

**AR 25–2**
Army Cybersecurity (Cited in para 1–4.)

**AR 70–1**
Army Acquisition Policy (Cited in para 1–4.)

**AR 71–9**
Warfighting Capabilities Determination (Cited in para 2–18*i*.)

**Federal Chief Information Officer Memorandum**
Data Center Optimization Initiative dated August 1, 2016 (Available at https://policy.cio.gov/dcoi/.) (Cited in para 5–3*a*.)

## Section II

### Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (https://armypubs.army.mil/). DOD publications are available on the Office of the Secretary of Defense website (http://www.esd.whs.mil/dd/). USC, CFR, and Public Law materials are available at https://www.gpo.gov/fdsys/.

**ACP 190(D)**
Guide to Electromagnetic Spectrum Management in Military Operations (Available at http://navybmr.com/study%20material/acp190dfeb13.pdf.)

**ADRP 6–0**
Mission Command

**AR 5–12**
Army Use of the Electromagnetic Spectrum

**AR 25–13**
Army Telecommunications and Unified Capabilities

**AR 25–22**
The Army Privacy Program

**AR 25–30**
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 25–59**
Office Symbols

**AR 25–400–2**
The Army Records Information Management System (ARIMS)

**AR 27–60**
Intellectual Property

**AR 215–4**
Nonappropriated Fund Contracting

**AR 335–15**
Management Information Control System

**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 420–1**
Army Facilities Management

**AR 500–3**
U.S. Army Continuity of Operations Program Policy and Planning

**AR 700–142**
Type Classification, Materiel Release, Fielding, and Transfer

**Army Directive 2016–38**
Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers

**Army Network Campaign Plan 2020 and Beyond**
(Available at https://army.deps.mil/army/cmds/hqda_ciog6/pages/ciog6-excomm.aspx.)

**CJCSI 3156.01A**
Management of Joint Unit Reference Numbers (Available at http://www.jcs.mil/library/.)

**CJCSI 3170.01I**
Joint Capabilities Integration and Development System (Available at http://www.jcs.mil/library/.)

**CJCSI 6211.02D**
Defense Information System Network (DISN) Responsibilities (Available at http://www.jcs.mil/library/.)

**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/order/sitepages/home.aspx.)

**CTA 50–909**
Field and Garrison Furnishings and Equipment

**DA Pam 25–40**
Army Publishing Program Procedures

**DA Pam 25–91**
Visual Information Procedures

**DA Pam 70–3**
Army Acquisition Procedures

**DA Pam 420–11**
Project Definition and Work Classification

**Defense Federal Acquisition Regulation Supplement**
(Available at www.acq.osd.mil.)

**Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG)**
(Available at https://iase.disa.mil/cloud_security/cloudsrg/pages/home.aspx.)

**Department of Defense Joint Technical Architecture, Version 6.0**
(Available at http://dtic.mil/dtic/.)

**Department of Defense Strategy for Operations in the Information Environment**
(Available from https://www.defense.gov/portals/1/documents/pubs/dod-strategy-for-operations-in-the-ie-signed-20160613.pdf.)

**DFAS–IN Manual 37–100**
The Army Management Structure for Fiscal Year __ (Available at https://dfas4dod.dfas.mil/library/.)

**DFAS–IN 37–1 Regulation**
Finance and Accounting (Available at https://dfas4dod.dfas.mil/library/.)

**DISA Circular 310–D70–30**
Global Information Grid (DISN) National Gateway Center (NGC) and Subscriber Operations (Available at https://www.disa.mil/about/disa-issuances/circulars.)

**DISA Circular 310–130–1**
Submission of Telecommunications Service Requests (Available at https://www.disa.mil/about/disa-issuances/circulars.)

**DOD Dictionary of Military and Associated Terms**
(Available at http://www.jcs.mil/doctrine/dod-terminology/.)

**DOD Net–Centric Data Strategy**
Memorandum, Chief Information Officer, May 9 2003 (Available from http://dodcio.defense.gov/.)

**DOD 5220.22–M**
National Industrial Security Program Operating Manual

**DOD 5400.11–R**
Department of Defense Privacy Program

**DOD 5500.07–R**
Joint Ethics Regulation (JER)

**DOD 8570.01–M**
Information Assurance Workforce Improvement Program

**DODD 3020.26**
DOD Continuity Policy

**DODD 3600.01**
Information Operations (IO)

**DODD 5000.01**
The Defense Acquisition System

**DODD 5144.02**
DOD Chief Information Officer (DOD CIO)

**DODD 5210.50**
Management of Serious Security Incidents Involving Classified Information

**DODD 5240.01**
DOD Intelligence Activities

**DODD 5400.11**
DOD Privacy Program

**DODD 5500.07**
Standards of Conduct

**DODD 5535.4**
Copyrighted Sound and Video Recordings

**DODD 8115.01**
Information Technology Portfolio Management

**DODD 8140.01**
Cyberspace Workforce Management

**DODI 1000.30**
Reduction of Social Security Numbers (SSN) Use Within DOD

**DODI 1015.10**
Military Morale, Welfare, and Recreation (MWR) Programs

**DODI 1015.12**
Lodging Program Resource Management

**DODI 1035.01**
Telework Policy

**DODI 4000.19**
Support Agreements

**DODI 4165.14**
Real Property Inventory (RPI) and Forecasting

**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 5000.74**
Defense Acquisition of Services

**DODI 5000.75**
Business Systems Requirements and Acquisition

**DODI 5120.04**
DOD Newspapers, Magazines, Guides, and Installation Maps

**DODI 5220.22**
National Industrial Control Security Program (NISP)

**DODI 5400.13**
Public Affairs (PA) Operations

**DODI 8100.04**
DOD Unified Capabilities (UC)

**DODI 8115.02**
Information Technology Portfolio Management Implementation

**DODI 8260.03**
The Global Force Management Data Initiative (GFM DI)

**DODI 8320.02**
Sharing Data, Information, and Technology (IT) Services in the Department of Defense

**DODI 8320.04**
Item Unique Identification (IUID) Standards for Tangible Personal Property

**DODI 8320.06**
Organization Unique Identification (OUID) Standards for Unique Identification of External Department of Defense Business Partners

**DODI 8320.07**
Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense

**DODI 8330.01**
Interoperability of Information Technology (IT), Including National Security Systems (NSS)

**DODI 8410.01**
Internet Domain Name and Internet Protocol Address Space Use and Approval

**DODI 8410.03**
Network Management (NM)

**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

**DODI 8530.01**
Cybersecurity Activities Support to DOD Information Network Operations

**DODI 8550.01**
DOD Internet Services and Internet-Based Capabilities

**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

**DODM 8260.03 Volume 1**
Global Force Management Data Initiative (GFM DI) Implementation: Unique Identification (UID) for GFM

**DODM 8260.03 Volume 2**
Global Force Management Data Initiative (GFM DI) Implementation: The Organizational and Force Structure Construct (OFSC)

**DODM 8400.01**
Accessibility of Information and Communications Technology (ICT)

**DTR 4500.9–R**
Defense Transportation Regulations (Available at https://www.ustranscom.mil/dtr/index.cfm.)

**Executive Order 12333**
United States Intelligence Activities (Available at https://www.archives.gov/.)

**Executive Order 13693**
Federal Leadership on Climate Change and Environmental Sustainability (Available at https://obamawhitehouse.archives.gov/.)

