Army Regulation 25–1

Information Management

Army Information Technology

Headquarters
Department of the Army
Washington, DC
15 July 2019

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–1
Army Information Technology

This major revision, dated 15 July 2019—

- Provides guidance regarding information accountability and transparency (para 1–7).
- Updates responsibilities (chap 2).
- Realigns content with Office of Management and Budget Circular A–130 (chap 3).
- Structures the major tenets of information technology portfolio management planning, selection and control, funding, procurement, implementation and fielding, and oversight (paras 3–1, 3–7, 3–14, 3–18, 3–26, and 3–30, respectively).
- Adds new Department of Defense Information Network life cycle replacement planning rates and activities for both modified table of organization and equipment and table of distribution and allowances (para 3–3).
- Adds new components of the Army's Capital Planning and Investment Control process; the Army's Information Technology Investment Management approach; the Army's Information Technology Investment Resource Management System; and the Army's enterprise Information Technology governance process (chap 3).
- Establishes the Migration Implementation and Review Council chaired by the Deputy, Chief Information Officer/G–6 and the Deputy, Chief Management Officer (para 3–4).
- Updates Army enterprise architecture processes (organizations, standards, compliance assessment/certification, and waivers) (para 3–5).
- Adds Army civilian information technology management (para 3–6).
- Incorporates new Internal Use Software policy guidance in accordance with Department of Defense Financial Improvement and Audit Readiness Guidance establishing Internal Use Software as a Mission Critical Asset category, which is material to the financial statements of the Department of Defense and the Army (para 3–15).
- Expands use of the Army Information Technology Approval System as a policy compliance tool that enables the Army to respond to public law, congressionally-directed actions, and Army policy (para 3–16).
- Names the Army-Air Force wireless NexGen Blanket Purchase Agreement as the service plan for commercial mobile wireless devices (paras 3–19 and 3–30).
- Expands Army Data Management Program guidance (para 3–33).
- Provides new Armywide strategic planning policy guidance for standard Army life cycle replacement of information technology assets (para 3–40).
- Updates temporary exception to policy guidance and replaces global information grid waiver with Commercial Internet Service Provider and Network Temporary Exception to Policy waiver (para 3–41).
- Deletes telecommunications and unified capabilities guidance (formerly para 4-1a(4)).

- Deletes the Defense Information Assurance Certification and Accreditation Process, Information Assurance, Information Assurance Vulnerability Alert, Certificate of Networthiness, and other cybersecurity policies, compliance requirements, and procedures from this regulation and refers to AR 25–2 and associated cybersecurity pamphlets for the latest policy guidance (para 4–16).

- Transfers Army Portfolio Management Solution Business Rules from this regulation and places it in DA Pam 25–1–1 (formerly appendix B).

- Enhances the internal control evaluation (appendix B).

- Introduces the acronym "DODIN–A" (the Army's portion of the Department of Defense Information Network) (throughout).

- Relocates previous detailed governance and network implementation guidance, processes, and procedures from AR 25–1 to the supporting DA Pam 25–1–1 and other Army regulations and pamphlets (throughout).

- Incorporates the following Army Directives: Army Directive 2009–03 (Army Data Management), dated 30 October 2009; Army Directive 2013–02 (Network 2020 and Beyond: The Way Ahead), dated 11 March 2013; Army Directive 2013–26 (Armywide Management of Printing and Copying Devices), dated 2 December 2013; and Army Directive 2016–18 (Divesting Legacy Information Technology Hardware, Software, and Services in Support of the Army Network), dated 22 June 2016 (throughout) (hereby superseded).

Headquarters
Department of the Army
Washington, DC
15 July 2019

*Army Regulation 25–1

Effective 15 August 2019

Information Management

Army Information Technology

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 regulation establishes policies and assigns responsibilities for information management and information technology. It applies to information technology contained in both business systems and national security systems (except as noted) developed for or purchased by the Department of Army. It addresses the management of information as an Army resource, the technology supporting information requirements, and the resources supporting information technology. This regulation implements Title 40, United States Code, Subtitle III (40 USC, Subtitle III); 44 USC, Chapters 35 and 36; 10 USC 2223 and 3014; and DODD 8000.01. It establishes the Army's Chief Information Officer and the full scope of the Army Chief Information Officer's responsibilities and management processes. These processes involve strategic planning, capital planning, business process analysis and improvement, assessment of proposed systems, information resource management (to include investment strategy), performance measurements, acquisition, and training.

Applicability. This regulation 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 platform Information/Technology/Industrial Control Systems; appropriated-funded morale, welfare, and recreation support systems; nonappropriated-funded morale, welfare, and recreation support systems; and to contractor-owned/contractor-operated systems operated on behalf of the Army. During mobilization, procedures in this publication can be modified to support policy changes as necessary.

Proponent and exception authority. The proponent of this regulation is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

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

Committee management. AR 15–1 requires the proponent to justify the establishment or continuation of a committee(s), coordinate draft publications, and coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This regulation 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 regulation supersedes AR 25-1, dated 25 June 2013 and the following Army Directives (ADs): AD 2009-03, dated 30 October 2009; AD 2013-02, dated 11 March 2013; AD 2013-26, dated 2 December 2013; and AD 2016-18, dated 22 June 2016.

Contents—Continued

Contents—Continued

Appendixes

Table List

Figure List

Chapter 1
Introduction

1–1. Purpose
This regulation establishes policies and assigns responsibilities for information management (IM), data management, and Information Technology (IT), to include platform IT (PIT) and operational technology. It provides policy for the planning, budgeting, governance, acquisition, and management of Army IT, personnel, equipment, funds, IT resources and supporting infrastructure, and services. Army organizations must adhere to basic principles throughout the information resource management (IRM) process.

1–2. References and forms
See appendix A.

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

1–4. Responsibilities
Responsibilities are listed in chapter 2.

1–5. Records management (recordkeeping) requirements
The records management requirements for all record numbers, associated forms, and reports required by this regulation are addressed in the Army Records Retention Schedule-Army (RRS-A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS-A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS-A, see DA Pam 25–403 for guidance.

1–6. Overview
Army IT is defined in simple terms as the capabilities and investments that provide the combination of hardware, software, and networks that generate readiness, enable mission-command, and enhance lethality across all warfighting functions. This combination includes the development, maintenance, sustainment, and security of all communications devices, networks, systems, and associated contracts, as well as personnel costs, throughout the Army in both the Operating and Generating Forces.

a. Army information is a strategic asset that must be protected and shared with authorized users in accordance with this regulation, AR 25–2, AR 380–5 and AR 530–1.

b. Functional processes must be examined and streamlined to improve their effectiveness and reduce cost before investing in IT solutions to support and enable them.

c. All aspects of the Army network infrastructure including information systems (ISs), applications, wireless technologies, mobile communications, and platforms will be planned, designed, developed, architected, configured, acquired, managed, operated, and protected in accordance with this regulation and AR 25–2.

d. This regulation applies to IT contained in mission-command systems; intelligence systems (except as noted); weapon systems (except as noted); business systems; and, when identified, National Security Systems (NSS) developed or purchased by the DA. This regulation does not apply directly to information systems acquired under the National Intelligence Program (NIP), the Military Intelligence Program (MIP), or to the operational support of intelligence and electronic warfare systems operating in a stand-alone configuration where inclusion of integrated support would not be efficient or effective.

1–7. Information accountability and transparency
a. Recordkeeping requirements. Records created under the purview of this regulation, regardless of content or format, will be kept, at a minimum, in accordance with the retention schedules found at https://www.arims.army.mil. The U.S. Army Records Management and Declassification Agency manages and operates the Army Records Information Management System (ARIMS). ARIMS is a role-based system designed to provide authorized personnel with web-based tools and technology to manage both hardcopy and electronic Army records. Additional requirements at the state level, including statutory, legal, financial, or administrative by the authority of the state's Governor and Adjutant General, will be governed by Title 32 USC and managed in accordance with state policy. Information used in decisionmaking and business processes

is an Army-owned record (whether stored electronically or as a hard copy), and will be scheduled, maintained, and preserved in accordance with AR 25–400–2.

b. Information as a resource.

(1) Except where restricted for reasons of national security, privacy, sensitivity, or proprietary rights, personnel will manage information as a shared resource and make it available to all authorized users to accomplish their mission and functions. Army personnel must carefully plan requirements for information and supporting IT as collecting, processing, distributing, and storing information is a significant cost to the Army. The management of information resources and IT is applicable to all Army organizations.

(2) The IT and related investments will be evaluated in terms of direct support and compatibility with Army Enterprise solutions, mandates, and processes and their corresponding information requirements.

(3) The IT embedded in or integral to weapon systems, machines, special-purpose processing node, servomechanisms, training devices, or test and evaluation (T&E) systems, except for those systems with no external interface, are included in the provisions of this regulation. This regulation supports the precept that information is a strategic defense asset during peacetime and wartime, and the peacetime information infrastructure must support wartime requirements by providing information services for rapid deployment and sustainment of U.S. Armed Forces around the world.

(4) The Army's Data Strategy is directly linked to the Department of Defense's (DOD's) Data Strategy—to make data visible, accessible, understandable, trustable, and interoperable (VAUTI). The Army Information Architecture (AIA) provides the foundational guidance for achieving the VAUTI goals and supplies compliance criteria to measure progress. The Army's success relies on secure access to high-quality information: any data, any time, any place, accessible by any authorized user; limited by policy, not by technology.

1–8. Information technology governance and management by mission areas

a. Several authoritative documents direct managing IT capabilities and investments by functionally defined mission area (MA) portfolios to include DODD 8115.01, DODI 8115.02, and the Secretary of the Army (SECARMY) Memorandum, Subject: Army Information Technology Integration and Governance, dated 5 April 2017. The four MAs are: Warfighter (WMA), Business (BMA), the Army portion of the DOD portion of the Intelligence (DIMA), and Enterprise Information Environment (EIEMA). Senior leader councils within each MA provide guidance and top-level governance.

b. Mission area organization.

(1) The BMA includes all IT investments characterized as defense business systems (DBSs). The Under Secretary of the Army (USA) as Chief Management Officer (CMO) is designated the lead for the Business portfolio. The Army Business Council (ABC) provides governance for the BMA. The Office of Business Transformation (OBT) is the Headquarters, Department of the Army (HQDA) lead for the BMA, and the USA and the Army Vice Chief of Staff of the Army (VCSA) serve as the command leads.

(2) The DIMA is a DOD-level MA, with the Army portion led by the Army Deputy Chief of Staff (DCS), G–2, responsible for Army-specific intelligence IT systems and Army equities in policy, operations, and investments. The Intelligence Senior Initiatives Group (ISIG) provides governance for the DIMA. The U.S. Army Intelligence and Security Command (INSCOM) is the command lead for the DIMA.

(3) The WMA includes all IT investments related to mission-command, warfighting operations, training, and readiness and is led by the Army DCS, G–3/5/7. The Army Warfighting Integration Council (AWIC) provides governance for the WMA. The U.S. Army Training and Doctrine Command (TRADOC) is the command lead for the WMA.

(4) The EIEMA includes all IT investments that facilitate the implementation, operation, security, and enterprise services for the Army portion of the DOD Information Network (DODIN–A). The Army Enterprise Network Council (AENC) provides governance for the EIEMA. The CIO/G–6 is the designated HQDA lead and U.S. Army Cyber Command (ARCYBER) is the command lead for the EIEMA.

1–9. Information technology oversight council

In April 2017, the Acting SECARMY directed HQDA to develop a holistic approach to Army IT strategy and establish a process to provide Army senior leaders with greater situational understanding of IT programs, investments, and resources. To accomplish these goals, the acting SECARMY and Chief of Staff of the Army (CSA) designated the CIO/G–6 as lead Army IT integrator and established the Information Technology Oversight Council (ITOC), an Army (4-star level) senior review group. The ITOC oversees the activities and assessments across the four MAs to provide guidance and direction, prioritize investments, allocate resources, and resolve conflicts. The ITOC is co-chaired by the USA and VCSA and is composed of voting and advisory members.

a. ITOC mission, purpose, and functions. The ITOC mission is to oversee integration and synchronization of information technology investment management (ITIM) activities across MAs and the Joint Capabilities Integration and Development

System (JCIDS); planning, programming, budgeting, and execution (PPBE) processes; Defense Acquisition System; and Army Business Operations Management activities to ensure—

(1) A reliable and accurate picture of likely benefits and costs.

(2) Mission needs are met in the optimal manner.

(3) Solutions are delivered cost-efficiently.

(4) Investments deliver the expected benefits and risk is identified and managed.

b. To execute the ITOC's mission, the ITOC will—

(1) Review annually long term IT objectives for alignment with The Army Plan.

(2) Ensure there is an enterprise architecture that describes desired end states in DOTMLPF-P terms.

(3) Review annually programs and projects to ensure alignment to the enterprise architecture.

(4) Ensure performance of programs, projects, and DOTMLPF-P solutions are assessed continually against strategic outcomes.

(5) Review annually trends from performance assessments and direct action to address critical issues.

Chapter 2
Responsibilities

2–1. Headquarters, Department of the Army principal officials

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

a. Serve as the HQDA proponent for information requirements and associated capabilities within assigned functional areas of responsibility.

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

c. Analyze their missions and revise their mission-related and administrative work processes, as appropriate, before making significant IT investments as determined by the Defense Business Council (DBC) in support of those processes.

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

e. Use E-Gov technologies to the maximum extent practicable to promote the goal of a paper-free (or nearly paper- free) business environment within the Army.

f. Manage and oversee the records of respective functional areas to appropriately secure, maintain, and preserve them throughout their life cycle (see DA Pam 25–1–1, AR 25–400–2, DA Memo 25–51, and DA Pam 25–403 for additional responsibilities and information on the life cycle of records).

g. Identify functional requirements for Army enterprise information systems and, as required, participate in related governance and advisory board activities.

h. Establish IT portfolio management (PfM) processes for assigned MAs in order to define and justify planned IT expenditures that are consistent with DOD and Army guidance.

i. Administer a telework program for their respective organizations and subordinate elements as prescribed in DOD and HQDA policy and guidance.

j. Oversee acquisition, operation, accountability, consolidation, and disposition of self-service printing devices.

(1) Promote economies and efficiencies for printing devices used throughout the agency or command.

(2) Establish, maintain, and enforce agency or command policy and management controls to ensure efficient and effective procurement, operation, and accountability of printing devices.

(3) Direct the use of Army Computer Hardware, Enterprise Software and Solutions (CHESS) when acquiring printing devices.

(4) Designate a functional manager(s) to oversee management of printing devices and printing device acquisition, operation, accountability, consolidation, and disposition.

2–2. Under Secretary of the Army

In addition to requirements listed in paragraph 2–1, the USA, or a designated representative, will serve as the—

a. Army functional proponent of the BMA to include establishing, implementing, leading, and managing the BMA portfolio of IT systems, per AR 5–1.

b. CMO, and manage, coordinate, oversee, and synchronize the BMA's business operations, processes, and decisionmaking procedures. This includes the management and integration of IT solutions in accordance with this regulation.

(1) Assess the effectiveness and performance of those stakeholders delegated responsibility for IT PfM and assert compliance with the requirements of 40 USC 11312.

(2) Conduct an annual IT portfolio review across MAs to identify redundant investments.

(3) Provide IT investment criteria and guidance.

2–3. Assistant Secretary of the Army (Acquisition, Logistics and Technology)

In addition to requirements listed in paragraph 2–1, the CIO/G–6 and the ASA (ALT) are strategic partners in transforming warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced data management (DM) and PfM solutions. ASA (ALT) responsibilities are defined in AR 70–1, and the ASA (ALT) IT unique requirements are to—

a. Serve as the source selection authority (or delegate the source selection authority responsibility) for acquiring IT systems, working together with the CIO/G–6.

b. Direct and review command, control, communications, and intelligence systems and target acquisition systems; and direct tactical IT requiring research, development, test, and evaluation (RDT&E) efforts.

c. Execute the planning, programming, budgeting, and life cycle management necessary for the research, development, and acquisition of information systems required for strategic and tactical programs.

d. Execute the RDT&E and procurement portions of IT programs and budgets, in collaboration with the CIO/G–6.

e. Oversee the installation IT infrastructure relative to its impact on the Army industrial base in coordination with Commanding General (CG), U.S. Army Materiel Command (AMC).

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

g. Ensure project managers (PMs) and program executive offices (PEOs) successfully complete developmental interoperability assessments, comply with Army Interoperability Certification (AIC) policy and configuration management procedures, and resource adequately for systems to undergo AIC testing (see DA Pam 25–1–1).

h. Ensure PMs and PEOs design, build, test, and field internet protocol (IP)-enabled IT and NSS to efficiently use IP address space. Coordinate materiel solution, and IP address space requirements with TRADOC and ARCYBER.

i. Review and approve the Army position for acquisition category (ACAT) ID and ACAT IAM programs at each decision milestone, and before the Defense Acquisition Board or IT Acquisition Board review. This includes the review and approval of acquisition program baselines (see DODI 5000.02 for further clarification on ACAT programs, DODI 5000.75 for business system requirements and acquisition, and DODI 5000.74 for Defense Acquisition of Services).

j. Serve as the milestone decision authority (MDA) for Army ACAT IC, ACAT IAC, and, unless delegated, for ACAT II programs.

k. Serve as the Army system architect under the oversight of the CIO/G–6. Validate Army system views (SVs) and ensure programs develop SVs that are integrated with approved operational views, as prescribed by TRADOC, and approved standards views, as prescribed by the CIO/G–6. As Army system architect, ASA (ALT) will—

(1) Oversee and produce system architectures.

(2) Verify, validate, and approve system architectures.

(3) Establish processes and procedures for generating system architectures.

(4) Evaluate and ensure interoperability of all Army IT architectures.

(5) Ensure PEOs and PMs develop architectures in accordance with AR 71–9 and Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3170.01.

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

m. Ensure that materiel developers (MATDEVs) comply with software assurance, technical architecture (TA), AIC, and baseline configuration management policies and procedures.

n. Serve as the Army's system engineer and plan, develop, acquire, field, sustain, and properly dispose of equipment and services, and leverage technologies to meet current and future Army needs. Apply approved system engineering methods to ensure the integration and interoperability of all Army C4ISR programs of record.

o. Review information support plans (ISPs) to ensure MATDEVs comply with official policies and procedures associated with systems having approved net-ready or interoperability requirements. Specifically, ensure ISPs identify information needs, dependencies, and interface requirements, focusing on interoperability, supportability, and sufficiency (see para 3–19).

p. Use the Installation-Information Infrastructure Modernization Program vision, direction, and architecture to develop contract spend plans in coordination with CIO/G–6.

q. Ensure that IT procurement and acquisition policies are emphasized to all Army activities authorized to obligate funds contractually, and will support other enforcement procedures as they are developed and coordinated.

r. Ensure Army utilization of CHESS and common hardware systems (CHS) as the mandatory sources for commercial IT hardware, software, services, and tactical/operational hardware solutions consistent with the requirements of this AR.

s. Appoint, in writing, an Army Data Steward (DS).

2–4. Assistant Secretary of the Army (Civil Works)
In addition to requirements listed in paragraph 2–1, appoint, in writing, an Army DS.

2–5. Assistant Secretary of the Army (Financial Management and Comptroller)
In addition to requirements listed in paragraph 2–1, the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)) will—

a. In collaboration with the CIO/G–6, review and co-certify the Army IT budget submission. The review will consist of collaboration with the CIO/G–6 on all acquisitions and IT investments.

b. Assist the BMA lead in financial management of IT.

c. Inform all Army activities authorized to commit funds to comply with IT funding execution policy and guidance and will support other enforcement procedures as they are developed and coordinated.

d. Appoint in writing an Army DS.

2–6. Assistant Secretary of the Army (Installations, Energy and Environment)
In addition to requirements listed in paragraph 2–1, appoint, in writing, an Army DS.

2–7. Assistant Secretary of the Army (Manpower and Reserve Affairs)
In addition to requirements listed in paragraph 2–1, appoint, in writing, an Army DS.

2–8. General Counsel
In addition to requirements listed in paragraph 2–1, the Office of General Counsel will—

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

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

c. Advise on legal issues associated with IT and cyberspace operations.

2–9. Administrative Assistant to the Secretary of the Army
In addition to requirements listed in paragraph 2–1, the Administrative Assistant to the Secretary of the Army (AASA) will—

a. Serve as the Archivist of the Army, in which role AASA will designate a Senior Agency Official to oversee and review the Army records management program. Ensure that records related to matters involved in administrative or legal proceedings are retained until the staff judge advocate or legal advisor authorizes resumption of normal disposition.

b. Oversee the ARIMS, including to—

(1) Serve as the proponent for AR 25–400–2.

(2) Advise the SECARMY concerning the destruction of records in legal custody in an Army repository outside the continental United States (OCONUS) during a state of war between the United States and another nation or when hostile action (by a foreign power, terrorist agents, or public demonstrators) appears imminent in accordance with 44 USC 3311.

(3) Establish life cycle management instructions for the systematic identification, maintenance, storage, retrieval, retirement, and destruction of Army information recorded on any medium (for example, paper, microforms, and electronic records).

(4) Ensure that mission-essential records are available in a usable format; and created, maintained, used, and disposed of at the least possible cost.

(5) Preserve records needed to protect the rights and interests of the Army and its current and former members, and records that are of permanent value (see AR 25–55).

c. Develop and maintain the Army Information Collection Budget required by 44 USC 35.

d. Establish records declassification requirements in accordance with Executive Order (EO) 13526.

e. Implement the Army's Privacy Program to include:

(1) Appointing a Senior Component Official for Privacy (SCOP) who will act as the SCOP with overall responsibility for the execution of the Army Privacy Program.

(2) The SCOP will work with the CIO to ensure protection of personally identifiable information (PII) throughout the life cycle of information systems, and/or electronic collections.

f. Prescribe Armywide policies and provide program management and supervision for records management.

g. Serve as the Army’s representative to receive and resolve claims that allege Army information disseminated to the public does not comply with information quality standards issued by the Office of Management and Budget (OMB) (see also chap 3 of this publication).

h. Oversee the Army Publishing Program (APP) per AR 25–30.

i. Monitor IT for HQDA internal use. Perform all IM and IT responsibilities for HQDA as those assigned to Army command (ACOM) commanders (see para 2–33 for more information).

j. Manage and oversee the HQDA Telework Program.

2–10. Chief Information Officer/G–6

a. The CIO/G–6 synchronizes the Army's global network activities to achieve secure, seamless, interdependent global network processes and services designed to synchronize warfighter requirements with trusted, global network capabilities and services. The CIO oversees the execution of the Army signal (G–6) function. The CIO/G–6 serves as the principal focal point in HQDA for IM matters with Congress, the Government Accountability Office (GAO), OMB, other Federal agencies, DOD, Joint Staff (JS), Army organizations and commands, and other military departments, academia, and industry. The CIO/G–6 provides policy and guidance on IT systems and networks in accordance with AGO 2017–01. This includes the review and evaluation of existing Army IM and IT policies to determine their adequacy, and overseeing the implementation of DOD IT or IM-related policies or guidance. The CIO/G–6 is the BMA Champion for IT controls related to: access-controls, segregation of duties, security management, configuration management, and contingency planning. The CIO/G–6 provides oversight and coordination for the implementation of policies in accordance with the following legal and regulatory authorities—

(1) 44 USC 35 (Federal Information Security Modernization Act (FISMA)).

(2) 44 USC 3501 (Paperwork Reduction Act of 1995).

(3) 44 USC 36 (E-Government Act).

(4) 40 USC Subtitle III (Clinger-Cohen Act).

(5) 10 USC 3014 (Office of the Secretary of the Army).

(6) 10 USC 2223(b) (Information Technology: Additional Duties of Chief Information Officers).

(7) 5 USC 552 (Freedom of Information Act).

(8) 5 USC 552a (Privacy Act of 1974).

(9) OMB Circular A–130 (Managing Information as a Strategic Resource).

(10) DODD 8000.01, DODD 8115.02, DODD 5144.02.

(11) DODI 8110.01, DODI 8320.07, DODI 8330.01.

b. The CIO/G–6, as the CIO, is the principal staff assistant and advisor to SECARMY on the strategy, policy, and execution of IRM and IT for the Army and the effect of IRM and IT on warfighting capabilities. The CIO is responsible for the Army's IM plans, programs, and policies pursuant to 10 USC 3014(c)(1)(D), including but not limited to information enterprise (IE) networks and network-centric policies and concepts; command, control, communications, and computers (C4); non-intelligence space matters; and enterprise-wide integration of Army information matters. The CIO sets the strategic direction for and supervises the execution of Army policies and programs for IRM and IT, including creating network architecture and information-sharing policy, modernizing Army IT resource management processes, and ensuring the synchronization of the Army's IE. The CIO directs Army IM policies and programs, to include DODIN–A, network architecture, and information-sharing policy. The CIO also directs IRM, to include the allocation and obligation of IT capital assets in accordance with 40 USC Subtitle III, 44 USC 35, and 44 USC 36. The CIO oversees all IT resources under the provisions of the Clinger-Cohen Act (CCA). The CIO/G–6 coordinates with the USA as the Army's CMO to develop Army enterprise-wide business system architecture and policy that supports Army business operations management.

c. The CIO will—

(1) Perform the IRM function within DA, to include developing DA's IRM strategy, and developing and implementing the IRM and IT capital planning and investment control (CPIC) strategy.

(a) Promote the effective and efficient design and operation of all major IRM processes.

(b) Develop IRM and IT policies and guidance that comply with laws, regulations, and standards.

(c) Develop, coordinate, and implement an assessment process for Army IRM and IT programs, including compliance with IRM and IT policies, guidance, standards, and oversight.

(2) Establish strategic direction and guidance for the use of PPBE for IRM and IT resources.

(3) Review budget requests for all core or baseline IT NSS.

(4) Provide guidance, as appropriate, to Army Secretariat and Army Staff (ARSTAF) elements on IT and NSS.

(5) Set policy for, advise, and assist the ASA (ALT) on the acquisition of IT, Platform IT, and information resources.

(a) Ensure resources are acquired and managed in a manner that implements policies and procedures defined by the CIO. This includes processes and technologies to maximize the acquisition value of, and assess and manage the risks for, acquiring IT and Platform IT.

(b) Advise the Assistant Secretary of the Army for Installations, Energy and the Environment and the Assistant Chief of Staff for Installation Management (ACSIM) on cybersecurity plans and policies for facility-related control systems (FRCS) and energy and environmental control systems.

(6) Establish, maintain, and implement a governance process for IRM and IT issues and chair the CIO Executive Board (EB).

(7) Develop, implement, maintain, and facilitate Army IT enterprise architecture, governance policy, infrastructure, and portals. All the separate MAs have responsibility for their architecture. The EIEMA has responsibility for the infrastructure and as such has the responsibility to provide the architecture, governance policy, and infrastructure portals for those shared services that integrate all the MAs.

(8) Develop and supervise policy execution for information-sharing and security, to include providing policy and guidance for communication and information security protections, ensuring compliance with information security standards promulgated by the OMB, and reviewing and validating Army requests for technical services and support requests from the National Security Agency.

(9) Develop policies and guidance for Army cybersecurity controls, to include but not limited to, key infrastructure, identity management, common access card (CAC), and other technology programs.

(10) Identify opportunities, validate requirements, screen business cases, provide guidance on, and monitor implementation of IRM and IT capabilities and dependencies in business process initiatives and programs.

(11) Monitor, consistent with ASA (ALT)'s acquisition authorities, the performance of IRM and IT programs; evaluate the performance of those programs on the basis of applicable performance measurements, and advise the SECARMY on the continuation, modification, or termination of an IRM or IT program or project.

(12) Ensure DA has a sufficient number of trained IRM and information security personnel, and make sure those personnel meet performance requirement goals established for IRM.

(13) Assess and ensure that IRM, IT, and national security systems comply with standards of the Federal Government and DOD, and are interoperable with other relevant IRM, IT, and national security systems of the Federal Government and DOD.

(14) Coordinate with and support the CMO in the development of business systems policies that have IRM and IT effects, and coordinate with and provide input to the CMO's strategic guidance on business operations, policies, procedures, and planning documents to obtain alignment and integration with IRM and IT data strategies and directives.

(15) Manage the electromagnetic spectrum in DOD, Service, joint, national, host nation, and international spectrum management activities to ensure Army compliance with U.S. Federal spectrum regulations and international spectrum treaties.

(16) Provide Army policy, oversight, and guidance for effective, integrated, timely, information-assured, survivable, and enduring connectivity and communications abilities of the national leadership command and control (C2) governing body.

(17) Provide Army policy, oversight, and guidance on enterprise-wide IT architecture and requirements, and assist the ASA (ALT) with the effective integration of positioning, navigation, and timing capabilities into Army platforms, weapons systems, and national security systems.

(18) Serve as the Army's lead agent for DODIN–A to enhance the ability to reconcile current to future force DODIN–A capabilities, improve business agility, and achieve warfighter decision superiority and support information-sharing with all Unified Action Partners. The CIO is the single authority accountable to—

(a) Deliver structured, controlled, repeatable, and measurable processes that drive accountability and compliance for the management of the Army's IT enterprise, aligned to a strategic management plan.

(b) Ensure secure DODIN–A capabilities and services to Army leadership and warfighters.

(c) Enable agile responses to rapidly changing operational requirements for Army and Joint missions.

(19) Direct IM function within the DA, to include—

(a) Develop the DA's IM strategy, policies, and guidance that comply with applicable laws, regulations, and standards.

(b) Oversee IM and IT resources PPBE.

(c) Develop and implement the IM and IT CPIC strategy, including the design and operation of all major information resources management processes.

(d) Develop, coordinate, and implement an assessment process for Army IM programs, to include compliance with IM policies, guidance, standards, and oversight.

(20) Serve as the HQDA lead for the IT-based capabilities and investments EIEMA. Validate, approve, prioritize, and synchronize all DODIN–A capabilities, experimentation, concepts, and architecture development efforts for the EIEMA. Provide guidance and direction, prioritize investment, and allocate resources to address current and future EIEMA IT requirements, capabilities, and investments for all Army IT systems (including formal Programs of Record and non-standard IT programs and/or systems).

(21) Serve as the authority to receive, resolve, and address appeal requests on quality, objectivity, and integrity of Army information disseminated to the public in accordance with Freedom of Information Act (FOIA) and Privacy Act programs.

(22) Establish, maintain, facilitate, and guide the implementation of the Armywide EA.

(23) Prescribe Army strategy, policy, and PfM for Army bandwidth capabilities and activities.

(24) Serve as member of the Federal CIO Council and the DOD–CIO EB.

(25) Develop, promulgate, and oversee compliance with cybersecurity policy.

(26) Prepare, coordinate, and co-certify the IT Budget in conjunction with the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)).

(27) Represent the Army on the Committee on National Security Systems.

(28) Provide policy, guidance, and set standards for the Armywide implementation and modernization of the DODIN–A to include support to unified action partners in a mission partner environment (MPE).

(29) Prescribe Army IE strategy, policy, PfM, architecture, and strategic communications that result in effective IT investments Armywide.

(30) Participate as a core member of the Army Business Council in the role of standards provider in support of the business enterprise architecture (BEA) and architecture products for integration into the Army enterprise architecture (AEA).

(31) Lead the AENC to establish strategic enterprise architecture (EA) guidance and direction, approve architecture initiatives, conduct in-process reviews (IPRs), direct trade-offs, shape the program objective memorandum (POM), and approve EA release and delivery.

(32) Co-Chair, with the ASA (FM&C), the Resource Integration Group (RIG) through which leadership works with the CIO to plan the overall portfolio of IT resources that achieve program and business objectives.

(33) Manage the Army Information Technology Approval System (ITAS) under the Army Request for Information Technology program.

(34) Develop and maintain the Army Baseline IT Service Catalog in support of the service catalog strategy.

(35) Prescribe server and application consolidation, collaboration tools, best business practices, and web services supporting the DODIN–A. Also, prescribe the configuration of web applications across the Army.

(36) Establish, in coordination with ARCYBER, IT Service Management policy and strategy.

(37) Provide policy and guidance to develop and maintain a competent military and civilian IT and cybersecurity workforce to support the Army's mission.

(a) Serve as the functional chief for Information Technology Management (ITM) Career Program (CP)-34 identifying talent management gaps and competencies that are critical to the life cycle management and readiness of the Army's IT and cybersecurity professionals.

(b) Provide the policy, oversight, and management of CP–34 professionals in accordance with AR 690–950.

(c) Monitor the operations and structure of the military and civilian personnel management systems to address the Army's requirements for qualified ITM civilian personnel, and establish ITM career development plans, programs, and objectives. (Further information is available in DA Pam 25–1–1, AR 690–950, AR 350–1, and at http://go.usa.gov/capzb.)

(38) Coordinate with the ACSIM to annually update the command, control, communication, and computers for information management (C4IM) services list and measurements contained in the Army's IT Metrics Program into the installation status report-services (ISR–S) process, radio frequency measures into ISR-mission capacity (ISR–MC) process, and to update ISR-infrastructure (ISR–I) inspection materials for information systems facilities.

(39) Prescribe Army IT PfM policy and oversee implementation of MA portfolios to ensure doctrine, organizations, training, materiel, leadership and education, personnel, facilities–policy (DOTMLPF–P) solutions are aligned with Army enterprise capabilities, and performance management tenants.

(40) Serve as the lead for managing Army participation in the DOD Enterprise Software Initiative (ESI).

(41) In coordination with ARCYBER, direct research into new IT technologies and training venues that deliver value across the enterprise.

(42) Serve as functional proponent for the Army enterprise portals (Army Knowledge Online (AKO), enterprise collaboration services).

(43) Serve as the Chief IT Architect of the Army and the functional proponent for the AEA, to include establishing, implementing, facilitating, maintaining, guiding, leading, and managing the AEA and the following:

(a) Develop, maintain, and publish the Army's authoritative IT and network interoperability standards.

(b) Establish the Army's processes and procedures for the development of IT architectures. Each MA is defined in the AEA and is responsible for the architecture subject to that MA. The EIEMA has an integration responsibility to provide shared services that span across MAs as the "shared services systems integrator for the Army."

(c) Integrate the Army's IT architectures.

(d) Certify compliance of Army IT architectures with IT and network interoperability standards.

(e) Establish and lead an Architecture Configuration Control Team to define and execute a process that will approve, maintain, and publish changes to IT architecture products.

(f) Develop Army architecture data standards (see the definition for IT Architecture in glossary).

(44) Establish and oversee the Army Data Management Program (ADMP).

(a) Appoint in writing the Army Chief Data Officer (CDO).

(b) Oversee nominations of Army Data Stewards.

(c) Confirm by letter the appointment of Army Data Stewards nominated by the Assistant Secretaries of the Army (ASAs), Deputy Chiefs of Staff (DCSs), ACOMs, and other areas as identified by the CDO.

(d) Sponsor the Army Data Board (ADB).

(e) Ensure that data and electronic content comply with provisions of Section 508 of the Rehabilitation Act Amendments of 1998.

(45) Provide oversight and direction for network-centric concepts and management, to include the Army's Risk Management Framework (RMF) Program.

(46) Serve as the functional proponent and primary interface with the Defense Information Systems Agency (DISA) on existing and emerging DOD enterprise services such as email, data center consolidation, collaboration, and unified communications.

(47) Lead development of a comprehensive Army network modernization strategy--employ a network architecture that synchronizes activities and incorporates an identification and reconciliation process for innovative or emerging capabilities.

d. The CIO ensures that the Army signal (G–6) function is fulfilled by providing advice to the SECARMY for ITM, IT, and communications issues and their effect on warfighting capabilities, including ensuring network support to current and future force capabilities. The senior military official within the Office of the CIO serves as the principal ARSTAF advisor to the CSA for IRM, IT, and communications issues, and their effect on warfighting capabilities. The Army DCS, G–6 oversees information management and signal operations, network and communications security, force structure, interoperability, equipping, and employing signal forces. The CIO/G–6, in the role of DCS, G–6, will—

(1) Advise the SECARMY and CSA on information and signal operations, force structure, equipping and employment of signal forces, advising on signal training, and on network and communications security. Assess the impacts to the warfighter of IRM- and IT-related strategy, policies, plans, services, and programs. Advocate for and monitor the implementation of IRM and IT requirements on behalf of the warfighter.

(2) Develop and execute the Army Network Strategy and monitor implementation of the Army Enterprise Network.

(3) Formulate and defend resources necessary for the Army to provide command, control, communications, computers, and IT capabilities in support of the warfighter; translate IRM, IT, and information resources requirements for warfighters into dollars; and provide necessary operational perspective.

(4) Execute the Army's data and information-sharing strategy.

(5) Provide policy, guidance, and resources for the Army's communication needs for all network layers, including top secret and higher levels of security, as well as access to coalition networks to support information-sharing with Army mission partners.

(6) Implement CIO policy and guidance for Army cybersecurity activities.

(7) Conduct oversight of Armywide activities in command, control, communications, and computers; satellite-enabled information networks; enterprise integration of Army information and IT; and IRM-related aspects of business continuity, disaster recovery, and contingency support.

(8) Supervise the implementation of other Armywide communications programs, including those non-intelligence space and joint satellite communications programs and projects, and visual information.

(9) As the functional proponent for the delivery of DODIN–A, provide Army senior leaders with situational awareness of Army IT programs, investments, and resources. As the integrator for HQDA, the CIO/G–6 will—

(a) Improve SECARMY and CSA situational understanding of Army IT across the four IT-based capabilities and investment MAs: WMA, BMA, EIEMA, and the Army portion of the DIMA.

(b) Lead an integrated process team (IPT) with the MA leaders for the development of a holistic Army IT strategy.

(c) Serve as the Secretariat for the HQDA ITOC.