**FAR 8.404**
Use of Federal Supply Schedules (Available at https://www.acquisition.gov/far/.)

**Federal Telecommunications Recommendation 1080B–2002**
Video Teleconferencing Services (Available at https://www.hsdl.org/?view&did=440852.)

**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 log-on required).)

**HQDA EXORD 155–17**
Institutional Network Modernization FY17/18 dated 20 April 2017 (Available at https://army.deps.mil/army/cmds/hqda_ciog6/sitepages/home.aspx).

**IEEE/EIA 12207: 2008**
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 Avenue, Building 4, Philadelphia, PA 19111–5094.)

**IEEE 802**
LAN/MAN Standards Committee (Available at no cost to DOD personnel; contact Defense Automation and Production Service, 700 Robbins Avenue, Building 4, Philadelphia, PA 19111–5094.)

**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 Avenue, Building 4, Philadelphia, PA 19111–5094.)

**NIST Special Publication 800–30**
Guide for Conducting Risk Assessments (Available at http://csrc.nist.gov/publications/pubssps.html.)

**NIST Special Publication 800–44**
Guidelines on Securing Public Web Servers (Available at http://csrc.nist.gov/publications/pubssps.html.)

**NIST Special Publication 800–82**
Guide to Industrial Control Systems (ICS) Security (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 https://www.whitehouse.gov/omb/circulars/.)

**OMB Circular A–130**
Management of Federal Information as a Strategic Resource (Available at https://www.whitehouse.gov/omb/circulars/.)

**OMB Memorandum M–03–22**
Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Available at https://www.whitehouse.gov/omb/memoranda/.)

**OMB Memorandum M–05–04**
Policies for Federal Agency Public Websites (Available at https://www.whitehouse.gov/omb/memoranda/.)

**OMB Memorandum M–07–16**
Safeguarding Against and Responding to the Breach of Personal Identifiable Information 2002 (Available at https://www.whitehouse.gov/omb/memoranda/.)

**OMB Memorandum M–10–22**
Guidance for Online Use of Web Measurement and Customization Technologies (Available at: https://www.whitehouse.gov/omb/memoranda/.)

**OMB Memorandum M–10–23**
Guidance for Agency Use of Third-Party Websites and Applications

**OMB Memorandum M–17–06**
Policies for Federal Agency Public Websites and Digital Services (Available at: https://www.whitehouse.gov/omb/memoranda/.)

**OMB Memorandum M–17–12**
Preparing for and Responding to a Breach of Personally Identifiable Information (Available at: https://www.whitehouse.gov/omb/memoranda/.)

**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 104–208**
Federal Financial Management Improvement Act of 1996

**Public Law 106–398**
National Defense Authorization, Fiscal Year 2001

**Public Law 107–174**
Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No Fear Act)

**Public Law 107–198**
Small Business Paperwork Relief Act of 2002

**Public Law 108–375**
National Defense Authorization Act for Fiscal Year 2005

**Public Law 112–81**
National Defense Authorization Act for Fiscal Year 2012

**Public Law 113–283**
Federal Information Security Modernization Act of 2014 (FISMA)

**TRADOC Pamphlet 525–3–1**
The U.S. Army Operating Concept, Win in a Complex World, 2020–2040 dated 31 October 2014 (Available at http://adminpubs.tradoc.army.mil/.)

**U.S. Congress Senate Publication 101–9**
Government Printing and Binding Regulations

**Unified Capabilities Requirement 2008, Change 3**
(Available at http://www.disa.mil/services/network-services/ucco.)

**16 CFR 312**
Children's Online Privacy Protection Rule

**36 CFR Chapter XII**
National Archives and Records Administration

**36 CFR 1194**
Electronic and information technology accessibility standards

**5 USC 552**
Public information; agency rules, opinions, orders, records, and proceedings (Freedom of Information Act)

**5 USC 552a**
Records maintained on individuals (The Privacy Act of 1974)

**5 USC 8101 et seq.**
The Federal Employees' Compensation Act

**10 USC**
Armed Forces

**10 USC 2223**
Information technology: additional responsibilities of Chief Information Officers

**28 USC 1346**
United States as defendant (Federal Tort Claims Act)

**29 USC 794d**
Electronic and information technology (known as Section 508 of the Rehabilitation Act of 1973, as amended)

**31 USC Chapter 13**
Appropriations

**31 USC Chapter 15**
Appropriation Accounting

**31 USC 3721**
Claims of personnel of agencies and the District of Columbia government for personal property (Military Personnel and Civilian Employees Claims Act)

**40 USC Subtitle III**
Information Technology Management (Clinger-Cohen Act)

**40 USC 11103**
Applicability to national security systems

**44 USC**
Public Printing and Documents

**44 USC Chapter 35**
Coordination of Federal Information Policy (Paperwork Reduction Act)

**44 USC Chapter 36**
E-Government Act of 2002 (E-Government)

**44 USC 3502**
Definitions

**44 USC 3504**
Authority and functions of Director (Government Paperwork Elimination Act)

**44 USC 3543**
Authority and functions of the Director

**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 website (https://armypubs.army.mil/), DD forms are available on the OSD website (http://www.esd.whs.mil/directives/forms/), and SF forms are available on the General Services Administration website (https://www.gsa.gov/reference/forms).

**DA Form 2028**
Recommended Changes to Publications and Blank Forms

**DA Form 3161**
Request for Issue or Turn-In

**DA Form 4951**
Lease/Purchase Analysis for Copying/Duplicating Machines

**DA Form 7222–1**
Senior System Civilian Evaluation Report Support Form

**DA Form 7223–1**
Base System Civilian Performance Counseling Checklist/Record

**DD Form 428**
Communication Service Authorization

**DD Form 448**
Military Interdepartmental Purchase Request

**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

**DLA Form 2500**
Certificate of Hard Drive Disposition
(Available from http://www.dla.mil/dispositionservices/offers/disposal/turnin/forms.aspx.)

**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 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 on the DD Form 2946 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 workplace (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 USG 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 USG, 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 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. Cybersecurity.* The applicant agrees to follow all cybersecurity requirements identified by the AO. The applicant agrees to complete user security awareness training, participate in all required training programs, and protect information at all times.

*l. Liability.* The applicant understands that USG 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 USG 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 USG 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 5 USC 8101 et seq (known as 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 (Senior System 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.

*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 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, DD Form 2946 will expire on a set date, unless renewed by agreement of the employee and the employer.

*v. Certification.* By signing DD Form 2946, the applicant certifies that they have read the terms of the agreement and agree to follow the policies and procedures outlined as well as all other applicable policies and procedures.

*w. Applicant's signature.* Employee signs DD Form 2946.

*x. Date.* Employee enters the date the DD Form 2946 is signed.

### 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 on).

*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 signs DD Form 2946, certifying that all of the 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 (paras B–3*h* through B–3*j* may not be applicable to the telework employee). If this is the case, state "not applicable" or "N/A". The following information is entered on DD Form 2946:

*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 it is a requirement and if ownership is by either the government agency or personal, and whether it is reimbursement by component. Check the following 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)* Facsimile 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 cybersecurity and RMF operations of the equipment 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.* Enter 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. Cancellation of the telework arrangement requires the following information entered on DD Form 2946:

*a.* Cancellation date (YYYYMMDD).
*b.* Initiated by:
(1) Employee.
(2) Management.
*c.* Reason(s) for cancellation.
*d.* Government-furnished equipment and/or property returned list property and date of return (Yes/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 DWCF bills. This list of bills must be provided to the TCO when they are appointed so they understand their duties.