(10) Serve as the executive sponsor of the Army Enterprise Service Management (AESM) process. Coordinate with key stakeholders for the development and execution of AESM via an Army IT Service Management Office (ITSMO) per guidance in the DOD Enterprise Service Management Framework (DESMF).

(11) Monitor the implementation and sustainment of enterprise IT services to verify their fit for purpose, security, and affordability.

(12) Serve as the HQDA representative on the MPE Executive Steering Committee in accordance with CJCSI 5128.01, and contribute to the development of policy, strategic vision, and oversight of the MPE implementation in coordination with Chairman, Joint Chiefs of Staff and other MPE stakeholders.

(13) Evaluate all proposed network, cybersecurity, communications security (COMSEC) and application interoperability agreements, standards and tactics, techniques, and procedures (TTP) for compliance with appropriate joint, interagency,

intergovernmental, and multinational (JIIM) network standards, the MPE Joint Membership and Exiting Instructions, and Army Computing Environments, prior to ratification. Ensure all stakeholders are included prior to approving the proposed standard, TTP, or policy.

(14) Coordinate with the U.S. Cyber Command (USCYBERCOM), DOD–CIO, ARCYBER, and the DCS, G–3/5/7 for the development of execution orders as required.

(15) Oversee the implementation and enforcement of DODIN–A global network requirements and operations to achieve standardization, compatibility, security, interoperability, and fiscal discipline of IRM and IT services supporting the warfighter.

(16) Serve as senior authority for telecommunications programs and committees (see AR 25–13 for more information).

(17) Serve as senior authority for Army visual information (VI) and multimedia products as defined in chapter 4 of this regulation and in DA Pam 25–91. The CIO/G–6 VI management office manages the Army's VI activities.

(18) Serve as the proponent for the information systems supporting (C4) and IT programs, to include, but not limited to—

(a) Serve as the Army focal point for IT system issues (to include NSS). Receive, coordinate, and integrate these issues, ensuring the integration of systems-development efforts with cross functional or technical lines.

(b) Participate in and provide representation for the PPBE process decision group, and exercise centralized oversight of IT expenditures for all appropriations, including formulating and defending the resources necessary to provide command, control, communication, and computers for information technology (C4IT) to the warfighter.

(c) Develop, coordinate, and manage the IT capital planning and investment management program.

(d) Recommend and coordinate new standards and ensure IT system conformance to the approved DOD IT Standards Registry (DISR), coordinate and support the priorities within IT for IS development-related activities, and secure resource support.

(e) Coordinate resource requirements for IT support activities.

(f) Coordinate IT requirements relevant to Army continuity of operations (COOP) plans and systems that support survival, recovery, and reconstitution; and ensure essential information services in support of DA COOP are available to alternate sites of HQDA agencies, ACOMs, and installations.

(g) Prescribe, in conjunction with the Office of the Administrative Assistant to the Secretary of the Army, records management requirements in the life cycle of information systems, beginning at the initial milestone.

(h) Collaborate with the DCS, G–8 in the development of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) positions presented at Functional Capabilities Boards, the Joint Capability Board, and the Joint Requirements Oversight Council.

(19) Manage, plan, and program for the Army Spectrum Management Program (AR 5–12).

(20) Ensure Army interoperability processes are structured to allow seamless transition for Joint Interoperability Certification. This includes, but is not limited to—

(a) Represent Army interests in Joint, DOD, and Army technical interoperability forums.

(b) Expand interoperability certification process to cover all capability areas in accordance with Joint/AIC criteria. Incrementally establish memorandums of agreement (MOAs) with functional proponents laying out AIC portfolio requirements and strategies.

(c) Establish and manage the Army's information support plan (ISP) review and approval process. Guide programs through the ISP associated processes to obtain Army and/or Joint Interoperability Certification. Approve all Army ISPs.

(d) Establish federated net-centric sites (FaNS) criteria for accreditation by the Office of the CIO/G–6.

(e) Coordinate with TRADOC and ASA (ALT) in the development and review of all mission threads.

(f) Prescribe guidance for the Army's use of the Department of Defense Research and Engineering Network (DREN).

(g) Prescribe Army IP address policy for IP address management and usage.

(h) Validate IT and NSS requirements through the review of data on the capabilities and Army Requirements Oversight Council Management System.

(i) Ensure that IT infrastructure requirements to sustain interoperability requirements are identified in the Army's budget submissions.

(j) Ensure the compatibility and interoperability of IT and NSS with Joint, unified, combined, Federal Government, and other Army systems as required.

(k) Provide the Army Coalition Interoperability Assurance & Validation (CIAV) Team for direct engagement, in partnership with the Joint Staff Joint Interoperability Test Command (JITC), with COCOMs to resolve process, training, and technical capability gaps hampering efficient information exchange with JIIM mission partners.

(21) Ensure requisite networks, to include the Combine Federated Battle Laboratories (CFBL) network, are compliant with Army requirements to conduct distributed assurance and validation events routinely with our CIAV mission partners.

(22) Establish, in coordination with ARCYBER, the vision, direction, and architecture of the Installation-Information Infrastructure Modernization Program and the Army Computing Infrastructure.

(23) Provide Army procurement guidance for the Army Non-Tactical Trunked Radio Land Mobile Radio program to ensure alignment with Homeland Security Presidential Directive 5 (HSPD 5).

(24) Serve as Strategic Management Process champion to ensure the alignment of the CIO/G–6 Strategic Management Plan.

(25) Serve as the Army's lead for the EIEMA to support the DOD EIEMA lead, and ensure enterprise information environment efforts are traceable to and fully enable the required capabilities for the Warfighting and Business MAs.

(26) Appoint in writing an Army DS.

2–11. Chief of Public Affairs

In addition to requirements listed in paragraph 2–1, the Chief of Public Affairs will—

a. Establish public affairs policy and regulatory guidance for release of Army VI products to the public.

b. Establish public affairs policy for oversight and management of content on Army public websites.

2–12. Chief, National Guard Bureau

The CNGB, directly or by delegation to the Director, Army National Guard (DARNG), will have the same responsibilities as those specified in paragraphs 2–21*a*, 2–21*b*, and 2–33. In addition to these responsibilities, the CNGB will ensure the DARNG will support CNGB responsibilities as they relate to DODD 5105.83 and will—

a. Serve as the lead agent for GuardNet.

b. Oversee organizations that operate and maintain GuardNet, the Army National Guard's (ARNG's) extension of the DODIN, providing DODIN–A services from the States, territories, and the District of Columbia (collectively referred to as States) that comprise the ARNG to the DODIN–A infrastructure. This includes, but is not limited to—

(1) Plan, program, and provide support capabilities and resources to the National Guard Bureau (NGB) and Joint Forces Headquarters (JFHQ) - State IT and IM service and support requirements.

(2) Execute technical authority and configuration management authority for GuardNet, systems, and functional processing centers, providing guidelines and direction for GuardNet IT configuration management as prescribed by ARCYBER.

(3) Execute all infrastructure-management activities, policies, processes, procedures, and protocols for the management of networks, telecommunications, facilities, data storage, IT and IM services continuity, and distributed computing operating within GuardNet.

(4) Provide technical and administrative guidance, direction, and resources to the JFHQ–States who assume direct responsibility for communications and IT and IM services operating within their State boundaries.

(5) Execute Army National Guard leases of communications, capabilities, and services, and ensure that such services conform to NGB, CIO/G–6, and ARCYBER guidance in collaboration with the JFHQ–States where applicable.

(6) Formulate, manage, support, and approve ARNG military communications as well as IT and IM exchange agreements between the U.S. Army, other Joint Services, JFHQ–States, and State government and first- response agencies in collaboration with the JFHQ–States, where applicable.

(7) Manage GuardNet-specific, system-to-system interfaces between the States and the Department of the Army in collaboration with the JFHQ–States, where applicable, and as prescribed by ARCYBER.

(8) Collaborate with the JFHQ–States or the National Capital Region (NCR) directors of information management who are responsible for Network Enterprise Center (NEC)-like responsibilities, as outlined in this regulation, for their respective States or the NCR.

(9) Manage NGB-specific Internet domains and the assignment of sub-domains requested through ARNG on behalf of NGB and supported organizations as prescribed by ARCYBER.

c. Serve as a member of the ITOC and provide representation to any associated integrated processing teams, working groups and committees.

2–13. Director of the Army Staff

The Director of the Army Staff will accomplish all the IT responsibilities assigned to the principal HQDA officials for the Office of the Chief of Staff, Army (see para 2–1 for more information).

2–14. Deputy Chief of Staff, G–1

In addition to the duties listed in paragraph 2–1, the DCS, G–1 will-

a. Establish and oversee the implementation of DOD policy to reduce social security number usage within DOD.

b. Appoint in writing an Army DS.

c. Review ISPs to ensure the Army is acquiring IT that meets approved mission requirements of the Human Resources community.

2–15. Deputy Chief of Staff, G–2

The CIO/G–6 and the DCS, G–2 are strategic partners in transforming warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced solutions. In addition to requirements listed in paragraph 2–1, the DCS, G–2 will—

a. Inform the CIO/G–6 of investments in the intelligence community for purposes of developing Armywide investment strategies.

b. Manage and oversee NIP-funded and MIP-funded IT efforts and other intelligence programs.

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

d. Serve as the HQDA functional proponent lead for the IT-based capabilities and investments DIMA. Establish, implement, lead, and manage the DIMA portfolio of IT systems. Validate, approve, prioritize, and synchronize all DODIN–A capabilities, experimentation, concepts, and architecture development efforts for the DIMA. Provide guidance and direction, prioritize investment, and allocate resources to address current and future DIMA IT requirements, capabilities, and investments for all Army IT systems (including formal Programs of Record and non-standard IT programs and/or systems). Lead the Intelligence Senior Initiative Group.

e. Oversee Army Intelligence Special Access Programs (SAPs) and serve as the intelligence SAP Army Staff proponent.

f. Serve as Army lead for the sensitive compartmented information (SCI) information assurance (IA) program, IP policy, and procedures pertaining to information systems processing intelligence information.

g. Serve as the Army's representative to the intelligence segment led by the Under Secretary of Defense for Intelligence and National Intelligence Technology Infrastructure. Coordinate with Army segment and sub-segment leads as appropriate to ensure alignment with the Army's IT PfM efforts.

h. Ensure and manage Armywide compliance with FISMA for Joint Worldwide Intelligence Communication System (JWICS) and non-cryptologic SCI systems.

i. Provide C4-related and IT-related combat and materiel development requirements, and update data input for supporting intelligence, electronic warfare, and security operations to TRADOC, AMC, and the U.S. Army Forces Command (FORSCOM).

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

k. Provide functional support to the C4IT PEOs and PMs as designated by the Army acquisition executive.

l. Coordinate the C4 and IT system design of proponent systems with TRADOC.

m. Collaborate with and support the CG, Army Cyber Command mission to operate, maintain, and defend the DODIN–A, and conduct cyberspace operations.

n. Collaborate with and support the CG, INSCOM for the execution of the Ground Intelligence Support Activity, which serves as the Army service provider for SCI systems, the single Army JWICS IP registration authority, and the responsible organization for implementing Army JWICS IP policy.

o. Review ISPs to ensure the Army is acquiring IT that meets approved mission requirements of the Intelligence Community.

p. Appoint in writing an Army DS.

2–16. Deputy Chief of Staff, G–3/5/7

The CIO/G–6 and the DCS, G–3/5/7 are strategic partners in transforming warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced solutions. In addition to requirements listed in paragraph 2–1, the DCS, G–3/5/7 will—

a. Synchronize and prioritize the Army's DODIN–A network requirements for delivering an interoperable, affordable, versatile, and effective set of mission-command and network solutions that meet current, emerging, and future needs of operational commanders. Approve IT requirements in accordance with AGO 2017–01.

b. Develop, validate, and establish priorities for strategic, theater, and tactical information requirements for strategic C2 programs, and assist the BMA lead in DODIN–A implementation.

c. Align the Army's requirements for the network with operational needs. Oversee the planning for mid- and long-range force development. Approve operational architectures and requirements. Set readiness goals and synchronize across the ACOMs.

d. Prioritize requirements for all network-related, operational needs statements or Joint urgent operational needs statement actions and new procurements, to ensure that they fit within the Army's enterprise network as a part of the DODIN–A and base communications governance construct.

e. Validate and establish priorities for operational information requirements at HQDA.

(1) Determine and publish Army architecture priorities in accordance with the Army Campaign Plan (ACP).

(2) Develop current and future views of the force structure of the Army to include the National Guard and Army Reserve to meet the requirements of the Army Enterprise.

f. Validate tactical VI combat camera (COMCAM) documentation support for Army operational planning documents for contingencies, emergencies, training exercises, and other peacetime engagements.

g. Lead development of a comprehensive Army network modernization strategy, employing a network architecture that synchronizes activities and incorporates an identification and reconciliation process for innovative or emerging capabilities.

h. Serve as the HQDA MA functional lead for the WMA IT-based capabilities and investments and operational activities and processes.

(1) Establish, implement, lead, and manage the WMA portfolio of IT systems.

(2) Validate, approve, prioritize, and synchronize all DODIN–A capabilities, experimentation, concepts, and architecture development efforts for the WMA.

(3) Provide guidance and direction, prioritize investment, and allocate resources to address current and future WMA IT requirements, capabilities, and investments for all Army IT systems (including formal Programs of Record and non-standard IT programs and/or systems).

(4) Develop a single, integrated WMA EA to support WMA PfM.

i. Serve as the Army's MA lead for the DODIN–A /Mission-Command General Officer Steering Committee (GOSC).

j. Direct formal release of the CIO/G–6 interoperability baseline to the field when necessary to ensure restriction of version proliferation that impacts interoperability.

k. Reviews ISPs to verify the acquisition of approved solutions and provide recommendations to synchronize integration of new solutions into the Army inventory.

l. Serve as the Army's proponent and/or oversight authority for Army JIIM interoperability activities.

(1) Develop, review, and distribute Army JIIM interoperability policy, strategies, priorities, and objectives throughout the Army. Ensure coordination with the CIO/G–6 on all IT-related content.

(2) As the single ratification authority within the Army for North Atlantic Treaty Organization standardized agreements and for American, British, Canadian, and Australian Armies' Program standards, ensure coordination with the CIO/G–6 on all IT-related actions prior to final ratification.

m. Review ISPs to ensure the Army is acquiring information technology that meets approved mission requirements of the Logistics community.

n. Plan and program IT resources to support the installations' common-use IT requirements, as required by the CIO and ARCYBER.

o. Appoint in writing an Army DS for their organization.

2–17. Deputy Chief of Staff, G–4

In addition to requirements listed in paragraph 2–1, the DCS, G–4 will—

a. Appoint in writing an Army DS.

b. Review ISPs to ensure the army is acquiring IT that meets approved mission requirements of the Logistics Community.

2–18. Deputy Chief of Staff, G–8

In addition to requirements listed in paragraph 2–1, the DCS, G–8 will—

a. Validate and revalidate requirements for all network-related, operational needs statements or Joint urgent operational needs statement actions and new procurements, to ensure that they fit within the Army's enterprise network as a part of the DODIN–A and base communications governance construct.

b. Review ISPs to validate programs are acquiring capabilities in accordance with their funded Acquisition Program Baseline.

c. Appoint in writing an Army DS.

2–19. Chief, Army Reserve

The Chief, Army Reserve will have the same responsibilities as specified in paragraphs 2–21, 2–21*a*, and 2–33*c*. In addition to these responsibilities, the Chief, Army Reserve will—

a. Manage the "USAR.army.mil" Internet domain and the assignment of sub-domains requested by other USAR organizations on Army Reserve Network (ARNet) II.

b. Oversee organizations that operate and maintain portions of the ARNet II (that is, the systems and networks that constitute the ARNet II).

c. Serve as a member of the ITOC and provide representation to any associated integrated processing teams, working groups and committees.

d. Administer command-level IT performance measurements as prescribed by the CIO and CMO (see DA Pam 25–1–1 for more information) and ensure installations complete quarterly and annual ISR reporting.

2–20. The Surgeon General/Commanding General, U.S. Army Medical Command

In addition to requirements listed in paragraph 2–33, The Surgeon General/CG, MEDCOM will—

a. Provide IT-related combat and materiel development requirements, and data supporting military medical operations, to TRADOC, AMC, FORSCOM, and CIO/G–6.

b. Enforce compliance with 2 USC Subtitle F (The Health Insurance Portability and Accountability Act (HIPAA) of 1996) for the protection of health information, to include specific security measures required to support HIPAA standards.

c. Provide functional oversight and management for medical control systems.

d. Appoint in writing an Army DS.

2–21. Assistant Chief of Staff for Installation Management

In addition to requirements listed in paragraph 2–1, the ACSIM will—

a. Provide installation-support solutions to meet installation IT service and support requirements as prescribed by the CIO and ARCYBER. Assist the BMA lead with installation, energy, and environment IT implementation.

b. Implement the VI program in accordance with this regulation as prescribed by the CIO/G–6. The senior VI officials will directly oversee, coordinate, and represent ACSIM on all VI-related programs and activities.

c. Provide functional oversight and management for FRCS and Supervisory Control and Data Acquisition Systems.

d. Integrate the C4IM services list and measurements contained in the Army's IT Metrics Program into the Installation Status Report-Services (ISR–S) and common levels of support process.

e. Coordinate with the CIO/G–6, ARCYBER, and other stakeholders to annually update the C4IM services list and measurements contained in the Army's IT Metrics Program into the ISR–S process, radio frequency measures into ISR–MC process, and to update ISR–I inspection materials.

f. Appoint in writing an Army DS.

2–22. The Judge Advocate General

In addition to requirements listed in paragraph 2–1, the Judge Advocate General will—

a. Provide IT-related combat and materiel development plans and data supporting military legal operations to Army organizations.

b. Oversee legal technology support provided by the CIO and ARCYBER for rapid, responsive, and continuous provision of military justice, claims, legal assistance, National Security law, and other legal support to the warfighter, commander, and staff across the full spectrum of military engagement.

2–23. Commanding General, U.S. Army Forces Command

In addition to requirements listed in paragraph 2–33, the CG, FORSCOM will—

a. Coordinate with the appropriate COMCAM organizations for current operations and training exercises.

b. Appoint in writing an Army DS.

2–24. Commanding General, U.S. Army Training and Doctrine Command

In addition to requirements listed in paragraph 2–33, the CG, TRADOC will—

a. In coordination with ARCYBER, formulate IM and IT doctrine for the Army.

b. Serve as the Army Operational Architect.

(1) Establish the processes and procedures to develop the operational architectures of the Operating Force.

(2) Support warfighting concept refinement to include: development of WMA solutions, war gaming, experimentation, studies, analysis, modeling, simulation, and network assessment.

(3) Serve as the Army Architecture Data Steward.

(4) Develop and maintain the repository of authoritative architecture products.

(5) Oversee and produce Army operational architectures.

(6) Verify, validate, and approve Army operational architectures.

(7) Verify, validate, and approve all JCIDS architectures for all MAs.

c. Support the Army DCS, G–3/5/7 in its role as the HQDA lead for the WMA IT-based capabilities and investments. As the command lead for the development of an integrated Army IT strategy, assist the Army DCS, G–3/5/7 to account for total investments for Army WMA IT systems (to include Programs of Record and non-standard IT programs and /or IT systems not managed under formal acquisition control).

d. Determine commercial, off-the-shelf (COTS), IT requirements by organization and echelon, and ensure that IT solutions for warfighting requirements include an integrated user-training program, simulator, or simulations development plan as appropriate.

e. Provide electromagnetic spectrum impact consideration in the formulation of Army countermeasures, concepts, and doctrine.

f. Establish doctrine for IP addressing and use of IP-enabled systems and equipment for all levels of deployment and usage. Develop programs of instruction and train students on TTPs associated with using IP-enabled systems in coordination with ARCYBER.

g. Incorporate records management training in functional and major operating system-producing courses.

h. Ensure that the IT support for accession and recruiting missions reflects an enterprise approach.

i. Support the Army's configuration control process for the Joint messaging standards implemented in the systems for which they are responsible. Provide support, as required, to the Army's representative to joint configuration control boards that configuration manage those same joint messaging standards (see DA Pam 25–1–1 for more information).

j. Support Network Integration Evaluation efforts as part of the Army's agile capabilities life cycle process and decisionmaking on issues of network development and sustainment.

k. Provide a model and simulation-supported analysis on priority network questions of the DODIN–A GOSC. Analysis will be coordinated between all Army organizations performing formal modeling and simulation of components that comprise the Army's DODIN–A network enterprise.

l. Review ISPs to determine if solutions being acquired meet approved warfighter requirements (see para 3–19).

m. Develop operational architecture views and products for the systems being acquired under the JCIDS to comply with the JCIDS Manual, ASA (ALT) system architectures and CIO/G–6 technical architecture views and products.

n. Develop all mission threads associated with the Operating Force in coordination with ASA (ALT) and CIO/G–6.

o. Appoint in writing an Army DS.

2–25. Commanding General, U.S. Army Materiel Command

In addition to requirements listed in paragraph 2–33, the CG, AMC will—

a. Provide functional support to the PEOs and PMs as designated by the Army acquisition executive.

b. Assist the CIO/G–6 in the preparation, maintenance, registration, and promulgation of the AEA.

c. Validate information system technical requirements and associated cost estimates for all Army military construction (MILCON) projects, except for those projects specifically designated to U.S. Army FORSCOM.

d. Perform system engineering for the sustainment battlefield functional area of the command, control, and subordinate systems.

e. Resource and execute AIC test activities as directed by and on behalf of the CIO/G–6.

f. Resource and execute configuration management processes, as directed by the CIO/G–6, to maintain configuration control and data integrity of Army systems during the AIC test certification process, and to maintain interoperability over the Army fielded baselines.

g. Support the CIO/G–6 in the execution of the AIC test process by providing test and configuration management personnel to execute AIC test events in compliance with CIO/G–6 policy and procedures.

h. Provide assistance to the CIO/G–6 with the synchronization of the FaNS AIC distributed environment, to include—

(1) Control and replicate the fielded and certified baseline for distribution.

(2) Provide system-of-systems (SoS) engineering integration support.

(3) Act as the central control node to synchronize the AIC distribution environment.

(4) Review ISPs to identify deficiencies in planned interoperability testing and provide recommendations to improve system integration into the Army's inventory of operational software (see para 3–19).

i. Ensure execution of IT contracts in accordance with CIO/G–6 guidance, to include—

(1) Ensure all software development contracts contain records management requirements. For examples of records management contract language, see http://www.archives.gov/.

(2) Ensure all contracts are compliant with Section 508 of the Rehabilitation Act Amendments of 1998.

(3) Ensure all software development contracts are approved by the CIO/G–6.

(4) Ensure all IT hardware acquisitions are Electronic Product Environmental Assessment Tool registered and ENERGY STAR® qualified, in accordance with EO 13514; and that they meet the Environmental Protection Agency ENERGY STAR® and green requirements for energy efficiency per EO 12845.

j. Administer command-level IT performance measurements as prescribed by the CIO and CMO (see DA Pam 25–1–1 for more information) and ensure installations complete quarterly and annual ISR reporting.

k. Appoint in writing an Army DS.

2–26. Commanding General, U.S. Army Special Operations Command

In addition to requirements listed in paragraph 2–33, the CG, USASOC will—

a. Comply with the USSOCOM direction for management of information resources within the special operations forces IE, as an Army component command under the operational control of USSOCOM.

b. Comply with USSOCOM direction for operational, administrative, and technical control of IT resources funded, developed, or procured through Major Force Program 11 funds.

2–27. Commander, U.S. Army Cyber Command

In addition to requirements listed in paragraph 2–33, the CG, ARCYBER will conduct cyberspace operations, including—

a. Exercise a single C2 authority for all collateral top secret and below DODIN operations in accordance with Army, Joint, and DOD regulations.

b. Serve as the primary Army service component command (ASCC) headquarters responsible for conducting cyberspace operations (offensive, defensive, and stability cyberspace operations) within the DODIN–A as directed and authorized on behalf of the Commander, USSTRATCOM or the Commander, USCYBERCOM. Organize, train, educate, man, equip, fund, administer, deploy, and sustain Army cyberspace forces to conduct cyberspace operations. Serve as the single authority for the engineering, operation, management, maintenance, and defense of the DODIN–A, including—

(1) Prescribe all common-user IT services and capabilities, in accordance with the holistic Army IT strategy and as approved by the ITOC.

(2) With the exception of JWICS, serve as the single authority to implement Army IP policy, conduct Army IP registration, and manage Army IP address space.

(3) Prescribe "army.mil" and "army.smil.mil" internet domains and the assignment of sub-domains requested by other Army organizations.

(4) Manage Army IT network and system capabilities to achieve survival, recovery, and reconstitution for COOP support requirements in accordance with AR 525–27.

(5) Execute Army Cybersecurity Service Provider (CSSP) requirements to include incident, event, and problem management, in accordance with DODI 8530.01. Serve as the Army's primary general service Cybersecurity Service Provider (CSSP) for the DODIN–A, and execute Army CSSP responsibilities in accordance with DODI 8530.01. This includes incident, event, and problem management; executing, monitoring, and managing cybersecurity services for Army-controlled networks; and coordinating and monitoring CSSP support for networks supported by Army forces, or in which the Army has cybersecurity responsibilities but are not under direct Army control.

(6) Comply with CIO/G–6 AEA requirements by registering all systems in the AEA architecture repository Army Capabilities and Architecture Development and Integration Environment (ArCADIE) for integration with other components of the AEA.

c. Oversee and report threats to the DODIN–A, and as required to other DOD agencies and their enabling technologies.

d. Support the Army EIEMA as the command lead for the development of an integrated Army IT strategy. Assist the CIO/G–6 to account for total investments for all IT systems, to include Programs of Record and non-standard programs and /or systems not managed under formal acquisition control.

e. Operate, maintain, and secure the DODIN–A across all theaters, on all Army installations, and on Joint Bases that have a DODIN–A presence, to include—

(1) Provide quality common-user IM and IT baseline services to Army organizations at the highest possible level, commensurate with resources as defined in the approved services list.

(2) Provide quality mission level and enhanced IM and IT services to installation customers on a reimbursable basis, as documented in the approved service level agreements (SLAs).

(3) Oversee shared and common-user IT systems within their assigned area of responsibility and provide technical oversight for the IT services provided.

(4) Develop MOAs and SLAs to document the above-baseline, customer and service provider expectations, and to ensure successful conduct of the full spectrum of the theater IM and IT mission.

(5) Implement and enforce Army-level IM and IT policies, standards, architectures, programs, plans, and PfM and budgets for common-user concerns within their assigned regions.

(6) Review and issue technical validation certification for IT non-service requirements that will be connected to the DODIN–A.

(7) Implement the tenets of the DODIN–A strategy, transition service delivery, management, and oversight from local-level provisioning to enterprise operations as capabilities evolve.

(8) Identify and consolidate theater IM and IT requirements; ensure that these requirements are validated, coordinated, and integrated in accordance with AR 70–1.

(9) Maintain network security assessment and authorization (A&A) documentation for the common-user network and systems under their purview, and exercise visibility of A&A documentation for mission systems and services operating in or on respective areas of responsibility (see AR 25–2).

(10) Ensure that current contingency plans provide for effective withdrawal or destruction of records in hostile or unstable conditions and are prepared by all installations, to include any element in an overseas area not under the jurisdiction of a major overseas commander (see AR 25–2).

(11) Implement an inspection program to verify the service provider's compliance with requisite policies, MOAs, and SLAs, and to assess customer satisfaction with the services provided.

(12) Maintain a uniform set of IT performance metrics, report to the Army IT Metrics Program, and coordinate with the ACSIM to integrate the metrics into the ISR–S program.

(13) Serve as the on-installation entry point for all installation-level IT infrastructure requirements, such as outside cable plant connectivity and campus-area switching upgrades.

(14) Provide IM and IT manager services on Army posts, camps, and stations, and provide common-user IT services in accordance with the C4IM services list.

(15) Serve as the initial focal point for tenant organizations and activities to obtain support for unique IT services, enhanced level of common-user services, or required services that are not listed in the C4IM services list and customer-facing catalog.

(16) Ensure that all systems are evaluated for risks presented to the DODIN. Ensure all identified risks are mitigated prior to certifying a system for fielding or connecting to the network. Identify issues and recommendations to overcome obstacles to achieve a RMF certificate.

(17) Determine procedures for enforcing architecture standards compliance on a single installation or assigned geographical area.

f. Prescribe the operational activities, policies, processes, procedures, and protocols for reportable insider threat intelligence and information, as well as incident management, event management, problem management, and database and internet/web management.

g. Prepare and rehearse a DODIN operations recovery COOP plan by providing an enterprise-level, disaster recovery (DR) strategy and architecture capability, to include resolution of actual or potential interruptions in service or reductions in quality of service in established response times; identifying and prioritizing infrastructure, service, and security events; establishing appropriate responses to those events; defining and eliminating problems that have detrimental impact on quality and cost of services; mitigating probability of problem occurrence; and ensuring optimal performance, security, and functionality of enterprise databases and hosted applications.

h. In coordination with the CIO/G–6, oversee compliance for collateral top secret and below networks and systems—

(1) Prescribe the operational aspects of information protection and data security, to include processes that enforce Armywide compliance with the Federal Information Security Management Act of 2014, OMB Circular A–130, DODM 5200.01 Volume 1, DODI 5230.24, and AR 380–5. Identify and analyze threats to the Army global enterprise network and its enabling technologies.

(2) Measure Army compliance with cybersecurity requirements and prescribe cybersecurity program operational execution activities, processes, and practices (see AR 25–2).

i. Enable external engagement—

(1) In support of JS information requirements—

(a) Develop and maintain system plans.

(b) Provide reports on JS-controlled communications assets, as required.

j. Oversee operational review and coordination of information infrastructure or architectures. Advise the CIO/G–6 on AEA, in support of implementation, management, and security of the DODIN–A.

k. Develop, validate, and execute approved Army telecommunications requirements to DISA and overseeing implementation of Army telecommunication requirements.

l. Review ISPs to ensure systems comply with policies established to defend DOD networks.

m. Integrate, synchronize, review, and endorse functional requirements documents for non-tactical networks with other requirements to conduct cyberspace operations. Provide comprehensive picture of the functional requirements to operate and defend the non-tactical portion of the DODIN–A. Propose requirements priorities to the CIO/G–6.

n. Provide a representative for the ASA (ALT) Configuration Steering Board who, along with other members of the board, will recommend changes to the current baseline.

o. Provide a representative to the CIO EB.

p. Provide a representative to the Army ITOC to assist in the development of a holistic Army IT Strategy to include periodic outcome-based assessments.

q. Provide enterprise management and services, to include—

(1) Assist the CIO/G–6 as the Army's IT integrator to achieve a single, virtual, DODIN–A by advising the end-to-end management of the Army's enterprise service area (service delivery, service operations, and infrastructure-management) using the AEA and Information Enterprise Architecture (IEA). Provide Army network enterprise services and capabilities, to include the mandated core enterprise services of the DOD IEA, installation IT services, and network connectivity. Prescribe the Army's IT Service Management Program—

(2) Prescribe all service delivery activities, processes, procedures, and protocols for configuration management, availability management, capacity management, change management, and release management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority for any system architecture design or device that impacts the DODIN–A and enabling technologies.

(3) Prescribe all service operations activities, processes, procedures, and protocols for incident management, event management, problem management, spectrum management, and database and internet web management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority over capabilities that impact the DODIN–A and enabling technologies.

(4) Prescribe all infrastructure-management activities, processes, procedures, and protocols for network and telecommunications management, facilities management, data storage management, IT services continuity management, and mid- and mainframe management for the Army's networks, systems, and functional processing centers. This includes technical and operational authority over capabilities that impact the DODIN–A and enabling technologies.

r. Operate and protect the non-tactical portion of DODIN–A.

s. Organize and chair the DODIN–A technical configuration control board, and direct the Army enterprise configuration control and release management.

t. Advocate for transformation, and engineer the enterprise network to efficiently and effectively serve the needs of the Army.

u. Oversee procurement requests to ensure that IT hardware, software, and services align with the Army's mission to operate, maintain, and defend its networks, and will support other enforcement procedures as they are developed and coordinated.

v. Support the CIO/G–6 to prescribe resources (people, projects, technology, and infrastructure) for service delivery, service operations, infrastructure-management, cybersecurity, and network defense.

w. Prescribe communication services in support of the news media during field exercises, contingencies, and combat operations when commercial capabilities are not available.

x. Provide an IT-operational engineering force with worldwide deployment capability to provide quick-reaction support to plan, integrate, install, operate, and maintain IT systems from the power projection platform to the tactical theater of operations.

y. Provide technical guidance for connectivity between Army DREN users and Army installations for Army enterprise services.

z. Develop and maintain the concept of operations (CONOPS) and TTP for operating the non-tactical portion of the enterprise network.

aa. In coordination with Program Executive Officer Enterprise Information Systems (PEO EIS), develop fielding schedules and propose priorities; and provide follow on, sustainment training for PM funded equipment and training.

bb. Provide a representative to the PEO EIS Configuration Steering Board who will, along with the other members of the board, recommend changes to the current baseline.

*cc. S*upport the CIO/G–6 with development and execution of future revisions of the Army Enterprise Service Management Framework (AESMF) and oversee implementation as it relates to DODIN operations.

(1) Publish and update the AESMF CONOPS.

(2) Publish implementation guidance such as Operations Order, Fragmentary Orders for the AESMF, and execute tasks to staff.

(3) Identify owners for the following life cycle processes and functions:

(a) Service Design Life Cycle Stage: Availability Management, IT Service Continuity Management, and Service Level Management.

(b) Service Transition Life Cycle Stage: Asset Management and Service Validation and Testing.

(c) Service Operations Life Cycle Stage: Access Management, Event Management, Incident Management, Problem Management, Request Fulfillment, Application Management (Function), IT Operations Management (Function), and the Technical Management (Function).

dd. In coordination with TRADOC and the ABC, propose requirements related to the non-tactical portion of the enterprise network.

ee. In coordination with CIO/G–6, review and provide input to PEO EIS for system designs related to the non-tactical portion of the DODIN–A.

ff. Oversee the Army Military Auxiliary Radio System (MARS) program and the Global High Frequency Enterprise Radio Network, including amateur radio operators licensed to operate as a MARS operator (see AR 25–6).

gg. Appoint in writing an Army DS.

2–28. Commanding General, U.S. Army Intelligence and Security Command

In addition to requirements listed in paragraph 2–33, the CG, INSCOM will—

a. Execute the Ground Intelligence Support Activity, which serves as the Army service provider for SCI systems, the single Army JWICS IP registration authority, and the responsible organization for implementing Army JWICS IP policy.

b. Review ISPs to ensure the Army is acquiring information technology that meets approved mission requirements of the Intelligence Community.

2–29. Commanding General, U.S. Army Criminal Investigation Command

In addition to requirements listed in paragraph 2–33, the CG, USACIDC will—

a. Operate the computer crime investigative unit.

b. Conduct criminal investigations of intrusions and related malicious activities involving U.S. Army IT and information, to include national security offenses, data exfiltration, and denial of service attacks, social engineering attacks, malicious logic, web page defacements, insider criminal activity, and so forth.

c. Provide criminal and technical intelligence analyses of vulnerabilities, methodology, tools, techniques, or practices obtained from computer crimes investigations or forensic examinations to support cybersecurity activities.

d. Conduct Electronic Crime Vulnerability Assessments to assess IAVA and related cybersecurity compliance.

e. Conduct crime prevention surveys to identify crime-conducive conditions involving Army IT.

f. Serve as chief enforcer of Federal laws governing the investigation of criminal offenses involving networks and systems, serve as the sole entity for felony investigative determinations, and serve as the sole Army interface with Federal and civilian law enforcement agencies.

g. Participate with the CIO/G–6; DCS, G–2, ARCYBER, INSCOM, NETCOM/9th SC (A), and 1st Information Operations (IO) Command in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which cybersecurity countermeasures will be directed.

2–30. Commanding General, U.S. Army Corps of Engineers

In addition to requirements listed in paragraph 2–33, the CG, USACE will—

a. Manage the "usace.army.mil" Internet domain and the assignment of sub-domains on CorpsNet.

b. Oversee organizations that operate and maintain portions of the CorpsNet (the systems and networks that constitute the CorpsNet), which is a separate network on the DODIN. Although a separate network, CorpsNet IM capabilities are prescribed by the CIO/G–6 and Army Cyber Command, and are executed by the USACE. This includes exercising technical authority and configuration management authority for CorpsNet systems and functional processing centers.

c. Provide guidelines and direction for CorpsNet IT configuration management.

d. Implement an IT architecture incorporating all engineering functions that require interface between the Civil Works Program, the Army MILCON program and implementation, and management of common assets.

e. Coordinate the documentation of data standards for MILCON and USACE Civil Works Program data elements with the CIO/G–6.

f. Coordinate with U.S. Army Information Systems Engineering Command (USAISEC) during the planning, design, and contract negotiations of the technical and functional requirements of information systems and communications systems for all Army MILCON projects.

g. Develop a technology transfer program for information systems developed as components of construction or engineering projects that includes a full accreditation package, coordination with the CIO/G–6 and receiving command's G6, and sustainment requirements for information technology being fielded, as part of a USACE project being transitioned to an operational activity.

h. Appoint in writing an Army DS.