*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. 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 for federal civilian employees, military commanders for military personnel, and contracting officers in the case of contractors or their employees (see para C–1*d* for information regarding telecommunication bill certification actions).

*d.* 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 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 un-tariffed services have been changed to tariffed services. The contracting officer's representative should keep a file of applicable tariffs and proposed tariff adjustments sufficient to explain monthly recurring costs.

(13) Maintain a trend analysis. Compare monthly recurring cost, long-distance charges, and total bill for each account with the previous month to see if any major changes occurred.

(14) Discuss disputes immediately with vendor's customer service representatives or your ARCYBER 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 Form 1034 (Public Voucher for Purchases and Services Other Than Personal).

(19) Process bills in a timely manner. Prioritize workload to allow time to prepare SF Form 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 vendor pay database by sending an email to the DFAS wide area workflow help desk at disa.ogden.esd.mbx.cscassig@mail.mil (https://wawf.eb.mil/xhtml/unauth/web/homepage/vendorcustomersupport.xhtml) in order to:

*(a)* Review the status and amounts of telecommunications vendor payments processed by DFAS.

*(b)* Aid in resolving payment questions from vendors.

(22) The following guidelines apply to billing for LH services:

*(a)* Bills for Army LH communications services are processed through the G8 LH. Customers must submit a DD Form 448 (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 DISA Direct Order Entry System. 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 accounts and/or negative unliquidated obligations while they are being disputed. 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 a reportable anti-deficiency act violation and may result in an interruption of service. G8 LH cannot hold a monthly bill until disputes are complete. If the dispute is justified, then appropriate adjustments will be made to the account.

*e.* 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.

*f.* 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. Phone calling cards require special security precautions to prevent unauthorized use. Cards are canceled when the cardholder separates from the organization, no longer requires a calling card, or when it is believed a calling card number has been compromised. 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.

*g.* The TCO must exercise continual management over cellular phone bills since 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).

*h.* 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 Federal Telecommunications System (commercial) or SBU voice. Installations and separate reporting activities may institute the measures to reduce telecommunications costs without degrading service.

*i.* Installations and separate reporting activities may institute the following measures 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. 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 for long-distance calls.

(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, the 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.

*j.* 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 37–1 Regulation.

(1) In some locations, USG 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) DOD establishes rates for Class B service. 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 37–1 Regulation.

(3) The subscriber pays charges for Class B service relocations resulting from on-post government quarters movements of personnel, unless the move is directed by USG or is for government convenience. 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 LH communications services are processed through the ATD. Customers submit a DD Form 448 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 the DISA 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.* Cable television (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 USG to pay for CATV services for NAF activities or individual subscribers. NAF 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, ASCC, DRU, and Unified Command public affairs offices through HQDA to Office of the Assistant Secretary of Defense (PA), Director, Defense Media Activity.

*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 element of resource (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 third and fourth positions identify the detail needed for management reports, budget exhibits, and general ledger requirements.

### D–2. Element of resource categories

EOR tables and additional information is available in the DFAS–IN Manual 37–100 at http://asafm.army.mil/offices/bu/dfas37100.aspx. The Army proponent for EORs is ASA (FM&C) (SAFM–BUC–F). EORs have been divided into four categories to facilitate readability and usage:

*a.* Current–civilian and military pay EORs.
*b.* Current–nonpay EORs.
*c.* Expired–civilian and military pay EORs.
*d.* Expired–nonpay EORs.

## Appendix E

## Army Capabilities and Architecture Development and Integration Environment

### E–1. General information

AR 71–9 directs that all IT and/or NSS products must comply with DODAF and AEA requirements and be documented in an Army architecture centralized database. MATDEVs and other IM officials requiring IT and/or NSS will ensure compliance with architectures. Directors of IM will review and ensure compliance with architectures. The Army architecture centralized database, implemented in 2006, is the 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 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 DODIN–A.

### E–2. Portal access

All unclassified Army architectures will be stored in the ArCADIE portal at https://cadie.army.mil and classified architectures will be stored on SIPRNET at https://cadie.army.smil.mil. To access the NIPRNET 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. 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 DM and integration success. The Army leverages integrated architecture data standards (IADS) developed by the Army architecture and DS communities and approved by the architecture DS. 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.* 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/default.aspx.

## E–4. Managed user access

Authentication verifies the identity of users and validates using a CAC through single sign-on and enterprise collaboration services. Each area of the environment is duty-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.army.mil/cadie/portal/default.aspx.

*b.* Help desk telephone numbers are located on the ArCADIE home page. 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, CIO/G–6 has appointed an architecture DS 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 DS in keeping the architecture COI informed falls under the function of the appointed FDMs of each domain. ArCADIE provides the means to support the governance process by enforcing data standards, common architecture development, and verification and validation for Army architectures.

## Appendix F

## Administrative Request Memorandum for Print Devices

### F–1. Background

Provide background information identifying the problem, condition, or reasons leading to the request.

### F–2. As-is printing environment

Provide the number of printers currently in use among the population to be supported by the new printing device.

### F–3. Objective

Briefly summarize the overall purpose, goal, or benefit to be achieved in accepting this request. Include other than monetary benefits expected from the printing device(s). Explain anticipated savings in time and maintenance, and justify the selection of the requested copier over comparable printing devices.

### F–4. Equipment requested

*a.* Specify model and manufacturer of printer from CHESS inventory.

*b.* Provide at least one alternative proposal from a different vendor considered in the printing device selection process.

*c.* Include special features or additional accessories; for example, automatic document feeder, automatic duplexing, collating, and reduction capabilities.

*d.* Provide the approval control number of the printing device identified for turn-in if the request is for a replacement printing device.

### F–5. Estimate the types of material to be copied in a typical month

*a.* Include description of each type.

*b.* Give number of originals, by type.

*c.* Include average number of copies to be made from each original.

*d.* Indicate copy to original ratio.

*e.* Give monthly volume estimate.

### F–6. Other information

*a.* Include the distance from the nearest printing device that would satisfy an existing requirement.

*b.* Give the proposed location of requested printing device (room, building).

*c.* Indicate the quantity and security classification of classified material to be reproduced, if applicable.

*d.* Justify any unforeseen increase in the amount of material to be reproduced. Give the basis for the increase such as a change in mission or function.

*e.* Include a completed DA Form 4951 for each printing device being considered.

### F–7. Method of procurement

*a.* Indicate whether the printing device will be procured under flat rental, metered rental, or purchase.

*b.* Indicate if equipment qualifies for purchase under the Quick Return on the Investment Program, or if it will qualify after the initial rental period.

### F–8. Basis for request. Enter the justification

*a.* Indicate procedures currently used for reproducing material and state why existing printing devices cannot be used; for example, relocation or centralization.

*b.* Include current monthly cost (for example, rental, purchase, maintenance, supplies) of production.

*c.* Give estimated total monthly cost (rental, purchase, maintenance, supplies) of proposed printing device.

## Appendix G

## Army Portfolio Management Solution Registration Business Rules

### G–1. General

All IT investments/solutions must be accounted for in APMS in accordance with AR 25–1. This section will provide general information about portfolio management as well as guidance on what to register and how to account for it in APMS.

### G–2. Department of Defense Information Technology Portfolio Repository

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

*(a) Department of Defense Information Technology Portfolio Repository–reportable.* This includes any investment that requires any compliance reporting, as well as all DBSs, including modified commercial off-the-shelf (COTS) systems. Refer to the APMS DSRM for additional guidance on registration criteria. 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.