2–31. Commanding General, U.S. Army Test and Evaluation Command

In addition to requirements listed in paragraph 2–33, the CG, ATEC will—

a. Support system acquisition, force development, and experimentation processes through overall management of the Army's T&E programs. ATEC is the Army's independent operational test activity and reports directly to the Vice Chief of Staff, U.S. Army through the Director of the Army Staff. The CG, ATEC, will perform responsibilities and duties as assigned in AR 73–1.

b. Serve as the principal developmental and operational test agency for Army enterprise systems and lead for evaluation of Army enterprise and information systems.

c. Support the CIO/G–6 in the assessment of network interoperability certification. Provide accredited test performance data for Army enterprise and information systems under consideration for Army acquisition.

d. Review ISPs to identify deficiencies in planned testing and provide recommendations to tightly correlate the ISP and associated Test & Evaluation Master Plan (see para 3–22).

2–32. Commanding General, U.S. Army Installation Management Command

In addition to requirements listed in paragraph 2–33, the CG, IMCOM will—

a. Manage and fund morale, welfare, and recreation (MWR) mission systems in accordance with Army Regulations and Policy to ensure compliance with ARCYBER operational control and with special business standards and legal requirements including PCI/DSS.

b. Develop and implement IT governance processes as necessary to ensure MWR IT programs, regardless of funding source, are secured and managed at the same or higher standard as required by this regulation.

c. Validate and approve IT purchases using non-appropriated funds (NAF) as delegated by the CIO/G–6.

d. Coordinate and support MWR IT systems, including funding requirements, standardized systems, and IRM to the CIO/G–6.

e. Establish MWR enterprise architectures and integrate those with Army enterprise architectures.

f. Ensure any research and development of new custom IT capabilities funded with NAF are synchronized with Army and DOD domain leads to prevent duplication of capabilities.

g. Ensure all NAF IT is purchased in accordance with the CIO/G–6 guidance and is awarded in accordance with NAF funding and procurement requirements.

h. Ensure MWR IT requirements on installations are prioritized and funded with infrastructure upgrades.

i. Develop and ensure standards are in place for commercial internet access, non-.mil domains, and networks for MWR programs that are authorized to operate in those environments.

j. Provide functional oversight and management for facility-related control systems.

k. With CIO/G–6, manage the VI program as specified in this regulation including as the proponent and information system owner for the VI metrics system.

2–33. Commanders of Army commands/Army service component commands/direct reporting units/and Army Reserve Component commanders (as authorized by their respective Headquarters, Department of the Army elements)

The CIO/G–6 and ACOM, ASCC, and DRU (as authorized by their respective HQDA elements) commanders are strategic partners. Together, they achieve the standardization, compatibility, interoperability, security, and resourcing of the DODIN–A global network enterprise to ensure warfighter decision superiority. The Army intends to reduce energy use, achieve efficiencies related to IT equipment, and help achieve Federally mandated goals. CHESS is the Army's mandatory source for establishing commercial IT contracts for hardware and software, is the preferred source for IT services, and offers only products that are Electronic Product Environmental Assessment Tool ® registered and ENERGY STAR® qualified with low standby power capability. For the internal IM and IT responsibilities of their commands, commanders will—

a. Establish a senior IM official who implements the command's IM and IT program in accordance with IM and IT policies, as prescribed by the CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities as prescribed by ARCYBER, to include—

(1) Provide, as required, representation to the Army ITOC and associated integrated process teams, working groups and committees.

(2) Provide, as required, representation to the CIO EB and associated working groups and committees.

(3) Identify the command's IT requirements and ensure that mission requirements are validated, coordinated, and integrated in accordance with AR 71–9.

(4) Monitor command mission-related IM requirements throughout their life cycle, to include those requirements for subordinate organizations available on other installations for IT requirements not included as part of established, common-use IT.

(5) Submit requests and requirements for mission-driven, installation-level IT infrastructure implementations (out-side cable plant connectivity, campus-area switching upgrades, and so forth) to the servicing installation NEC for processing through ARCYBER to the CIO/G–6 for ultimate approval or disapproval (see DA Pam 25–1–1 for complete process).

(6) Fund command-unique IT requirements and applicable facilities site remediation dependencies, in support of mission and business, including long-haul communications, IA, and other IT requirements not identified as part of common-use IT or DODIN–A global network enterprise capability.

(7) Coordinate IT plans, programs, and requirements with appropriate information system security managers in accordance with AR 25–2.

(8) Develop, manage, and maintain IT contingency plans, as prescribed by ARCYBER, to ensure the uninterrupted execution of essential missions and functions under all conditions (see DA Pam 25–1–2).

(9) Validate IP address requests from subordinates and ensure that only IP addresses registered by the Army through the procedures published by ARCYBER are employed on networks within their purview.

(10) Develop AEA artifacts for respective command-unique functions and act as the integrator for any "SoS" under their purview, as prescribed by the CIO (see DA Pam 25–1–1).

(11) Enforce DISR compliance for designated systems.

(12) Analyze and revise mission-related and administrative work processes necessary to complement pending, significant IT investments.

b. Enforce compliance with AR 25–400–2 to oversee and manage command records, in order to appropriately secure, maintain, and preserve such records throughout their life cycle.

c. Ensure that written contingency plans provide for effective withdrawal or destruction of records and equipment in hostile or unstable conditions are prepared by all commands and other elements in overseas areas not under the jurisdiction of a major overseas commander.

d. Conduct command-wide evaluations of records management programs to verify the adequacy of documentation, maintenance, use, and disposition of records at least once every 3 years.

e. Identify information systems and communication systems' functional requirements for Army MILCON projects involving respective command missions.

f. Promote a paper-free business environment in the Army through optimum use of electronic business and electronic Government technologies.

g. Administer command-level IT performance measurements as prescribed by the CIO/G–6 and CMO (see DA Pam 25–1–1 for more information) and ensure installations complete quarterly and annual ISR reporting.

h. Direct that CHESS is the mandatory source for purchases of COTS IT hardware, software, desktops, and notebook computers, and all other IT purchases, regardless of dollar value, when available, or a statement of non-availability (SoNA) in accordance with paragraph 3–19*d* must be obtained when a contract vehicle is not available; and that CHESS procurement vehicles are the preferred source for acquisition of IT services. A CHESS statement of non-availability and an ITAS waiver are not required for service contracts. These requirements apply regardless of funding source or appropriation. NAF contracting officers refer to AR 215–4 that direct use of pre-awarded contracts as the preferred method.

i. Develop and distribute command policy on the issuance of IT devices to employees in accordance with chapter 3 of this regulation.

j. Oversee acquisition, operation, accountability, consolidation, and disposition of self-service printing devices to include designating a functional manager(s) to oversee management of printing devices and printing device acquisition, operation, accountability, consolidation, and disposition.

k. Ensure command's IT PfM is conducted in accordance with the provisions of this AR and DA Pam 25–1–1 including oversite of Army Portfolio Management Solution (APMS) and life cycle management.

l. Manage the command's CP–34 program requirements.

m. Execute the cybersecurity and vulnerability program for the command.

n. Manage the command's portion of any Army or joint enterprise license agreements (ELAs). Ensure ELAs are executed, budgeted, and programmed in accordance with CIO/G–6 directives. Identify and recommend ELA's to the CIO/G–6 for Armywide proponency.

o. Assist in establishing a program to integrate PM fielded systems into the command portfolio to minimize operational impacts.

p. Ensure all mission systems in the command have assigned information system owners and other roles necessary for budgeting and managing IT mission systems.

2–34. Commanders of Army service component commands

In addition to requirements listed in paragraph 2–33, ASCC commanders will—

a. Identify the command's IT requirements and ensure that mission requirements are validated, coordinated, integrated, and prioritized in accordance with AR 71–9. Collaborate with ARCYBER, TRADOC, AMC, and FORSCOM to obtain command-unique IT requirements beyond common-use services.

b. Provide IT functional specifications, requirements, and relevant materiel development systems and programs to ASA (ALT), DCS G–3/5/7, AMC, TRADOC, FORSCOM, ARCYBER, and CIO/ G–6.

c. Establish and maintain staff liaison relationships with FORSCOM, TRADOC, AMC, INSCOM, MEDCOM, and IMCOM to recommend new or improved IT-related doctrine, force structure, training, and materiel.

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

e. Manage satellite communications (SATCOM) assets assigned to support ground mobile forces.

f. Integrate records management support into operational plans for the collection and transfer of records created by deployed units in contingency operations, in accordance with AR 25–400–2.

2–35. Commanders or directors of major subordinate commands, field operating agencies, and separately authorized activities, tenant, and satellite organizations

Based upon guidance from their parent organization, commanders or directors of major subordinate commands (MSCs), field operating agencies (FOAs), and separately authorized activities, tenant, and satellite organizations will accomplish the same IM responsibilities as their parent organization, commensurate with their respective mission, size, responsibility, and location. In addition to the duties listed in paragraph 2–21, these commanders will—

a. Establish a senior IM official to implement the command's IM and IT program, in accordance with IM and IT policies as prescribed by the CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute DODIN operations and cybersecurity activities as prescribed by ARCYBER.

b. At a minimum, FOAs and other organizations will—

(1) Establish or appoint in writing an IM office or officer to plan or supervise the execution of IM.

(2) Coordinate with the relevant NEC for common-use IT services.

(3) Designate in writing a subordinate organization records manager, who will perform duties as described in AR 25–400–2, DA Pam 25–403, and DA Memo 25–51.

2–36. Joint Force Headquarters-State, U.S. Army Reserve Command, or comparable-level community commanders

In addition to the duties listed in paragraph 2–33, JFHQ-State, USARC, or comparable-level community commanders will—

a. Establish a senior IM official to implement the command's IM and IT program, in accordance with IM and IT policies as prescribed by the CIO. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute DODIN–A global network enterprise activities as prescribed by ARCYBER. The senior IM official NEC will—

(1) Perform voice and data network management functions for the installation or assigned geographical boundary, to include installation, operations and maintenance, and configuration management of common-user component devices.

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

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

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

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

(6) Perform cybersecurity functions in accordance with AR 25–2.

(7) Perform functions as the single authority to validate the purchase of IT items on the installation, in accordance with IM and IT policies as prescribed by the CIO.

b. Coordinate with ARCYBER for baseline C4IM services. JFHQ–States will coordinate with the ARNG Network Operations and Security Center.

c. Provide non-tactical VI documentation (VIDOC) support within VI activity capabilities and request additional support through the NEC VI manager when local capabilities cannot meet requirements.

d. Coordinate with the NEC when moving to a Regular Army installation.

e. Ensure that fielded systems are networthy and AEA compliant.

2–37. U.S. Army Center for Army Analysis

The Director, U.S. Army Center for Army Analysis will appoint in writing an Army DS for their organization.

2–38. U.S. Army Modeling and Simulation Office
The Director, U.S. Army Modeling and Simulation Officer will appoint in writing an Army DS for their organization.

2–39. U.S. Army Capabilities Integration Center
The Director, U.S. Army Capabilities Integration Center will appoint in writing an Army DS for their organization.

2–40. Program executive officers and direct reporting product managers
PEOs and direct reporting product managers will—

a. Develop AEA compliant architectures for assigned systems in coordination with CIO/G–6 and consistent with DOD and Army guidance.

b. Develop and coordinate architecture products as input to architectures under their purview.

c. Develop and submit ISPs in accordance with DODI 8330.01 (see DA Pam 25–1–1).

d. Ensure that all fielded systems are logistically supportable during the life cycle of the system and follow integrated logistics support responsibilities in accordance with AR 700–127.

e. Prepare the Major Acquisition and Major High Value IT Investments (formerly Exhibit 300s) business case(s) for systems as applicable for submission with the IT budget in accordance with OMB Circular A–11 and CIO Budget Guidance.

f. Submit all DBSs to the DBC.

g. Ensure records management requirements are included in office operations and systems throughout their life cycle.

h. Design, build, test, and field IP-enabled IT and NSS to efficiently use IP address space. Coordinate materiel solution IP address space requirements with TRADOC and ARCYBER as required. Request IP addresses to support materiel solutions in accordance with procedures published by ARCYBER.

i. Ensure compliance with RMF cybersecurity A&A requirements, the Army RMF Program, and AEA for all PM-developed IT systems.

j. Ensure that compliance with DOD policy regarding accelerated use of COTS IT and NSS by establishing a baseline and documenting progress in this effort.

k. Comply with AIC policy, configuration management procedures, and resource adequately for systems to undergo AIC testing (see DA Pam 25–1–1).

l. Support the Army's configuration control process for the Joint messaging standards that are implemented in the systems for which they are responsible. Provide support, as required, to the Army's representative to the Joint configuration control boards that manage the configurations for these same Joint messaging standards.

m. Ensure that all installation-level IT infrastructure requirements and prioritization modeling recommendations (outside cable plant connectivity, campus-area switching upgrades, and so forth) needed to support a specific product, program, or system fielding on Army posts, camps, and stations are validated and prioritized by ARCYBER and approved by CIO/G–6 prior to implementation (SAIS–NSI) (see DA Pam 25–1–1 for complete process).

n. Provide IT functional specifications, requirements, and relevant development systems and programs with ATEC to establish & maintain RDT&E capabilities.

o. Adhere to the platform requirements as specified in the BMA, WMA, DIMA, and EIEMA common operating environment (COE) architecture and information-sharing requirements specified in the AIA.

p. Ensure data, information, and IT services are made VAUTI throughout their life cycle for all authorized users.

2–41. Program, project, and product managers and information technology materiel developers
Program, project, and product managers and IT materiel developers (MATDEVs) will—

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

(1) Develop architecture views and products for the IT systems being acquired to comply with either JCIDS or Business Capability Acquisition Cycle (BCAC) guidance, and adhere to the Office of the Secretary of Defense (OSD) and Army policies.

(2) Develop and acquire technical support solutions and ensure that they are within the constraints of the AEA.

(3) Coordinate AEA architectures for their systems with the PEO and the management official of gaining commands and installations (not applicable to weapons platforms).

(4) See the DISR online tool at https://gtg.csd.disa.mil to build standards views.

(5) Coordinate their systems architecture with Army Architecture Integration Center prior to fielding systems. For more information, see DA Pam 25–1–1.

(6) Program for resources required to develop architectures and architecture products for assigned systems.

(7) Program for resources required to perform accreditation and interoperability testing for integration with existing systems.

(8) Identify bandwidth requirements to support program and collaborate with ARCYBER for bandwidth support.

b. Coordinate fielding plans for their systems with senior IM officials of gaining commands and installation NECs to ensure compatibility with existing systems and IT support structure.

c. Ensure that records management requirements are included in systems throughout their life cycle in accordance with AR 25–400–2.

d. Develop and prepare Major Acquisition and Major High Value IT Investments (formerly Exhibit 300s) business case(s) for systems as applicable for submission with the IT budget in accordance with OMB Circular A–11 (not applicable to weapons platforms).

e. Submit all DBSs for review to the DBC.

f. Act as the systems engineer, technical integrator, and MATDEV for assigned ISs.

g. Ensure that IT materiel testing, acquisition, and support comply with Joint, North Atlantic Treaty Organization, and the American, British, Canadian, Australian armies' operations, standardization, and interoperability agreements; and Federal and international standards.

h. Plan, program, and conduct new equipment training for assigned systems and recommend required training for inclusion in their Army schools programs.

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

j. Ensure software testing is compliant with the requirements found in AR 70–1.

k. Assess the ability to share and reuse data-related resources and register those resources with the appropriate Army or DOD registry.

2–42. Information management organizations below Headquarters, Department of the Army level

a. Subordinate organizations below HQDA will designate a senior IM official and establish supporting offices within their organization. Regardless of designation, all organizations will comply with governing legislation; Federal, DOD, and SECARMY guidance; and the appropriate responsibilities delineated in chapter 2 and elsewhere in this regulation (see also DA Pam 25–1–1). The ARNG will comply with Defense Appropriations Bill 1997, Senate Report 104–286. Command senior IM officials will directly supervise the IM staff, related programs, and activities; and execute DODIN–A global enterprise network activities as prescribed by ARCYBER. Every ACOM and ASCC will appoint in writing a senior IM official as a principal staff officer. DRUs may appoint in writing a senior IM official as a principal staff officer if required and designate in writing by the respective HQDA official. MSCs may appoint in writing an equivalent IM official with similar staff responsibilities as an ACOM's or ASCC's senior IM official.

b. Senior IM officials will—

(1) Perform voice and data network management functions for the installation or assigned geographical boundary, including installation, operations and maintenance, and configuration management of common-user component devices.

(2) Determine procedures for enforcing architecture standards compliance on a single installation, assigned geographical area, or mission function area of responsibility.

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

(4) Appoint in writing a frequency manager, if required, to coordinate, plan, program, manage, and supervise frequency management responsibilities (see AR 5–12).

(5) Perform cybersecurity functions in accordance with AR 25–2.

(6) Perform functions as the single authority to validate and approve the purchase of IT items in accordance with IM and IT policies as prescribed by the CIO.

c. The USAR secures particular services via the C4IM services list from installation NECs; however, due to their mission, the USAR provides all data-related and cybersecurity-related services to USAR locations via the Army Reserve Network.

d. Tenant commands, satellite organizations, separately authorized activities, Government-owned and contractor-operated facilities, regional support activities, U.S. Army Reserve (USAR) regional support commands, FOAs, and major staff entities will not establish a NEC but will have an information management officer (IMO) appointed in writing on official orders to coordinate internal IT services with the appropriate NEC. The IMO will identify their organization's information requirements to the supporting NEC or theater signal command. The IMO is the primary interface between the NEC and the supported organization(s). Where no post, camp, or station installation exists, the host command or activity will coordinate IT services with the respective theater signal command. See DA Pam 25–1–1 for a detailed list of responsibilities. For the USAR, only the USAR NEC may negotiate with or coordinate with the theater signal command.

Chapter 3
Information Technology Governance and Investment Management

Section I

Planning

3–1. Introduction
The ITIM chapter outlines the life cycle of an IT investment. This chapter addresses Army IT and data governance and requirements for reporting, accountability, and compliance through the IT life cycle. Compliance with Army policies is supported through the Army's governance boards, reporting structures, and oversight procedures. Often IT resources are managed and acquired as stand-alone systems rather than as integral parts of a functional MA, resulting in duplicative investments that deliver the same or similar solutions or investments that are at times not interoperable or compliant with DOD and Army standards and policies. CPIC is a systematic approach to select, control, and evaluate information technology investments. As mandated in 40 USC 11101 through 40 USC 11704, Information Technology Management, requires Federal agencies to focus on the results produced through CPIC for IT investments to ensure accountability and responsibility. The CIO/G–6, in coordination with other HQDA organizations, will establish a comprehensive approach to manage the life cycle of Army information resources (includes information and associated resources; equipment, personnel, funds, and IT) that support the Army mission. Information resources management activities must be performed in an efficient, effective, economical, secure, and privacy-enhancing manner to support Army goals with the best group of investments. A standardized, repeatable IT investment management process will improve the identification, acquisition, control, and oversight of information resources. The process must assess—

a. Inventory of the physical and software assets associated with an investment.

b. Maintainability and sustainability of the information resources and infrastructure supporting the system.

c. Equipment life cycle posture to manage significant upgrades, replacements, or disposition scheduled to support missions.

d. Terms and conditions of contracts and other agreements linked to strategic plans to ensure all are sufficient to enable Army to meet statutory and regulatory requirements.

3–2. General
The Army's ITIM approach is one that follows a repeatable process of planning, investment, and execution throughout the life cycle of the investment, or portfolio of investments. The cycle begins when capability gaps or requirements are identified. These gaps are based on emerging guidance or legislation. This approach applies to all IT and must be included in all mission area and command IT management processes (see DA Pam 25–1–1).

3–3. Analysis
Where possible, all commands, DRUs, and MAs must begin the planning phase by developing a strategy that describes their technology and information resource goals that align to the appropriate Army strategy (for example, The Army Plan and The Army Campaign Plan) and demonstrate how the technology and information resources goals map to the Army's mission and organizational priorities.

a. *Risk management.* Part of planning, through the life cycle of IT investments, risks to be considered:

(1) Security.

(2) Privacy.

(3) Records Management.

(4) Public Transparency.

(5) Supply Chain Security.

b. *Information technology investment resource management.* The CIO/G–6 will—

(1) Work in coordination with ASA (FM&C) and ASA (ALT) to develop and maintain an Armywide budget development process for planning, programming, and budget stages regarding programs that include IT resources (all, not just those that are technology oriented).

(2) Manage the RIG through which the CIO/G–6 and the DCS, G–8 (as co-chairs) working with other RIG members plan the overall portfolio of IT resources that achieve program and business objectives by weighing potential and existing investments against other investments. The RIG identifies gaps between planned and actual cost, schedule, and performance goals for IT investments and develops a plan to address gaps. The RIG approves the IT components of plans to ensure IT investments are assessed appropriately. The CIO affirms the agency budget submission to OMB.

(3) Approve the IT investment portion of the budget request. The designated command privacy official will review the IT investment portion of the budget to ensure privacy requirements and costs are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).

(4) The CIO and Army CFO jointly affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources. The IT portfolio includes appropriate estimates of all IT resources included in the budget request.

(5) In coordination with ASA (FM&C) and ASA (ALT), define Armywide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.

c. Commercial off-the-shelf information technology planning activities. In the context of the U.S. Government Federal Acquisition Regulation (FAR), COTS is a term for commercial items, including hardware, software, and services, available in the commercial marketplace that can be purchased and used through a DOD contract. COTS IT refers to COTS procured IT capabilities. COTS IT helps to provide a common-user infrastructure used to generate force activities. TRADOC develops the minimum mission-essential COTS IT requirements needed to sustain a life cycle strategy and to achieve assigned, full spectrum operations. COTS IT will be included in an appropriate modified table of organization and equipment (MTOE), a table of organization and equipment, and a table of distribution and allowances (TDA) documentation. .

d. Managing the planning phase. Command senior IM officials will manage the organization's implementation of the Army's IT investment strategy, IT infrastructure changes, acquisition strategy, and IA prerequisites. This responsibility should not be delegated to subordinate command, senior IM officials.

e. Commercial off-the-shelf information technology management process for modified table of organization and equipment units. Common COTS IT assets are defined as IT hardware (computers, printer, and digital senders) procured by tactical units to accomplish operational tasks. The COTS IT Management Process provides a sustainable life cycle strategy to ensure tactical force's COTS IT requirements are met at home station, training centers, and while deployed.

(1) The COTS IT Management Process is a four-step sequential process that determines, validates, and documents requirements in order to ensure proper programming of funding.

(a) TRADOC assesses and determines COTS IT requirements by organization and echelon. This is a continuous process based on requirements and improvements in IT.

(b) DCS, G–3/5/7 validates requirements submitted by TRADOC utilizing existing requirements validation processes.

(c) DCS, G–3/5/7 documents the validated requirements using the documentation processes outlined in AR 71–32.

(d) DCS, G–8 incorporates COTS IT resource requirements into POM submissions. DCS, G–8 and DCS, G–3/5/7 will implement funding solutions, Training Resource Model funding, programming for life cycle replacement, and new requirement resourcing.

(2) For replacement of COTS IT in a MTOE unit, a 4-year/25percent life cycle will be used to authorize COTS IT (computers, printers, digital senders) per year. This is based on operating in a tactical field environment and is in accordance with the approved 4-year life cycle replacement strategy that is a part of the COTS IT Management Process for MTOE Units.

f. Commercial off-the-shelf information technology process for table of distribution and authorization units. Common COTS IT assets are defined as IT hardware (computers, printer, and digital senders) procured by generating force units to accomplish organizational tasks. For replacement of COTS IT in a TDA Unit, a 5-year/20 percent life cycle will be used for planning and budgeting purposes. This standard is based on operating in a garrison office environment. Exceptions include zero/thin clients in which a 7-year life cycle will be used, and any other mission where the Program Evaluation Group (PEG) determines that the mission drives a shorter life cycle.

g. Department of Defense information network – Army life cycle replacement planning activities. DODIN–A assets are COTS IT products which comprise the Army's portion of the DOD information network. DODIN–A assets include computing devices (that is, servers), storage devices, security devices (for example, firewalls, intrusion detection/protection systems, security appliances, and so forth), and integrated communications devices (for example, routers, switches, network appliances, session controllers, and so forth). For replacement DODIN–A assets, a 5-year life cycle, but not more than a 7-year life cycle, will be used for planning and budgeting purposes. This 5- to 7-year life cycle replacement rate provides organizations the flexibility to effectively and efficiently manage COTS IT equipment supporting DODIN operational and security requirements.

h. Coalition and combatant command mission network life cycle replacement planning activities. For planning and programming purposes, 5- to 7-year life cycle replacement rates also apply. This includes all mission-specific equipment acquired for installation or extension of coalition or mission networks in support of combatant commands. Examples are Combined Enterprise Regional Information Exchange (CENTRIX), MPE – Information System, and Battlefield Information Collection and Exploitation System.

i. Mission-unique information technology equipment planning activities. This pertains to IT equipment, beyond basic telecommunication equipment (for example computers, phones), procured for installation in new, restored, or modernization facilities to ensure new occupants are able to perform their organization's mission. Examples include secure and unsecure audio/video teleconference and collaboration capabilities, digital monitors, projectors, and cable/satellite TV equipment. Once installed in facilities, a 5-year life cycle will be used for planning and programming purposes. A 5-year life cycle also applies to Joint, Coalition & Army Headquarters having operations centers, and intelligence centers outfitted with mission-unique equipment (MUE).

j. Defense business system hardware planning activities. For DBSs operating on COTS IT hardware, a 5-year/20 percent life cycle will be used for planning and budgeting purposes.

k. Other life cycle replacement considerations. Operational needs may necessitate IT equipment be replaced at any point before the end of its normal life cycle (for example TDA units operating hardware in harsh environments, hardware identified having cyber vulnerabilities, hardware technical obsolescence, hardware supporting high performance computing environments, and so forth). Army organization should account for these special considerations when planning and programming for life cycle replacement.

3–4. Governance

Army enterprise IT governance provides strategic guidance, ensures Army objectives are achieved, evaluates whether risk is managed appropriately, and verifies that enterprise resources are used effectively. The CIO/G–6 will maintain a decision-enabling framework to ensure visibility of IT investments throughout their life cycle. All HQDA governance bodies that manage IT and consist of members from more than one HQDA organization, ACOM, ASCC, DRU, or DOD components must include the CIO as a member and define the process and policies in sufficient detail to address information resources appropriately. At a minimum, these processes and policies will:

a. Evaluate investments and projects in development to determine the applicability of agile development.

b. Use approved open data standards to the maximum extent possible when implementing IT systems.

c. Evaluate the cost schedule and performance variances of IT projects across the portfolio using appropriate measurements (leverage ITSM, EA, and other agency IT or performance management).

d. Establish policies and procedures to conduct IT investment reviews, operational analysis, or other applicable performance reviews.

e. Meet data and information needs through Armywide data governance policy that clearly establish roles, responsibilities, and processes by which Army personnel manage information as an asset and relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives.

f. Phase out unsupported information systems and system components as rapidly as possible, and planning and budgeting activities for all IT systems and services incorporate migration planning and resourcing to accomplish this requirement.

g. Integrate information security and privacy into the system development process.

h. Use the performance measurements to evaluate the use of agency information resources. The CIO/G–6 may recommend the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO/G-6's evaluation, within the terms of the relevant contracts and applicable regulations.

i. Establish and maintain a process to regularly engage program managers to ensure that IT investments are meeting customer needs and achieving the strategic objectives of the Army.

j. Measure performance in accordance with statutory and regulatory guidance.

k. CIO/G–6 hosts eight primary governance forums that support the EIEMA: CIO EB, Migration Implementation and Review Council (MIRC); AENC, ITOC, RIG, ADB, Army Data Council (ADC), and the Army Standards Council (ASC) (see DA Pam 25–1–1). For more information and board charters, visit the CIO/G–6 Governance milWiki page at https://www.milsuite.mil/wiki/armycio/g–6_governance.

3–5. Enterprise architecture

a. Army enterprise architecture.

(1) The AEA provides policy and guidance governing the composition and use of architecture documentation within the Army. The LandWarNet (LWN) 2020 and Beyond Enterprise Architecture (LWN 2020 EA) document describes, and provides guidance for, the endstate EA of LandWarNet. It informs near- and mid-term Army IT investment and acquisition decisions to assure that they are aligned with the Army Network Campaign Plan and the DOD IEA, which encompasses the Joint Information Environment (JIE).

(2) An EA is an information asset base, which contains information that defines the mission, the technologies necessary to perform the mission, and the transition processes for implementing new organizations, processes, and technologies in response to changing mission needs. An EA includes a baseline architecture, a target architecture, and a sequencing plan.

(3) The AEA encompasses all of the products and artifacts related to the architecture of the Army's IT solutions and capabilities. This includes, but is not limited to functional, system/system-of-systems, operational, technical, capability set, implementation/solution, and MA. In addition, the AEA contains the standards and reference architectures applicable to Army IT systems. An attribute of each architecture is the timeframe in which it is valid or intended, so that the AEA includes current (that is, "baseline") architectures, strategic architectures (that is, "target" architectures) and a sequencing plan.

(4) The purposes of the AEA are as follows:

(a) To completely and accurately document all aspects of the Army IT architecture.

(b) To support the tracking and alignment of Army IT initiatives and process improvements with the Army Network Strategy and to inform IT investment decisions.

(c) To support the acquisition, implementation, and management of the Army IT systems that provide the IT capabilities needed to enable the Army's mission and operational capabilities.

(d) To help reduce waste and duplication, increase shared services, close performance gaps, and promote interoperability.

(5) The AEA incorporates Federal information security and privacy requirements into the Army's enterprise architecture to ensure that risk is addressed and information systems achieve the necessary level of trustworthiness, protection, and resilience.

(6) All Army component architectures and capability set architectures will be registered through the ArCADIE as the Army's architecture federation partner to support DOD-wide discoverability, accessibility, and decisionmaking. The ArCADIE is available at https://cadie.army.mil. DA Pam 25–1–1 contains additional information regarding ArCADIE capabilities, access, and governance.

(7) The CIO/G–6 will set policy and formally define, approve, and control the artifacts contained in the IEA. All artifacts will be described via metadata to enable automated search and discovery.

b. Army Enterprise Architecture governance.

(1) The CIO/G–6 will formally approve, manage, and control the contents of the AEA, and ensure that the use of the AEA is integrated with appropriate planning management processes, such as PfM, configuration management, resource allocation, and strategic planning efforts.

(2) AEA governance is achieved through the following boards—

(a) The AENC establishes strategic EA guidance and direction.

(b) The AENC also approves architecture initiatives, conducts in-process reviews (IPRs), directs trade-offs, shapes the POM, and approves release and delivery.

(c) AENC council of colonels defines, directs, and manages the activities required to develop the artifacts contained in the AEA.

(d) The CIO/G–6 certifies integration, validates architectures, establishes standards and patterns, and approves implementation; see DA Pam 25–1–1. The CIO/G–6 also leverages the ISP to verify compliance with approved technical and enterprise architectures.

c. Army enterprise architecture organization. The AEA comprises of three primary types of architectures.

(1) Operational architecture. The operational architectures are led by each of the MA leads, and provide a description of today's Army business processes and how they will evolve over time. These operational architectures potentially contain both IT and non-IT functions (as derived from one or more DOTMLPF–P solutions). Information related to the specific content and processes associated with operational architectures is found in the Chairman of the Joint Chief of Staff Instruction (CJCSI 3170.01H) and AR 71–9.

(2) Systems Architecture. The Systems Architecture is led by ASA (ALT) and represents the individual solutions and services that comprise DODIN–A. These architectures are at the tactical layer, and are complete and detailed enough to support system acquisition and integration. Information related to the specific content and processes associated with Systems Architecture is found in DOD IEA 2.0 and DOD Architecture Framework (DODAF) 2.02, and its associated DOD and Army reference documents.

(3) Information Technology Architecture. The purpose of the IT Architecture is to translate the Army Network Strategy and other driving documents into a roadmap that provides the technical guidance, standards, implementation conventions, and business rules necessary to guide investment and acquisition strategies and decisions for the DODIN–A. The IT Architecture is captured in two separate documents: the Enterprise Architecture, and the Enterprise Reference Architectures. The architecture data and information found throughout these documents is delivered to the Army's acquisition community through the NCS Systems of Systems Reference Architecture. All MAs and technical architectures must integrate with the AEA.

(a) *Army Information Architecture.* AIA is the core component of the ADMP. The AIA, based on DOD IEA, provides the specific information-sharing, data exchange, and compliance standards that enable Army stakeholders to envision,

design, develop, deploy, and use information systems consistently to help meet the Army information-sharing objectives. Organizations, systems, data assets, and data services will be assessed against the AIA through the AIA Compliance Assessment process. Developers will use the AIA as design and development guidance for enabling information-sharing. Developers will use the AIA as a set of compliance requirements for assessing the level to which systems meet net-centric information-sharing objectives. The primary content of the AIA is a collection of principles and business rules that address the following topics: data asset development and management; data and services deployment; data delivery and use; and secured availability.

(b) *Army enterprise architecture certification/compliance.* Army enterprise architecture certification/compliance (AEACC) policy guidance and the architecture compliance assessment (ACA) (see DA Pam 25–1–1) are a means for ensuring that all Army IT solution architectures and resulting systems comply with the rules put forth in the current LWN Enterprise Architecture (EA) and associated reference architectures (RAs). LWN applies to the Army's portion of the DODIN. The DODIN–A comprises the IT assets of all Army activities, agencies, and components. It is the Army's single, global, information enterprise that provides information technology (IT) capabilities, services, and information securely to all Army users and allied organizations. The ACA results measure the level of compliance of Army IT solution architectures and resulting systems and will be used as part of the IT investment management/acquisition decisions.

(c) *Approval of Information Support Plans.* An ISP is a requirement for all ACAT programs that connect in any way to the communications and information infrastructure including both IT and NSS programs. It identifies and documents information needs, infrastructure support, and IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability, and sufficiency concerns. The ISP is summarized in the Acquisition Strategy and reviewed at Milestones B and C. An approved ISP is required for Joint interoperability certification as well as entrance criteria for AIC testing. (DODI 5000.02 and CJCSI 6212.01F)

(d) *Approval process.* The CIO/G–6, Cybersecurity Directorate manages the Army ISP staffing and approval process. The CIO/G–6 is the Army's link with the JS, Command, Control, Communications & Computer/Cyber Directorate (J–6), Requirements Division, and Architecture Branch for the certification of the net-ready key performance parameters (NR–KPP) and the DOD–CIO on ISP guidelines and program compliance. For more information, see DA Pam 25–1–1. The director of the CIO/G–6 (Cybersecurity Directorate) is the Army's approval authority for all Army ISPs.

(e) Architectural views. As part of the ISP, the PM must submit architectural views to describe the interoperability requirements of the IT. The ISP review process will assist the PM to refine these views, and result in a set of detailed measurable interoperability criteria for use in interoperability test and certification.

(f) Portal. PMs must develop the ISP online by entering system information through the Global Information Grid Technical Guide-Federated (GTG–F) portal available at (https://gtg.csd.disa.mil). ISP formatting and content requirements are specified by the GTG–F and described in the Defense Acquisition Guidebook (DAG). Deviations from these requirements require the CIO/G–6 approval. Until GTG–F is available on the Secret Internet Protocol Router Network, Secret ISPs are submitted and approved using the DISA Interoperability and Supportability Legacy Data Repository. PMs will submit Top Secret ISPs using a staffing notification to the appropriately classified network that includes the location of the document on the JWICS and the points of contact. Classified ISPs use the format and content requirements described in the DAG until the GTG–F is available on the appropriately classified network.

(g) Review. The CIO/G–6 will lead the Armywide review of all ISPs. The roles and responsibilities section of this document direct those organizations required to review and provide comments for ISPs (see DA Pam 25–1–1).

(h) Voting member. The CIO/G–6 (Cybersecurity Directorate), SAIS–CBC, serves as the Army voting member to the DOD Interoperability Steering Group (ISG), the governing body for Joint interoperability requirements, acting as the interface between the DOD–CIO, JS, PMs, System Sponsors, and for all issues related to waivers to policy, requests for interim certificates to operate or Joint interoperability certification.

(i) Army Information Technology Standards.

1. IT standard(s) are common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods, and related management systems practices. Standards include the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

2. All Army IT systems will comply with the applicable IT standards contained in the Global Information Grid Technical Guide-Federated (GTG–F) portal (https://gtg.csd.disa.mil), DOD IT Standards Registry (DISR), and Army Technical Guidance Repository (ATGR) (https://www.kc.army.mil/trm_tool/) via ArCADIE's Magic Draw Teamwork Server. Exceptions to this requirement are permitted only via a waiver or an approved change request (CR) as specified in DODI 8330.01. Architectures must also conform to DOD IEA and Federal architecture policies and directives. The ATGR can also be accessed via the CIO/G–6 Enterprise Architecture website (https://ciog6.army.mil/architecuture/tabid146/default.aspx).

3. The Army IT standards waiver and change request processes will be completed in accordance with Annex A, IT Standards Guidance to DODIN–A End-to-End Enterprise Architecture for all IT Standards (for example: data, system, performance, design, naming, process, or cyber).

3–6. Civilian information technology management

CP–34 builds the readiness of the Army Civilian ITM workforce through the Army Civilian Training, Education, and Development System, a requirements-based program that ensures planned and competitive professional development through progressive work assignments, self-development, formal training, and education (interns through GS–15). In addition to the standard Career Program offerings (http://go.usa.gov/cAPZB), CP–34 provides a course-based certification program that addresses the high impact skills required in today's IT workforce.

Section II

Select and Control

Select and control are two distinct phases. The select phase is a process where the solution analyses are completed, business cases are developed, and resource requirements are identified. Portfolio managers will be designated by all Army components, ACOMs, ASCCs, DRUs, and MAs and domains. The control phase is the activity focused on funding, acquiring, fielding, and conducting oversight of investments.