*(b) Non-Department of Defense Information Technology Portfolio Repository–reportable.* Depending on reporting requirements, not all entries in APMS are reported to DITPR. This could be for an investment where the Army is not the lead agent but uses an Army appropriation. These investments will be reported to DITPR by the owning service component or agency.

### G–3. Registration

Regardless of registration method (DITPR–Reportable or Non-DITPR–Reportable) you must complete the entire registration process. Systems and applications that reside on enterprise services must be identified separately and accounted for as independent records in APMS. For example, applications that are developed to create workflow, tracking, and other functions that support specific functional business processes in SharePoint and are funded separately from the parent solution must be registered and the funding accounted for in APMS as separate records and not consolidated under the main investment record. IT solutions can be consolidated under another record if, collectively, the combined component solutions provide a single system (or SoS) and the individual components do not have separate compliance–Reporting requirements. Mission applications and systems should not be consolidated under a parent network record; the functional proponent or champion of the investment will register the application or system. Network operations/management tools should be registered separate from the network to ensure visibility of this type of investment. One example of IT that could be consolidated under one or more records by the organization is end-user computing IT (see para G–5*h*).

### G–4. Army Portfolio Management Solution folders

*a.* All APMS records must complete the modules in the Required Data, DITPR, BMA Line of Business, JCA, and Required and Budgeted Detail folders as appropriate.

*b.* DITPR–Reportable records additionally require Joint Common Systems Function List be completed.

*c.* The following documents are required for Non-DITPR–Reportable items:

(1) Required Data folder (Army Required and Parent/Child Relationships only).

(2) Financial Data folder.

(3) Joint Common Systems Function List.

*d.* All applicable types of appropriations must be listed on the Financial Data folder (for example, operations and maintenance; other procurement; research, development, testing, and evaluation; MILCON). Identify all HW, SW, and services that support an investment on the Components tab of the Command Detail folder. This information will be used to validate Army IT waiver and approval system requests.

### G–5. Army Portfolio Management Solution information technology infrastructure and naming conventions

Individual records will be added for the infrastructure investments outlined in this appendix, which may include a consolidation of HW, SW, and services. If a record already exists in APMS for your infrastructure, you are not required to change the name to meet the naming conventions described in this appendix. If further delineation is necessary for any investment name, use the appropriate office symbol as identified at https://www.arims.army.mil/ and in accordance with AR 25–59.

*a.* Data centers or continuity of operations plan sites are defined as a collection of computers, data storage systems, and ancillary equipment in a specialized space used for computing resources. For naming convention, the acronym will match the data center identification from APMS. The item name will match the data center name from APMS. Data center records include, but are not limited to, the following:

(1) Blade servers and racks.
(2) Mainframe and mini computers.
(3) Storage area and SAN devices.
(4) Matrix switches used to interconnect equipment.
(5) Optical storage systems.
(6) Tape drives and tape storage devices.
(7) High-speed printers.

*b.* All laboratories, virtual reality, and simulation centers supporting the research, development, test, and evaluation of information technologies, IS, and applications will be aligned with the appropriate JCA or line of business attributes and binned in the appropriate mission area and domain the lab supports (for example, Air and Missile Defense Simulation Laboratory (binned in WMA); Defense Forensic Science Center Materiel Technology Laboratory Family of Systems (binned in BMA); and Labs used to test AEN computer equipment, operating systems and SW, HW, firmware (binned in EIEMA)). Any additional life cycle IT investment obtained to replace, extend, or improve the existing laboratory will be registered as a dependency to the existing laboratory investment already in APMS. The naming convention for APMS lab records will begin with the word "LAB" and then the functional purpose or unit name and location (for example, LAB–XXX Simulation-Cyber Center of Excellence, Fort Gordon).

*c.* Naming conventions for all telephone switching equipment owned by the Army will begin with either private branch exchange (PBX) or voice system, then the installation name (for example, PBX–MCCOY). These records will be binned in the EIEMA core enterprise services domain. These records include:

(1) All PBX systems.
(2) All major key systems.
(3) All central office-class switching systems.
(4) Voice Over Internet Protocol equipment when attached to the PBX or switch, unless provided over the LAN through LAN routers.
(5) All multiplexors, main distribution frames, intermediate distribution frames, and other wiring.
(6) The cost of telephones purchased to upgrade or support the systems.

*d.* For all networks (including unique or special use) at each installation, mission applications or systems are not to be consolidated under a network record in APMS (use Dependencies folder to establish relationship). These records will be binned in the EIEMA communications domain. Examples include—

(1) Medical Network (MEDNET).
(2) SIPRNET.
(3) NIPRNET.
(4) Other specialty networks.

*e.* Naming conventions for all RHNs, including all satellite, radio, switching, and multiplexing equipment and encryption equipment will begin with the words RHN in the name and then have the regional designation (for example, RHN–NETOPSV1.0). These records will be binned in the EIEMA communications domain.

*f.* All collections of audio and visual conferencing hubs used as switching centers for large shared video or audio teleconferencing, when it is owned by the Army, will be binned in the EIEMA core enterprise services domain. For naming convention, audio and visual records will begin with "AUDIO VISUAL" followed by the installation or location and then the organization name (for example, AUDIO VISUAL–SHAFTER–ORG).

*g.* A common user interface (CUI) record in APMS is used to collect and aggregate data for general end-user computing HW, SW, and services for an entire organization. The CUI records do not include any IT that requires a stand-alone accreditation or is purchased as a single investment; those require a regular record in APMS. The APMS command administrators may choose to register infrastructure records down to the sub-organization level for better fidelity but will have a minimum of one CUI record to consolidate their end-user computing IT. The CUI records are non-DITPR reportable. These records will be binned in the EIEMA computing infrastructure domain. For naming convention, common user infrastructures will start with CUI then the command name and the organization office symbol (for example, CUI–COMMAND–office symbol). The CUIs include, but are not limited to the following:

(1) Desktops.
(2) Laptops.
(3) BlackBerry smart phones and other commercial mobile devices.
(4) PDAs.

(5) Printers.
(6) Facsimile.
(7) Scanners.
(8) Desktop applications that do not require a stand-alone record in APMS.

*h.* ICS and supervisory control and data acquisition systems at each installation will not to be consolidated under a network record in APMS. The investment owners should consult with the BMA manager to determine the appropriate binning (these records are not to be automatically considered as an EIEMA investment). These investments will be binned/aligned in the mission area/domain whose business processes or mission they support.

## Appendix H

## Army Standard for Life Cycle Replacement of Information Technology Assets

### H–1. General

The Army acknowledges the need to manage its IT assets and improve overall life cycle management (planning, acquisition, deployment, management, retirement, and disposal) to increase productivity, decrease downtime, and elevate user experience.

### H–2. Life cycle replacement rates

Table H–1 provides recommended life cycle replacement rates for end-user devices and other IT assets. Army organizations should use these rates for planning and budgeting purposes. Equipment can be replaced at any point prior to the indicated rates based on operational needs.

### H–3. Annual budget planning cycle

Army organization strategic planning must incorporate regular IT HW life cycle replacement (see OMB Circular A–130). Army organizations will include regular life cycle replacement cost into the organization annual budget planning cycle (see OMB Circular A–11). Army organizations will utilize recommended industry standards business rules for IT HW and MUE life cycle replacement categories (see table H–1).