3–7. Analysis process

All Army organizations will have portfolio managers to execute a process to analyze the life cycle of each of their IT investments. The process will contain explicit criteria for analyzing all major IT investments in their portfolio. Implementation of these processes will be commensurate with the size, scope, duration, and delivery risk of the investment. IT portfolio managers will use—

a. Qualitative and quantitative research methods to determine the goals, needs, and behaviors of current and prospective managers and users of the investment to strengthen the understanding of requirements;

b. The following standards in merit-based decisions:

(1) Projected and actual costs.
(2) Risks (cost, schedule, performance, information security, supply chain, and privacy).
(3) Benefits.
(4) Ability to meet operational or mission requirements.
(5) Total life cycle cost of ownership.
(6) Performance.
(7) Information security levels commensurate with NIST standards and guidelines (see AR 25–2).
(8) Interoperability.
(9) Privacy in accordance with Privacy Impact Assessment requirements.
(10) Accessibility.
(11) Ability to share or reuse.
(12) Resources required to switch vendors.
(13) Availability of quality support.
(14) Alignment to the Army strategy.

3–8. Information technology investment recommendations

Once the analysis is complete, the portfolio manager will develop investment recommendations that include supporting evidence and documentation. The recommendations will ensure:

a. IT investment planning documents or artifacts include all IT resources.

b. Decisions related to major IT investments are supported by business cases with appropriate evidence.

c. IT investments enable core Army missions and operational functions and processes.

d. IT capital investment plans and budgetary requests are reviewed.

e. Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis.

f. All acquisition requirements are met.

3–9. Information technology investment selection

IT governance decisions will consider the portfolio manager's recommendations and ensure that all acquisition strategies, plans, and requirements (as described in the FAR), or interagency agreements that include IT are reviewed and approved by the CIO.

3–10. Implementation plan

All commands, DRUs, and all MAs must develop and publish an annual IT implementation plan for submission to the appropriate MA lead and the CIO/G–6 annually. The implementation plan will be leveraged in the control phase (see para 3–12). The plan will include—

a. Organizational vision, core missions, and alignment with Army strategic plans.

b. Goals and objectives.

c. IT baseline and the current situation.

d. Evaluation of needs.

e. Resource plan.

f. Key metrics, timelines, and milestones to track IT transformation.

g. Mitigation strategy for redundancies, gaps, risks, and performance issues.

h. Need for audit readiness integration for the system development.

i. Controls and procedures related to the management of the IT system.

3–11. Army information technology budget

a. The IT budget is a report supporting budgetary material and congressional justification for information technology and cyberspace operations. It defines the portion of the Army's overall budget that is IT. All Army organizations that program, budget, or execute (obligate) resources that support IT and cyberspace operations in any fiscal year of the Future Years Defense Program will report IT and cyberspace operations data in preparation for the Army's inputs to the OSD, OMB, and Congress.

b. The Army IT Budget submission will be compliant with—

(1) Fiscal Year (FY) Budget Estimates Submission Guidance issued by OSD Cost Assessment and Program Evaluation Office and Under Secretary of Defense (Comptroller).

(2) OMB Circular A–11, Sections 51.19, 51.3, 25.5, and 55; Preparation, Submission, and Execution of the 2163 Budget.

(3) OMB Circular A–123 and Section 2165 Internal Control.

(4) OMB Circular A–130, Managing Federal Information as a Strategic Resource.

(5) DOD Financial Management Regulations (DOD FMR 7000.14–R) or NAFI financial reporting requirements for NAF IT.

(6) Federal Information Technology Acquisition Reform, Title VIII Subtitle D Sections 831 through 837 of H.R.3979 - Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015.

c. The CIO/G–6 extracts data for reporting in the IT Budget from APMS and requires all organizations to maintain investment profiles (name, acronym, description, various taxonomies, and so forth) and resources for their IT assets in APMS. Command admins, system owners, and resource managers must align resources to the appropriate category of expense, capability function, and investment stage. Refer to the APMS Desk Side Reference Manual for more information.

3–12. Control

This phase implements the decisions described in the transition/implementation plan developed during the Select Phase. During the Control Phase, which is ongoing, program execution is monitored by the investment owner, and reported to portfolio managers, as appropriate, to ensure that approved mission benefits, cost, schedule, and performance baselines remain attainable. If these parameters cannot be attained or are projected to be unacceptable within the approved criteria, the IT investment must be reevaluated in the Select Phase and against established selection criteria. Requirements, planning parameters, and resources should be realigned to revise the IT portfolio baseline.

Section III

Funding

3–13. Programming and budgeting for information technology

Army organizations will use the IT implementation plans approved during the Select Phase to guide the development of their annual POM and budget submissions to CIO/G–6 and DCS, G–8 for approval. These processes in conjunction with

the approved IT implementation plans prioritize funding to address capability gaps and strategic requirements. The resulting IT investment plan is briefed to respective PEGs; and used to defend the funding of IT investments.

3–14. Information technology purchases (capital asset management)

a. All Army IT investments will be managed as part of the Army's IT portfolio. All Army IT will be accounted for in the APMS system. APMS is the Army's authoritative data source (ADS) for IT investments and their associated systems and applications; as well as, information on system and application hosting environments, supporting three principle PfM-related functions: (1) Portfolio and IT decisionmaking, (2) Budget formulation and reporting, and (3) Portfolio and IT status reporting.

b. APMS registration criteria can be found at the APMS home page: https://cprobe.army.mil/enterprise-portal/web/apms, in DA Pam 25–1–1, and in the APMS Desk Side Reference Manual. Commands are responsible for ensuring system owners validate and update their data in APMS in accordance with the guidance in DA Pam 25–1–1. IT investments not registered or accounted for in APMS will not be funded. IT investments not registered or accounted for in APMS will not be funded. Each Army MA will use APMS to implement this requirement.

c. The APMS is used in support of DBSs (as defined in 10 USC 2222(j)) and as described in AR 5–1.

d. The CIO/G–6 will issue annual IT funding guidance to commands and to system owners with capabilities registered in APMS which clearly states how their IT budget dollars are expected to be executed.

e. Army organizations and Army MA leads will—

(1) Ensure that all IT investments in their portfolios are registered in APMS and that their records are kept current.

(2) Review their portfolios annually for performance, redundancies, gaps, risks, environmental impacts, and strategic alignment of the IT investments.

(3) Report the status of their portfolios through appropriate governance forums.

(4) Conduct IT PfM in accordance with DA Pam 25–1–1.

f. HQDA proponents, ACOMs, ASCCs, PEOs, and other organizations will ensure that all business, non-tactical, or platform systems that support generating force activities IT systems are web-enabled and linked to the enterprise portal or request a waiver from the CIO/G–6.

3–15. Management and accountability of internal use software

a. Internal use software (IUS) that meets the criteria for capitalization in accordance with Generally Accepted Accounting Principles must be reported on Army financial statements within the general property, plant, and equipment (PP&E), Net line on the balance sheet, and as IUS within Note 10 of the financial statements. The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics published DODI 5000.76, Accountability and Management of IUS on 2 March 2017. It is the authoritative reference for the management of IUS regarding establishment of IUS policy, procedure, as well as assigning roles and responsibilities. DODI 5000.76 supplements financial reporting as discussed in DOD FMR 7000.14, and Federal Accounting Standards Advisory Board's Statement of Federal Accounting Standard Number 10. The April 2015 Financial Improvement and Audit Readiness Guidance establishes IUS as a Mission Critical Asset category because it is likely to be material to the financial statements of both the Army and the DOD.

b. What is IUS? In general, IUS is software that includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program. Most often, software is an integral part of an overall system(s) having interrelationships between software, hardware, personnel, procedures, controls, and data. IUS includes software that—

(1) Is acquired or developed to meet the entity's internal or operation needs (intended purpose).

(2) Is a standalone application, or the combined software components of an IT system that can consist of multiple applications, modules, or other software components integrated and used to fulfill the entity's internal or operational needs.

(3) Can be purchased from COTS vendors, modified "off-the-shelf," internally developed, or contractor-developed.

(4) Is used to operate an entity's programs (for example, financial and administrative software, including that used for project management).

(5) Is used to produce the entity's goods and to provide services (for example maintenance work order management and loan servicing).

(6) Is developed or obtained for internal use and subsequently provided to other Federal entities with or without reimbursement.

c. What is not IUS? IUS is not computer software that is integrated into and necessary to operate general PP&E, rather than perform an application. This software shall be considered part of the PP&E of which it is an integral part and capitalized and depreciated accordingly (for example airport radar and computer operated lathes).

d. Accountability of Internal Use Software. The Army will—

(1) Maintain accountability over all IUS until formally relieved of responsibility for accountability for that IUS when it is removed from use in accordance with DOD FMR 7000.14–R.

(2) Manage IUS to ensure resources are used efficiently and effectively, in accordance with the 40 USC, Subtitle III (Clinger-Cohen Act).

(3) Perform fiduciary reporting of capitalized IUS in accordance with DOD FMR 7000.14–R and the Statement of Federal Financial Accounting Standards, Number 10.

(4) Maintain property management and accountability of IUS records and performs fiduciary reporting of capitalized IUS using approved accountable property systems of record.

e. IUS must be capitalized when all of the following conditions are met for the IUS:

(1) It is purchased COTS, internally developed, or contractor-developed, solely to meet the Army's internal needs.

(2) It is operated in a stand-alone mode and is not integrated or necessary to operate hardware or equipment. If not in stand-alone mode, it is subject to capitalization criteria of the asset in which it is integrated.

(3) It is used to operate the Army's programs (that is financial and administrative software including that used for project management) or to support multiple Army MAs (that is BMA, DIMA, EIEMA, and WMA).

(4) Total project cost meets or exceeds the current capitalization threshold. As of the time of this publication, the current capitalization threshold is $250,000 or more.

(5) Expected useful life is two years or more.

f. The Army shall not capitalize—

(1) Software developed as part of a research effort (that is algorithm).

(2) Software integrated into, and necessary to operate an Army asset such operating systems and firmware. Such software is subject to capitalization criteria of the asset in which it is integrated and capitalized accordingly.

(3) Software that the Army does not own outright or for which the Army does not own a capital lease to operate.

(4) Data conversion, maintenance, and training costs.

(5) Costs incurred solely to repair a design flaw in the software.

(6) Costs incurred to develop "free software" to be released to the public or other Federal agencies for purposes of advancing scientific and technological knowledge.

(7) Table 3–1 illustrates specific development activities that will be capitalized and reported.

g. CIO/G–6 will develop comprehensive guidance to provide detailed instructions to commands on how to account for their respective IUS assets.

Table 3–1
Capitalization of development cost

Project phase	Task	Treatment
Preliminary design: Conceptual planning/Planning and requirements	Project evaluation or need determination	Expense
	Concept formulation and testing	Expense
	Evaluation and testing of alternatives	Expense
	Project approval	Expense
Software development: Design/Development and testing/Implementation	Design, including software configuration and software interfaces	Capitalize
	Coding	Capitalize
	Installation to hardware	Capitalize
	Project personnel costs	Capitalize
	Testing, including parallel processing	Capitalize
	Quality assurance testing	Capitalize
	Technical documentation, including user manuals	Capitalize
	Data conversion software	Expense
	General and admin costs	Expense
Operational software: Operations and maintenance/Disposition	Enhancements	Capitalization criteria dependent

Table 3–1
Capitalization of development cost—Continued

	Training	Expense
	Data conversion, includes cleansing, deleting, and repackaging of data	Expense
	Help desk	Expense
	Application maintenance/Bug fix	Expense

3–16. Execution

a. All hardware and software solutions must be acquired through CHESS or CHS procurement vehicles or receive an approved waiver through the ITAS, available at https://cprobe.army.mil/enterprise-portal/web/itas/home. IT solutions will be implemented in accordance with an approved business case in conjunction with governance reviews to ensure both milestones and expected results are realized.

b. When obligating funds for IT resources, the element-of-resource/commitment item codes must be specified in the obligation documentation from the list of approved elements of resource/commitment item codes (see DA Pam 25–1–1).

Section IV

Procurement

3–17. Mandatory sources for procurement

There are a number of Army IT policies that govern the procurement of IT solutions. The type of IT solutions being procured will dictate which policies or processes will be followed. These policies will be addressed in the sections below. The mandatory source for all COTS IT hardware and software is CHESS. The mandatory source for commercial IT hardware for tactical/operational requirements is CHS. Commands and agencies will track, manage, and report inventory for enterprise software licenses and hardware inventories in accordance with this regulation and as described in DA Pam 25–1–1. The applicable Authorizing Official must approve software, including new software packages, software upgrades, free software, freeware, shareware, and unlicensed open source software, prior to installation.

3–18. Army information technology service management

This process applies when developing or maintaining enterprise services. The Army will follow the DOD Enterprise Service Management Framework (DESMF) to implement Information Technology Service Management (ITSM) as the basis for Army Enterprise Service Management (AESM). The intent of AESM is to continually increase effectiveness, improve security, and gain efficiencies in Army IT services by standardizing the service delivery process. For more information on the roles and responsibilities for the AESM Framework, refer to the Secretary of the Army Memorandum, Subject: Army Information Technology Service Management (ITSM) Policy, dated 17 November 2014. The AESM pertains to all Army-managed enterprise IT services. An ITSM Office (ITSMO) will be identified and recognized at a future date once the foundation of the AESM framework has stabilized and a repeatable process of managing IT services is established and followed by Army stakeholders. The ITSMO mission is to—

a. Establish and implement Armywide ITSM process to ensure customer-centric IT services are aligned with IT mission requirements through standardized processes, people, technology, and governance.

b. Centrally manage the development, implementation, support, and improvement of enterprise IT tools and services across the Army.

c. The process must be integrated with the enterprise IT governance processes to ensure proper visibility of enterprise services and effectively manage risk.

3–19. Commercial off-the-shelf products and services

The CCA and other Federal policies, laws, and directives require the maximum use of COTS and non-developmental item products and services. DODD 5000.01 identifies the DOD order of preference in capability acquisition. The first order of preference is the procurement or modification of commercially available products, services, and technologies from domestic or international sources, or the development of dual-use technologies.

a. Each system program manager or acquiring organization will establish a baseline and maintain an inventory of its commercial IT and NSS software assets, non-commercial IT and NSS software assets, commercial IT and NSS services, and noncommercial IT and NSS services in APMS. The baseline will be developed and maintained at the system or program level, and at a component summary level. The baseline will be reported to the MA domain owner, and it will enable

Army leaders and managers to determine the status of commercial IT and NSS software and services, plan for increasing their use, and measure progress toward achieving the DOD goal.

b. To ensure accountability for accelerating the use of commercial solutions in DOD and to obtain senior leadership visibility into the progress towards achieving this goal, each program manager or acquiring organization must annually confirm that its system is in compliance with the above and report the results achieved toward meeting the goal of increasing the use of commercial IT and NSS in the Army.

c. Acquisition program dollars will not be used to fund IT services that are defined as baseline in the most current version of the Army-approved C4IM services list.

d. CHESS is the mandatory source for all COTS IT software and hardware. The purchase of IT software and hardware from a non-CHESS vendor requires a statement of non-availability from Product Development (PD) CHESS and an approved ITAS waiver from CIO/G–6 prior to submission of the procurement request to the appropriate contracting channel. All waiver requests must include a statement of non-availability and justification explaining the extenuating circumstances or unique configurations required by the mission or reason for not purchasing through CHESS. The CHESS contract vehicles and electronic market (e-mart) are available at https://chess.army.mil/. Requests for waivers may be submitted through the same website.

e. CHS is the mandatory source for all commercial IT hardware to meet tactical/operational requirements in accordance with the AFARS, Part 5139, Acquisition of Information Technology, dated 29 August 2016. CHS coordinates across Army organizations to modify commercial information technology hardware to meet operational requirements for transport or ruggedization, to ensure configuration management, to support end-of-life configuration changes, or to support organizational requirements that are not well defined. CHS provides software primarily for operating systems, basic input/output systems, and firmware purposes. Organizations that receive written authorization from CHS to use a CHS contract for hardware or services are exempt from the requirement to obtain an approved ITAS waiver or CHESS SoNA.

f. Commercial mobile wireless devices (for example, cell phones, smartphones, and electronic tablets with cell capability) are provided in the service plans of wireless contracts under the Army-Air Force Wireless NexGen Blanket Purchase Agreement. See AR 25–13 for managing usage of commercial mobile wireless devices under multifunction or portable electronic devices (PEDs).

g. Product Lead CHESS acts as the Army's Software Product Manager within the Department of Defense Enterprise Software Initiative (DOD ESI) on behalf of the CIO/G–6.

3–20. Enterprise agreements

a. ELAs and enterprise service agreements (ESAs) are types of enterprise agreements to license COTS software that have been required and validated by two or more ACOMs or Army staff elements. An ELA or ESA facilitates maintenance, service, or license procurement to the entire population of an entity. Licenses obtained via ELAs are distributed through a centrally managed process led by the CIO/G–6. ELAs and ESAs are designated as enterprise assets that leverage economies of scale in procurement of licenses or services. Army organizations will use ELAs or ESAs when at all possible.

(1) The CIO/G–6, ASA (ALT), and AMC will evaluate potential Army ELAs or ESAs.

(2) The CIO/G–6 will—

(a) Develop and approve enterprise license agreements.

(b) Define and develop a business approach to capture technical requirements from commands to determine the feasibility, necessity, and continuance for an ELA or ESA.

(c) Develop and perform requirements analysis and collection, business case analysis, justification, market research, funding strategies and IT policy in support of the acquisition strategy and planning to procure software licenses and service agreements on an Enterprise scale.

(d) Manage the post award activities of ELA or ESA renewal payment executions, annual software inventory audits, and the validation of license entitlements across Army commands.

(e) Report actual sales, utilization, owned license quantities, overall product spend and capitalization of entitlements to commands.

(f) Serve as the review and approval authority for waiver requests through ITAS.

(g) Serve as the review and approval authority for IT software procurements ordered through CHESS.

(h) Issue IT Governance and guidance as required in the management and oversight of ELAs and ESAs.

(3) The CIO/G–6 will manage ELAs and ESAs (and any Joint ELAs) with contract support provided by AMC designated offices and programmatic support from ASA (ALT).

(4) The CIO/G–6 in conjunction with PL CHESS, will manage COTS hardware and software enterprise agreements. The major activities of acquisition planning, contract development, life cycle management and strategic communication will be the framework for ELA and ESA management.

(5) CHESS, as managed by ASA (ALT), is the Army's designated software product manager and the mandatory source for all software through the ELAs. CHESS also manages the consolidation of licenses for enterprise and non-enterprise groups of customers consolidating their requirements to obtain more favorable prices, terms, and conditions.