**Table H–1**
**Hardware and mission unique equipment life cycle replacement categories**

| | |
|---|---|
| **COTS IT Hardware (Computers, Printers, Digital Senders)** | |
| MTOE Units | 4 years |
| Table of Distribution and Allowances (TDA) Units | 5 years |
| DBS COTS IT Hardware | 5 years |
| Zero/Thin Client | 7 years |
| **Computing Devices** | |
| Blade | 5 years |
| Blade Chassis | 6 years |
| Hyper-converged | 5 years |
| Server | 5 years |
| **Storage Devices** | |
| SAN Chassis | 5 years |
| Disk Shelf | 5 years |
| Fiber Channel Port | 3 years |
| **Security Devices** | |
| Intrusion Protection System/Intrusion Detection System | 5 years |
| Firewall | 5 years |
| Full Packet Capture | 5 years |
| Security Appliance | 5 years |
| Communications security | 5 years |

**Table H–1**
**Hardware and mission unique equipment life cycle replacement categories—Continued**

| | |
|---|---|
| **Integrated Communication Devices** | |
| Router | 5 years |
| Switch | 5 years |
| Optical Networking (for example, Optical Transport Network) | 7 years |
| Network Appliance | 5 years |
| Session Border Controller | 7 years |
| VTC Multipoint Control Unit | 5 years |
| **Mission Unique Equipment** | |
| Secure and Unsecure Audio/Video and Collaboration Equipment | 5 years |
| Digital Monitors | 5 years |
| Projectors | 5 years |
| CATV/Satellite Television Equipment | 5 years |
| Equipment Racks | 15 years |
| Power Distribution Unit | 7 years |
| Uninterrupted Power Supply | 5 years |

## Glossary

### Section I

### Abbreviations

**ABC**
Army Business Council

**ACA**
architecture compliance assessment

**ACAS**
Army Centralized Army Service Request System

**ACAT**
acquisition category

**ACCT**
Architecture Configuration Control Team

**ACMO**
Army Configuration Management Office

**ACOM**
Army command

**ACP**
allied communications publication

**ACSIM**
Assistant Chief of Staff for Installation Management

**ADB**
Army Data Board

**ADC**
Army Data Council

**ADCCP**
Army Data Center Consolidation Plan

**ADMG**
Army Data Management Guide

**ADMP**
Army Data Management Program

**ADRP**
Army doctrine reference publication

**ADS**
authoritative data source

**AEA**
Army Enterprise Architecture

**AEN**
Army Enterprise Network

**AENC**
Army Enterprise Network Council

**AESD**
Army enterprise service desk

**AESM**
Army enterprise service management

**AESMF**
Army Enterprise Service Management Framework

**AIA**
Army Information Architecture

**AIC**
Army interoperability certification

**AIS**
automated information system

**AITR**
Army Information Technology Registry

**AKO**
Army Knowledge Online

**ANS**
Army Network Strategy

**AO**
authorizing official

**AoA**
analysis of alternatives

**APB**
acquisition program baseline

**APE**
Army program element

**APL**
approved products list

**APMS**
Army Portfolio Management Solution

**AR**
Army Regulation

**ArCADIE**
Army Capabilities and Architecture Development and Integration Environment

**ARCYBER**
U.S. Army Cyber Command

**ARNG**
Army National Guard

**ASA (ALT)**
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

**ASA (FM&C)**
Assistant Secretary of the Army (Financial Management and Comptroller)

**ASC**
Army Standards Council

**ASCC**
Army service component command

**ASCII**
American Standard Code for Information Interchange

**ASR**
Army service request

**ATD**
Army Telecommunications Directorate

**ATM**
Asynchronous Transport Mode

**ATO**
authority to operate

**AV**
all viewpoints

**AWRAC**
Army web risk assessment cell

**BASECOM**
base communications

**BMA**
business mission area

**BPA**
blanket purchase agreement

**BWC**
backward capability

**C2**
command and control

**C4IM**
command, control, communications, computers, and information management

**C4IT**
command, control, communications, computers, and information technology

**CAC**
common access card

**CAP**
Computer/Electronic Accommodations Program

**CATV**
cable television

**CCA**
Clinger-Cohen Act

**CDD**
capability development document

**CDO**
chief data officer

**CfM**
configuration management

**CFR**
Code of Federal Regulations

**CHESS**
Computer Hardware, Enterprise Software and Solutions

**CHS**
common hardware systems

**CIO**
Chief Information Officer

**CIO EB**
Chief Information Officer Executive Board

**CJCSI**
Chairman of the Joint Chiefs of Staff instruction

**COE**
common operating environment

**COI**
community of interest

**CoN**
Certificate of Networthiness

**CONOPS**
concept of operations

**CONUS**
continental United States

**COTS**
commercial off-the-shelf

**CP–34**
career program 34

**CPD**
capability production document

**CTA**
common tables of allowances

**CUI**
common user interface

**DA**
Department of the Army

**DA Form**
Department of the Army form

**DA Pam**
Department of the Army pamphlet

**DBMS**
database management system

**DBS**
Defense business system

**DCIM**
data center inventory management

**DCS**
Deputy Chief of Staff

**DD Form**
Department of Defense form

**DDMS**
Department of Defense Discovery Metadata Specification

**DECC**
Defense Enterprise Computing Center

**DER**
data engineering resource

**DESMF**
Defense Enterprise Services Management Framework

**DFAS**
Defense Finance and Accounting Service

**DIMA**
Department of Defense intelligence mission area

**DISA**
Defense Information Systems Agency

**DISN**
Defense Information Systems Network

**DISR**
Department of Defense Information Technology Standards Registry

**DITPR**
Department of Defense Information Technology Portfolio Repository

**DLA**
Defense Logistics Agency

**DM**
data management

**DOD**
Department of Defense

**DODAF**
Department of Defense Architecture Framework

**DODD**
Department of Defense directive

**DODI**
Department of Defense instruction

**DODIN**
Department of Defense information network

**DODIN–A**
Department of Defense information network–Army

**DODM**
Department of Defense manual

**DQM**
data quality management

**DRMS**
Defense Reutilization and Marketing Service

**DRU**
direct reporting unit

**DS**
data steward

**DSE**
data services environment

**DSM**
data strategy metrics

**DSN**
defense switched network

**DSRM**
Desk Side Reference Manual

**DTR**
Defense Transportation Regulations

**DWCF**
defense working capital fund

**EAMS–A**
enterprise Access Management System–Army

**EIA**
Electronic Industries Alliance

**EIEMA**
enterprise information environment mission area

**EIT**
electronic and information technology

**ELA**
enterprise license agreement

**eMASS**
Enterprise Mission Assurance Support Service

**EOP**
external official presence

**EOR**
element of resource

**ESI**
enterprise software initiative

**ETL**
extraction, transformation, and loading

**EXORD**
Execution Order

**FaNS**
Federation of Net-Centric Sites

**FAR**
Federal Acquisition Regulation

**FDED**
Fort Detrick Engineering Directorate

**FDM**
functional data manager

**FIPS**
Federal Information Processing Standard

**FOIA**
Freedom of Information Act

**FOUO**
for official use only

**FSS**
federal supply schedule

**FTS 2001**
Federal Telecommunications System 2001

**FYDP**
Future Years Defense Program

**GHz**
gigahertz

**GO**
general officer

**GOSC**
General Officer Steering Committee

**GPC**
government purchase card

**GS**
general schedule

**GSA**
General Services Administration

**GTG–F**
Global Information Grid Technical Guidance Federation

**HMW**
health, morale, and welfare

**HQDA**
Headquarters, Department of the Army

**HTML**
hypertext markup language

**HTTP**
hypertext transfer protocol

**HTTPS**
hypertext transfer protocol secure

**HW**
hardware

**I3A**
installation information infrastructure architecture

**I3MP**
Installation-Information Infrastructure Modernization Program

**IA**
information assurance

**IADS**
integrated architecture data standards

**IAVM**
information assurance vulnerability management

**IC&L**
interoperability capabilities and limitations

**ICD**
initial capabilities document

**ICS**
industrial control systems

**IEA**
Information Enterprise Architecture

**IEC**
International Electro-technical Commission

**IEEE**
Institute of Electrical and Electronic Engineers

**IEPD**
information exchange package documentation

**IES**
information exchange specification

**IM**
information management

**IMO**
information management office/officer

**IRM**
information resource management

**IS**
information systems

**ISCE**
information systems cost estimate

**ISDN**
Integrated Services Digital Network

**ISEC**
information system/electronic collection

**ISO**
International Standardization Organization

**ISP**
information support plan

**ISR**
Installation Status Report

**ISR–S**
Installation Status Report–Services

**IT**
information technology

**ITAS**
Information Technology Approval System

**ITM**
information technology management

**ITOC**
Information Technology Oversight Council

**ITSM**
information technology service management

**IV&V**
interoperability verification and validation

**IV&VA**
interoperability verification and validation accreditation

**JCA**
Joint Capability Area

**JCIDS**
Joint Capabilities Integration and Development System

**JIE**
Joint Information Environment

**JIST**
Joint Integrated Satellite Communications Technology

**LAN**
local area network

**LH**
long haul

**MATDEV**
materiel developer

**MC**
Mission Command

**MDEP**
management decision package

**MEDCOM**
Army Medical Command

**MEDNET**
Medical Network

**MILCON**
military construction

**MIRC**
Migration Implementation and Review Council

**MPLS**
Multi-Protocol Label Switching

**MS**
milestone

**MTOE**
modified table of organization and equipment

**MUE**
mission unique equipment

**MWR**
morale, welfare, and recreation

**NAF**
nonappropriated fund

**NC**
net-centric

**NCS**
network capability set

**NEC**
Network Enterprise Center

**NETCOM**
U.S. Army Network Enterprise Technology Command

**NIEM**
national information exchange model

**NIPRNET**
non-secure internet protocol router network

**NIST**
National Institute of Standards and Technology

**NR–KPP**
net–Ready key performance parameter

**NSS**
National Security System

**NVA**
network vulnerability assessment

**OBT**
Office of Business Transformation

**OCONUS**
outside the continental United States

**OMB**
Office of Management and Budget

**OPA**
other procurement–Army

**OPSEC**
operational security

**OPTEMPO**
operations tempo

**OSD**
Office of the Secretary of Defense

**OV**
operational view

**PAS**
Privacy Act Statement

**PBX**
private branch exchange

**PC**
personal computer

**PDA**
personal digital assistant

**PDF**
portable document format

**PEG**
program evaluation group

**PEO**
Program Executive Office

**PEO EIS**
Program Executive Office, Enterprise Information Systems

**PEO–SD**
program executive officer-self-determination

**PIA**
privacy impact assessment

**PII**
personally identifiable information

**PIN**
personal identification number

**PKI**
Public Key Infrastructure

**PL**
product lead

**PM**
program manager

**POA&M**
plan of action and milestones

**POC**
proof of concept

**POM**
program objective memorandum

**POP**
point of presence

**PPBE**
planning, programming, budgeting, and execution

**PRB**
Project Review Board

**R&M**
renovation and modernization

**RCC**
Regional Cyber Center

**RHN**
Regional Hub Node

**RIG**
Resource Integration Group

**RMF**
Risk Management Framework

**SAN**
storage area network

**SAR**
satellite access request

**SATCOM**
satellite communications

**SBU**
sensitive but unclassified

**SDP**
service delivery point

**SES**
senior executive service

**SF**
standard form

**SIPRNET**
secret internet protocol router network

**SLA**
service level agreement

**SLM**
service level management

**SMART**
specific, measurable, actionable, relevant, and timely

**SMS**
Strategic Management System

**SNAP**
systems/network approval process

**SNS**
social networking sites

**SoNA**
Statement of Non-Availability

**SOR**
system of records

**SORN**
System of Records Notice

**SoS**
system of systems

**SSN**
social security number

**StdV**
standards view

**STIG**
security technical implementation guides

**SUT**
system under test

**SV**
system view

**SW**
software

**TAP**
The Army Plan

**TCO**
telephone control officer

**TDA**
table of distribution and allowances

**TDD**
telecommunications device for the deaf

**TDM**
time-division multiplexing

**TEMP**
test and evaluation master plan

**TEP**
temporary exception to policy

**TIR**
test incident report

**TOE**
table of organization and equipment

**TOS**
terms of service

**TPN**
tactical processing node

**TRADOC**
U.S. Army Training and Doctrine Command

**TSACS**
Terminal Server Access Control System

**UC**
unified capabilities

**UID**
unique identification/identifier

**UML**
Unified Modeling Language

**URL**
uniform resource locator

**USACE**
U.S. Army Corps of Engineers

**USAISEC**
U.S. Army Information Systems Engineering Command

**USAR**
U.S. Army Reserve

**USC**
United States Code

**USD(C)**
Under Secretary of Defense (Comptroller)

**USG**
U.S. Government

**VPN**
virtual private network

**VTC**
Video teleconferencing

**WAN**
wide area network

**WIDS**
Wireless Intrusion Detection Systems

**WLAN**
wireless local area network

**WMA**
warfighting 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 Pam 70–3.

**American Standard Code for Information Interchange**
The standard code used for information interchange among data processing systems, data communications systems, and associated equipment in the United States. The American Standard Code for Information Interchange (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**
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. The representation of digital data using analog signaling media such as analog tone modulation of a radio frequency carrier. Data transmitted over an analog transmission medium (for example, voice grade channel using an analog modem).

**Application**
A SW 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.

**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 ACOMs, ASCCs, DRUs, field operating activities, 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**
ARCYBER is an operational level Army force designated as an ASCC by the Secretary of the Army as the U.S. Army Cyber Command. ARCYBER is the primary Army headquarters responsible for conducting cyberspace operations (offensive cyberspace operations, defensive cyberspace operations, and DODIN operations), as directed and authorized on behalf of the Commander, U.S. Strategic Command or Commander, U.S. Cyber Command. ARCYBER organizes, trains, educates, mans, equips, funds, administers, deploys, and sustains Army cyber forces to conduct cyberspace operations.

**Army Enterprise Architecture**
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 Warfighters into a blueprint for an integrated and interoperable set of IS 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 Enterprise Service Desk Federation**
The AESD capability is a federation of Army IT service desks across the globe to perform common enterprise IT service desk functions, as well as unique command systems and application support. The AESD Federation is not an organization but regionally aligned service desk resources, dedicated to performing an enterprise function. The AESD provides a single point of contact for service requests in all theaters.

**Army Operational Data Repository**
A metadata repository used for architectures of functional Army systems.

**Army Telecommunications Directorate**
A subordinate element of the U.S. Army Networks, Engineering, and Telecommunications Directorate under the command of the Commanding General, NETCOM, a major subordinate command of ARCYBER that provides centralized management of the Army's worldwide commercial-leased and government-owned telecommunications; serves as the Army interface with the DISA, Defense Information Technology Contracting Organization, 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 ADS may be the functional combination of multiple, separate data sources.

**Automated information system**
An acquisition program that acquires IT, excluding IT involving equipment vital to a weapon system or weapons systems or is a tactical communication system (see 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.

**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 SW that moves documents from websites 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.

**Cable television system**
A facility consisting of a set of closed transmission paths and associated signal generation, reception, and control equipment that is designated to provide cable service that includes both audio and video programming, and 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 packet switch stream call types include 30 bits per second dial-up data; 1,200 bits per second dial-up data; or 9,600 bits per second digital data.

**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**
*a. Class A (official).* Telephone service authorized for the transaction of official government business 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.
*b. 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.
*c. Class C (official–restricted).* Telephone service authorized for the transaction of official government business on a DOD and/or military installation, and without access to telephone company central office or toll trunks.
*d. Class D (official–special).* Telephone service installed on military installations for official government business and restricted to special classes of service, such as fire alarm, guard alarm, and crash alarm.

**Command, control, communications, and computer systems**
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications, and computers designed to support a commander's exercise of C2 across the range of military operations.

**Command, Control, Communications, Computers, and Information Management Services List**
The C4IM Services List pertains to NEC and Network Operations and Security Center provided services and managed infrastructure. The list's service groups are communication systems and systems support, cybersecurity, and automation.

**Command, control, communications, computers, and intelligence**
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.

**Commercial communications work order**
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.

**Common hardware systems**
A rapid execution vehicle designed to meet tactical requirements using state-of-the-art computing and networking equipment to improve connectivity, interoperability, logistics, and maintenance support to Soldiers.

**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.

**Communications systems**
A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

**Community of interest**
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**
A group of people who have a common interest in some subject or problem, who 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.

**Conference call**
Call in which more than two access lines are connected.

**Configuration**
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.

**Connection fee**
The charge, if any, imposed on a subscriber by the CATV franchisee for initial hookup, reconnection, or relocation of equipment necessary to transmit the CATV signal from the distribution cable to a subscriber's receiver.

**Context**
The interrelated conditions that compose the setting in which the architectures exist. It includes environment, doctrine and tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

**Customer/user**
The requester and recipient of information services.

**Cybersecurity**
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

**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 comprises 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 website 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 management services**
Data management services provide for the independent management of data shared by multiple applications. These services include data dictionary, directory services, and database management system (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 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 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 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, and C2). The service may or may not be switched.

**Dedicated transmission service**
The service category covering provision of private-line transmission of voice or data using end-to-end transmission media.

**Defense Information Technology Management System**
Manages the reporting of automation resources inventory and excess including HW and SW.

**Delay**
The interval of time between transmission and reception of a signal.

**Department of Defense information network**
The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to Warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, SW (including applications), data, security services, other associated services, and NSS.

**Department of Defense Information Technology Standards Registry**
The DISR is an online repository for a minimal set of primarily commercial IT standards formerly captured in the Department of Defense Joint Technical Architecture, 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 DISN. In addition, the DISR provides the capability to build profiles of standards that programs will use to deliver NC capabilities.

**Digital switching**
A process in which connections are established by operations on digital signals without converting them to analog signals.

**Doctrine**
Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. Doctrine represents consensus on how the Army conducts operations today.

**Domain**
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.

**Domestic**
Within the United States, Puerto Rico, the U.S. Virgin Islands, Guam, the Northern Marianas, and American Samoa.

**Dual–tone multi–frequency 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 facsimile.

**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 is 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 service delivery point (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). EOPs are established on commercial venues for the purposes of creating a transparent information-sharing environment and gaining feedback from the public.

**Facsimile transmission**
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 facsimile 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**
The government organization that plans, develops, establishes, and manages the Federal Telecommunications System program to meet federal requirements for common user local and long-distance telecommunications services government-wide (Federal Telecommunications Service prior to October 1997).

**Federal Telecommunications System 2001**
A combination of federal telephone contract options for commercial long-distance telecommunications services available to federal agencies. Federal Telecommunications System 2001 (FTS 2001) is managed by GSA.

**File transfer protocol**
A transmission control protocol/internet protocol 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 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 friendlier 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.

**Global Information Network**
Legacy term used to describe the DOD's globally interconnected network of information capabilities (replaced by the term DODIN).

**Government office equipment/services**
Equipment and/or systems purchased, leased, and/or owned by the government. This includes, but is not limited to, IT equipment, pagers, internet services, email, library resources, telephones, portable electronic devices, smartphones, facsimile machines, photocopiers, and office supplies.

**Governmental regulatory body**
The Federal Communications Commission, statewide regulatory body, public utility commission, or anybody with less than statewide jurisdiction when operating pursuant to state authority.

**Government–wide purchase card**
Provides a means to purchase items at a lower cost and gives unit commanders organic procurement capability.

**Hardware reuse**
Excess HW must be condition-coded as serviceable or unserviceable. All serviceable HW, 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**
Authoring SW language used on the internet and for creating web pages. Hypertext markup language (HTML) is essentially text with embedded HTML commands identified by angle brackets and known as HTML tags.

**Hypertext transfer protocol**
The communications protocol used by a web browser to connect to web servers on the internet.

**Hypertext transfer protocol secure**
The protocol for accessing a secure web server. The use of HTTPS in the uniform resource locator (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 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, compute 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**
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 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, HW (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**
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 that 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, SW, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a federal contractor incidental to a federal contract (see 40 USC Subtitle III).

**Information technology 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.

**Information technology equipment used for Department of Defense component cryptologic applications**
Equipment acquired that becomes excess will be reported to the National Security Agency in accordance with its implementing circulars.

**Information Technology Infrastructure Library**
A set of internationally recognized best business practices on the management and provision of operational IT Services.

**Information technology requirements**
Clear definitions of the functional requirements, not just the technical or system requirements.

**Infrastructure**
Most generally relates to and has a HW orientation but is frequently more comprehensive and includes SW and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. It includes processors, operating systems, service SW, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include HW builds versus schedule and costs.

**Installation information infrastructure architecture**
The I3A is a standard architecture for 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 DM ensures the provision of correct information to the right person(s) at the necessary time. As a subset of IM, 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 DM 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**
An ISDN in which the same digital switches and digital paths are used to establish connections for different services; for example, voice, data, or video.

**Internet**
A global interconnection of individual networks operated by USG, industry, academia, and private parties. The internet originally served to connect laboratories engaged in government research and has been expanded to serve millions of users and a multitude of purposes.

**Internet protocol**
A DOD standard protocol designed for use in interconnected systems of packet-switched computer communication networks. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small packet networks.

**Internet–based capabilities**
All publicly accessible information capabilities and applications available across the internet in locations not owned, operated, or controlled by DOD or the Federal Government. Internet-based capabilities include collaborative tools such as social media, user-generated content, social SW, email, instant messaging, and discussion forums (for example, YouTube, Facebook, MySpace, Twitter, Google Apps) (see DODI 8550.01)

**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.

**Knowledge management**
The process of enabling knowledge flow to enhance shared understanding, learning, and decision making (see ADRP 6–0).

**Lease**
IS 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 Federal 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 area network**
A data communications system that lies within a limited spatial area, has a specific user group, has a specific topology, and is not a public switched telecommunications network, but may be connected to one. LANs are usually restricted to relatively small areas, such as rooms, building, ships, and aircraft. 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. LANs are not subject to public telecommunications regulations.

**Location**
A physical space, such as a building or a room. A physical point where the FTS 2001 contractor delivers service to a user.

**Mandatory**
Those services, features, or equipment that 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 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 defense switched network (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 SW application that uses a database to store and search records that describe such items as documents, images, and videos. Search portals and applications can use metadata catalogs to locate the data assets that are relevant to their queries.

**Metadata registry**
Repository of all metadata related to data structures, models, dictionaries, taxonomies, schema, and other engineering artifacts that are used to support interoperability and understanding through semantic and structural information about the data. A federated metadata registry is one in which multiple registries are joined electronically through a common interface and exchange structure, thereby effecting a common registry.

**Mission**
A group of tasks with their purpose assigned to military organizations, units, or individuals for execution.

**Mission area**
A defined area of obligation with functions and processes that contribute to mission accomplishment.

**Mission related**
Processes and functions that are closely related to the mission (for example, the mission of "direct and resource the force" has the mission–Related functions of planning, programming, policy development, and allocating of resources).

**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. 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**
NSS means "any telecommunications or information system operated by USG, the function, operation, or use of which involves intelligence activities, involves cryptologic activities related to national security, involves C2 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)." (See 40 USC 11103.)

**Net–centric**
Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision-making cycles. NC capabilities enable network-centric operations and net-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 Enterprise Center**
The NEC is the installation information manager. As the installation NEC, assigns the functions of the installation staff officer who monitors IM.

**Network programming**
Programming supplied by a national or regional television or radio network, either commercial or noncommercial.

**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 public affairs activities**
Defined in DODI 5400.13.

**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.

**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.

**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 structures 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.

**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.

**Optional**
Those service, features, or equipment that offerors 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.

**Performance measure**
A quantitative or qualitative characterization of performance.

**Personally identifiable information**
Information which can be used to distinguish or trace an individual's identity, such as their name, SSN, biometric records, and so on, 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 on.

**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 HW and SW, 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**
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 on). These can be subscription based or free, single-use or repeated use content. Also called vlogs.

**Point of presence**
Point of presence (POP) is the physical location defined by a provider of FTS 2001 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 FTS 2001 service. A POP is the demarcation point between access services and transport services.

**Portable electronic device**
Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, PDAs, pocket PCs, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

**Private branch exchange**
Telephone switching equipment conforming to the Federal Communications Commission registration requirements for interconnection to the public switched network.

**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 IS should be aware of the various procurement approaches available for acquiring IS and services.

**Program objective memorandum**
A memorandum in prescribed format submitted to OSD 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**
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 reliable certification authority.

**Public switched network**
Any common carrier network that provides circuit switching among public users, including foreign postal telephone and telegraphs. 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 assets, they must contract for the services or establish inter-Service support agreements with Army or other Services for NEC support.

**Request for service**
A request for leased long-haul telecommunications services.

**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 proponent's mission.

**Research, development, and acquisition**
A term that includes procurement and research, development, test, and evaluation appropriations.

**Satellite communications**
Communications via satellite, including DOD use of military owned and operated SATCOM systems that use government radio frequency bands, as well as commercial SATCOM 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 SATCOM accesses. Operation of any military SATCOM terminals requires valid satellite database authorizations.

**Segment**
A defined area of obligation with functions and processes that contribute to mission accomplishment.

**Sensitive but unclassified 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 voice subscriber**
An individual, station, installation, or location having direct access into an SBU voice switch.

**Sensitive but unclassified 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 PBX or through a console.

**Service and network management**
Service and network management is managing the network and the devices connected to it. Service and network management includes 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.

**Service delivery point**
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 USG acquires access separately.

**Service due date**
The date when USG 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 C4IT capability program, with coordinated doctrine, training, organization, and material developments.

**Service level agreement**
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**
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 life cycle adages of service strategy, service design, service transition, service operation, and continual service improvement. The Army Service Management Program is being developed after the Information Technology Infrastructure Library Service Management concept model.

**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. This also includes 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.

**Smartphone**
A cellular telephone with built-in applications and internet access. Smartphones provide digital voice service as well as text messaging, email, web browsing, still and video cameras, MP3 player, video viewing and often video calling. In addition to their built-in functions, smartphones can run a myriad of applications, turning the once single-minded cell phone into a mobile computer.

**Social networking sites**
Online networking platforms that allow registered users to interact with other users for social or professional purposes. Examples include MySpace, Facebook, and LinkedIn.

**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 HW.

**Software reuse**
Licensed COTS SW 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.

**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 (such as point-to-point, data, C2) and may or may not be switched.

**Standard**
Within the context of the AEA, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. It may also establish requirements for selection, application, and design criteria of materiel.

**Standard data element**
A data element that has been coordinated through the standardization process and approved for use in DOD IS.

**Statement of Non–Availability**
A SoNA is issued by CHESS as validation that Army organizations have complied with the AR 25–1 regulation to purchase all COTS IT through CHESS; however, no viable contract vehicle was available at the time of the requirement submission. A SoNA does not constitute approval to purchase or deviate from any Army regulation or policy.

**Statistical sampling**
An administrative certification that long-distance phone calls are necessary in the interest of USG, 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.

**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.

**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 sub-installation belonging to another command, and from which it is receiving specified types of supply or other services.

**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 "ani-sochronous" 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.

**System owner**
Information system owners are responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of an information system or information. The term application owner is synonymous with system owner.

**Systems architect**
Has the integration and oversight functions for all Army IS. 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**
How a website organizes its data into categories and subcategories, sometimes displayed in a sitemap.

**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 Forms 1367 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 TDD or TDD-compatible device is used by the speech and/or hearing-impaired user community to access the Federal Relay Service. A TDD generally consists of a keyboard, display screen, and a means (via modem or direct connection) to access a telecommunications network. It is recognized that this function can be performed by a computer with SW 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 determining whether such information is being properly protected in the interest of national security (see AR 380–53).

**Telephone control officer**
An individual, appointed in writing by the installation commander, supervising management and implementation of the installation telephone system usage control program. TCOs will also be appointed within ACOMs, ASCCs, and DRUs in accordance with organization policies.

**Terminal Server Access Control System**
An authentication program used on Unix and Linux based systems, along with certain network routers. Its main function is to allow a remote access server to communicate with an authentication server to determine whether a user has the proper rights to access a network or database.

**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 SW, 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 USG 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 contractors' various POPs.

**Trunk**
A communications path connecting two switching systems (for example, PBX, 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.

**Underpinning contracts**
A contract with an external provider covering the delivery of goods and/or services that contributes to the delivery of C4IM services to customers. The terms and conditions of underpinning contracts should reflect and be reflected in the appropriate SLA 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.

**Unfinanced requirements**
Requirements that cannot be financed within the resources available.

**Unified capabilities**
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**.**

**Uniform resource locator**
A URL is the internet addressing scheme that defines the route to a document, file, or program.

**Unofficial telephone calls**
Unauthorized calls for other than official government business in support of an Army installation.

**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, or Soldiers' products in accomplishment of a designated mission.

**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.

**Vetronics**
Blending of two words "vehicle" and "electronics" and used as a technical designation in the context of military equipment and avionics.

**Video**
Pertaining to bandwidth and spectrum position of the signal that results from television scanning and is used to produce an electronic image.

**Video teleconferencing**
Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video; includes full-motion video, compressed video, and sometimes freeze (still) frame video.

**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 SW 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**
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 websites or institutional websites as communication tools. Also called blogs.

**Web server**
A website including HW and SW that includes the operating system, web SW, other SW and data, or the SW that manages web functions at a website.

**Web services**
A standardized way of integrating web-based applications using open standards over an internet protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.

**Website**
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 nonswitched service types that generally use radio (for example, mobile, cellular, packet, or satellite) as their principal transmission medium.

**Wireline**
A categorization of switched and nonswitched 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

This section contains no entries.