(6) All Army ELAs and ESAs must comply with DOD ESI. The Defense Federal Acquisition Regulation Supplement, subpart 208.74, which details enterprise agreements, requires DOD components to fulfill requirements for COTS software and related services such as software maintenance in accordance with the DOD ESI. This includes purchasing from the DOD inventory before using any other source. DOD enterprise agreements, negotiated with specific Original Equipment Managers or their agents, provide the best available prices, terms, and conditions. Organizations should consult with CHESS, the Army representative to the DOD ESI, before re-negotiating any of the terms or conditions of an ESA. The DOD ESI is the DOD implementation of the Federal-wide Software Managed and Acquired on the Right Terms (SmartBUY) program. ELAs and ESAs that have been designated as SmartBUY agreements are mandatory for use when requirements evaluation has led to the designated brand name software product or service. SmartBUY and other ESI policies are available on the CHESS website at https://chess.army.mil.

b. Information Technology Enterprise Solutions – Software (ITES–SW) contracts are the Army's mandatory source for the purchase of COTS software products and related services via CHESS that have obtained full Army approval under the following categories: IT Utility and Security; Modeling and Simulation; Multimedia and Design; and Program and Development. Customers must obtain a SoNA from CHESS and an approved ITAS Waiver from the CIO/G–6 if they wish to purchase outside of CHESS. The scope of the ITES–SW contract includes COTS software products and related services that have obtained full approval applicable under the following categories: IT Utility and Security; Modeling and Simulation; Multimedia and Design; and Program and Development. Additional information on ITES–SW is available on the CHESS website at https://chess.army.mil.

c. Army organizations (including contractors purchasing IT intended for use by Army organizations) or NECs will coordinate acquisition plans with PD CHESS regarding planned acquisition of specific products.

(1) CHESS, in coordination with CIO/G–6, will determine the most cost-effective method for obtaining the licensing, such as improving the existing ELA/ESA or establishing a new agreement.

(2) CHESS, in coordination with CIO/G–6, is responsible for authorizing new ELAs and ESAs; and CHESS is responsible for granting/issuing SoNAs when software is not available from one of these or other CHESS-managed agreements.

(3) CIO/G–6 is responsible for granting/issuing approved ITAS waivers for organizations to acquire COTS software from sources other than CHESS.

(4) The CHESS website is https://chess.army.mil. The DOD ESI website, which lists all ESI-managed software, is available at http://www.esi.mil.

d. Exceptions.

(1) Commands and agencies who wish to procure COTS hardware or software, not currently provided by CIO/G–6 or CHESS-managed license agreements and where no other reasonable product is available, will submit a SoNA followed by an ITAS waiver request through the CIO/G–6 ITAS site. CHESS and CIO/G–6 will review and make final determinations.

(2) Refer to DA Pam 25–1–1 for specific descriptions business processes described above for managing COTS hardware and ELA/ESA enterprise agreements.

3–21. Leasing information technology assets

Commands and agencies who wish to lease hardware and software will follow the same process as if purchasing hardware and software (see DA Pam 25–1–1).

3–22. Modifications

Software applications, whether combined with hardware or as separate end items, are subject to the same procedures regarding modifications as other IT. Software applications that are approved for standardized use across multiple commands will have one configuration manager assigned by AMC. The configuration manager will establish and publish procedures that identify which organizations are using the application, track when an organization discontinues use, and let users recommend required, post-production software support changes and enhancements. ASA (ALT) must approve the cancelation of post-production software support for any software application approved for standardized use.

3–23. Information technology and national security systems acquisition process

The acquisition process begins when an organization's C4 and IT needs have been established and approved in the appropriate capability documentation. The appropriate capability documentation is published by DCS, G–3/5/7. The acquisition process is outlined in AR 70–1.

a. The CIO/G–6 will perform a compliance assessment on all ACAT I, II, and special-interest programs for 40 USC Subtitle III (Clinger-Cohen Act) compliance in accordance with DODI 5000.02. Programs are required to conduct a self-

assessment based on the CIO/G–6 assessment criteria, which serves as the basis for the required evaluation. In support of the milestone decision for ACAT I, II, and special-interest programs, an CIO/G–6 CCA compliance assessment determination will be completed prior to a milestone and FRP/FDD decision.

b. The responsibility for CCA compliance assessments for ACAT III programs is assigned to the Army MDA for the Joint program executive office, PEO, direct reporting PMs, Army commands, and agencies of the program. The responsible organization will perform the compliance assessment and determination in accordance with DODI 5000.02. When the compliance determination for ACAT III programs is complete, the determination will be forwarded to the CIO/G–6, who retains Title 10, United States Code, C4, and IT acquisition oversight.

c. The CCA determination applies to ACAT programs, Business System programs and Service (S)-CAT contracts. The CIO performs compliance assessments and determinations on ACAT programs prior to a milestone and full-rate production decision; on Business Systems prior to the acquisition acceptance test procedure (ATP) and limited and full deployment ATPs; and on service category service contracts prior to contract award. The ACAT or Business System Category program or Service contract PM or functional service manager is required to provide a streamlined assessment to serve as the basis for the required CIO/G–6 compliance assessment and determination.

3–24. Service and support agreements with Department of Defense activities

a. Army IT organizations will provide requested support to other DOD activities when the head of the requesting activity determines it would be in the best interest of the U.S. Government, and when the head of the supplying activity determines capabilities exist to provide the support without jeopardizing assigned missions. The service provider will provide an SLA for delivery of IT services. A service and support agreement with an associated SLA will be negotiated between the two activities to specify the types and level of services and basis for reimbursement. The supporting NEC must be a participant in the interconnection security agreement (ISA) coordination in accordance with NIST SP 800–47. An ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability of information between agencies. Depending upon the scope of the ISA, the respective signal command may be included as a third-party.

b. Army activities may enter into support agreements with non-DOD Federal activities when—

(1) Funding is available to pay for the support.

(2) The agreement is in the best interest of the U.S. Government.

(3) The supplying activity is able to provide the support.

(4) The support cannot be provided as conveniently or economically by existing DOD services or commercial enterprise.

(5) It does not conflict with any other agency's authority.

c. These determinations must be approved by the head of the major organizational unit ordering the support and specified in an ISA or SLA.

Section V

Implementation and Fielding

3–25. Configuration management

Configuration management (CM) procedures ensure that the Army maintains accountability for and control of changes to the fielded software baseline. The baseline identifies systems that have been certified interoperable and determined satisfactory for operation as a component of the Army network. The CM process is managed by the CIO/G–6, Cybersecurity and Information Assurance Directorate, SAIS–CBC.

a. The Army Interoperable Certified Fielded Baseline (AICFB) Report serves as the document of record for the current Army Certified Baseline. The AICFB Report is released quarterly. Each AICFB Report is published with a unique baseline change number.

b. The quarterly AICFB Report identifies—

(1) New or changed software versions that have been certified interoperable and are authorized to operate as a component of the Army network.

(a) Systems, system software versions, and baseline segments that have been approved for removal from the baseline. Verification that the systems and system software versions are no longer fielded is accomplished during the removal request processing.

(b) Systems that have been approved via the Interoperability Capabilities and Limitations Assessment; Waiver; and Exemption processes.

(2) Central Technical Support Facility (CTSF), Fort Hood, TX, maintains the configuration management database and CM library. The CTSF ensures that all artifacts associated with the AICFB are catalogued and maintained under CM control.

3–26. Information support plans

a. An approved ISP is a requirement for all IT and NSS programs, unless specifically granted a waiver (to include ACAT programs that connect to the communications and information infrastructure). It identifies and documents information needs, infrastructure support, and IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability, and sufficiency concerns. The ISP is initiated prior to milestone B and updated prior to Critical Design Review, Milestone C, and post-Milestone C whenever there are changes to the system during life cycle sustainment that effect interoperability. An ISP of record is required for Joint interoperability certification (see DODI 5000.02 and DODI 8330.01).

b. The CIO/G–6, Cybersecurity and Information Assurance Directorate manages the Army ISP staffing and approval process. CIO/G–6 is the Army's link with the JS Command, Control, Communications & Computer/Cyber Directorate (J–6), Requirements Division, and Architecture Branch for the certification of the Net-Ready-Key Performance Parameters (see CJCSI 5123.01H) and the DOD–CIO on ISP guidelines and program compliance. For more information, see DA Pam 25–1–1. The CIO/G–6 is the Army's approval authority for all Army ISPs.

(1) As part of the ISP, the PM must submit architectural views to describe the interoperability requirements of the IT solution. The ISP review process will assist the PM to refine these views, and results in a set of detailed measurable criteria for use in interoperability test and certification.

(2) PMs must develop the ISP online by entering system information through the GTG–F portal (https://gtg.csd.disa.mil). ISP formatting and content requirements are specified by the GTG–F and described in the DAG. Deviations from these requirements require the CIO/G–6 approval. Until GTG–F is available on the Secret Internet Protocol Router Network, Secret ISPs are submitted and approved using the DISA Interoperability and Supportability Legacy Data Repository. PMs submit Top Secret ISPs using a staffing notification on the appropriately classified network that includes the location of the document on the Joint Worldwide Intelligence Communications System and the points of contact. Classified ISPs use the format and content requirements described in the DAG until the GTG–F is available on the appropriately classified network.

(3) The CIO/G–6 will lead the Armywide review of all ISPs. The roles and responsibilities section of this document direct those organizations required to review and provide comments for ISPs (see DA Pam 25–1–1).

(4) The CIO/G–6, Cybersecurity and Information Assurance Directorate, SAIS–CBC, serves as the Army voting member to the ISG, the governing body for Joint interoperability requirements, acting as the interface between the DOD–CIO, JS, PMs, System Sponsors, and JITC for all issues related to waivers to policy, requests for interim certificates to operate or Joint interoperability certification.

c. Army information technology standards.

(1) Standard/IT Standard(s) are common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods, and related management systems practices. Standards include the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

(2) All Army IT systems will comply with the applicable IT standards contained in the GTG–F portal (https://gtg.csd.disa.mil), DOD IT Standards Registry (DISR), and (ATGR) (https://www.kc.army.mil/trm_tool/) via ArCADIE's Magic Draw Teamwork Server. Exceptions to this requirement are permitted only via a waiver or an approved CR as specified in DODI 8330.01. Architectures must also conform to DOD IEA and Federal architecture policies and directives. The ATGR can also be accessed via the CIO/G–6 Enterprise Architecture website (https://ciog6.army.mil/architecuture/tabid146/default.aspx).

(3) The Army IT standards waiver and change request processes will be completed in accordance with Annex A, IT Standards Guidance to DODIN–A End-to-End Enterprise Architecture for all IT Standards (for example, data, CYBER, system, performance, design, naming, or process).

3–27. Information technology support principles

a. Information transmission economy and systems discipline. All Army organizations will implement procedures to promote the optimal responsive, cost-effective use of all types of DOD information systems and services and ensure the application of sound management practices in accomplishing information system services' economy and discipline (see also DODI 8100.04, DODD 8000.01, and DA Pam 25–1–1).

b. Continuity of operations. HQDA and operational organizations (such as JFHQ–States for the ARNG) must ensure the uninterrupted execution of their respective essential missions and functions under all probable conditions. As noted in AR 500–3, the HQDA COOP plan is the model upon which organizations will create their COOP plan, which must include procedures for the relocation of key leaders and staff to an alternate site(s), plans for the protection of critical records and

files, and provisions for establishing minimum essential operational capabilities at relocation facilities. HQDA staff elements, ACOMs, and other separate reporting organizations are required to maintain a COOP plan consistent with AR 500–3. An IT contingency plan is one essential element of COOP. At a minimum, each critical and essential C4 and IT system must be supported by its own contingency plan that ensures its continuous operation or restoration within specified timeframes determined during COOP planning. For guidance and procedures related to IT contingency planning, refer to DA Pam 25–1–2. All COOP plans must be tested at least annually.

c. Network-centric applications and support. It is Army policy to employ net-centric concepts to support essential missions and functions. The cornerstones of net-centric information-sharing are to make data visible, accessible, and understandable while also promoting trust. Implementation of net-centric concepts to streamline processes will provide producers and consumers with capabilities to save manpower, reduce redundancy, increase accuracy, speed transmission, increase information availability, and allow functions that would be impractical or impossible without their use.

3–28. Information technology support services for Army organizations on Army installations

Information technology support services consist of the following four categories: baseline, enhanced, mission-funded, and mission-unique. These services are described in the Army C4IM services list and DA Pam 25–1–1. The current approved C4IM services list and customer-facing DODIN–A Services Catalog is available at https://www.itmetrics.hua.army.mil/.

Section VI

Oversight

3–29. Management control mechanisms

The Army uses a number of processes and tools to conduct oversight of the implementation and fielding of IT solutions. These processes are management control mechanisms to enforce policy and standards, measure performance, and provide visibility of IT investments to Army leadership.

3–30. Army request for information technology

a. Army Request for Information Technology (ARFIT) is the Army's program for gaining visibility and accountability of the Army's IT spending and enforces compliance with Army IT policy in the year of execution. It is the Army's approach for approval and oversight for all IT expenditures, except for IT embedded in weapons systems or funded by NIP or MIPs. ARFIT promotes the use of cost-efficient enterprise procurement vehicles like CHESS or CHS.

b. ARFIT establishes Army policy and processes for the procurement of all information technology hardware, software, and services, without a cost threshold and regardless of the appropriation or type of procurement. A joint effort between the CIO/G–6 and 's OBT, ARFIT creates a single integrated process consistent with the Clinger-Cohen Act of 1996, which requires responsibility, authority, and accountability at all echelons, while giving visibility of all IT procurement at the enterprise-level.

(1) The ARFIT approval process covers all execution-year IT hardware, software, and services purchased with Army appropriated, non-appropriated, and Army Working Capital Funds and other DOD funds used to support Army IT investments An exception is granted (no ITAS waiver is required) for the purchase of expendable/miscellaneous IS supplies (CDs, printer cartridges, and so forth) or computer peripheral devices (cables, keyboards, mouse, and CAC readers) under the amount of $500 per purchase.

(2) The ARFIT process is managed using the ITAS tool. All IT requests for Military Intelligence (MI) Programs and Sensitive Compartmented Information Facility Information Technology must be processed through the ARFIT–MI process.

(a) The ARFIT–MI process is for NIP, MIP, and Sensitive Compartmental Information Facility Information Technology funds and must be processed through the ARFIT–MI process.

(b) Organizations must obtain a waiver from the HQDA DCS, Intelligence (G–2)/ Department of the Army Intelligence Community Information Management Directorate (DAMI–IM) to use non-IT programmed MIP or NIP funds for the acquisition of all IT hardware, software, and services valued at or over $10K for Operations and Maintenance, Army, and $100K for Research, Development, and Acquisition. Funding thresholds are cumulative and IT expenditures span all hardware, software, development, services, contractor support, testing, licenses and maintenance fees, web site and portal expenses, and audiovisual and communications capabilities.

(c) An approved ARFIT–MI web account must be active to request ARFIT–MI waivers.

(d) ARFIT–MI resides on secure internet protocol router network (SIPRNET) located at https://asid.daiis.mi.army.smil.mil.

(3) ARFIT promotes the use of mandatory enterprise contractual vehicles to include—

(a) CHESS – Scope: COTS IT including WiFi wireless.

(b) Army-Air Force Wireless (NexGen) Blanket Purchase Agreement – Scope: Wireless (Cellular) end-user devices.

(c) Product Manager Joint Automatic Identification Technology – Scope: Radio Frequency Identification Devices.

(d) CHS – Scope: Configuration managed IT.

(4) ARFIT also supports IT policies outside of the CIO/G–6. These policies include—

(a) AFARS 5139.101. An ITAS waiver is required for hardware and software purchases outside CHESS/CHS contracts.

(b) AD 2016–38. An ITAS approval memo is required for the expenditure or commitment of funds related to data center IT investments, including hosting services (including commercial and private cloud hosting), hardware, software, storage, or other services associated with a data center before executing funds, regardless of whether the item is purchased through CHESS.

(c) DCS, G–3/5/7 annual funding guidance that requires an ITAS approval memo for life cycle of MTOE COTS IT purchases.

(d) Command policies that direct the use of ITAS for some or all IT purchases.

3–31. Army interoperability certification

The CIO/G–6 is the AIC Authority. The Army Interoperability Certification process enables assessment and certification of horizontal and vertical interoperability, with an acceptable cybersecurity defense posture, of all Army IT/NSS systems, regardless of Acquisition Category. All IT/NSS programs under Army management, including Joint programs and technology demonstrations, require an assessment and issuance of an AIC determination prior to all Material Release decisions.

a. The CIO/G–6 Cybersecurity and Information Assurance Directorate manages the AIC process, issues AIC policy, approves AIC procedures, and issues AIC determinations for Army IT/NSS systems with an acceptable cybersecurity defense posture/approves Verification, Validation, and Accreditation for all Simulation, Stimulation, or Emulation services used to support AIC test execution; and serves as the tri-chair for COE Test, Evaluation, & Certification Senior Management Group, that establishes interoperability test and evaluation requirements.

b. To obtain performance analysis on which to base an AIC determination, the Army partners with the other Services, Federal agencies, coalition mission partners and test agencies to leverage and synchronize test events and test data. The goal is to optimize interoperability assessments, conducted under representative operational conditions, gain schedule efficiencies, and reduce testing costs, with the intent to provide proven and certified interoperable and secure capability to the user in a timely manner.

c. The FaNS environment and its methodologies provide the Army agile, efficient, and persistent distributed capabilities for integration, interoperability testing, and Cybersecurity SoS Network Vulnerability Assessment. The FaNS environment is made-up of developmental integration and test facilities from across the DOD that meet specific network requirements and are accredited by the CIO/G–6 to conduct configuration management, cybersecurity, physical security, and test functions necessary to and to perform AIC testing.

d. Systems are tested to ensure acceptable performance against approved interoperability requirements as documented in system associated capabilities documents (Joint Capabilities Integration and Development System or Business Capability Life Cycle) or ISPs. Integrated multi-system performance requirements are documented in the form of a set of mission threads representing the combined approved interoperability requirements of the associated systems. The mission threads are the basis for test cases that are used to access digital interoperability and support the AIC determination process. An AIC certifies that:

(1) An IT/NSS, or groups of IT/NSS systems, can successfully perform its technical (digital/automated processes) interoperability requirements.

(2) An IT/NSS system can securely generate and utilize relevant information as expected in order to execute specified operational processes.

(3) An IT/NSS system is able to perform successfully its end-to-end information-sharing functions without adversely impacting its intended network environment(s).

(4) An IT/NSS system is backwards interoperable with previously certified software.

e. The CIO/G–6 Cybersecurity and Information Assurance Directorate resources, directs, and ensures the Army Research Laboratory's Survivability/Lethality Analysis Directorate conducts a SoS Network Vulnerability Assessment in conjunction with each AIC event to inform the system Authorizing Official and to inform Army leadership of systems vulnerabilities and the cybersecurity defense posture in a system-of-systems environment.

f. The CIO/G–6 Cybersecurity and Information Assurance Directorate approves all changes to the fielded software baseline component of the Army's operational network to reduce and prevent negative impacts to systems interoperability.

g. See DA Pam 25–1–1 for AIC procedures.

3–32. Coalition interoperability assurance and validation

The CIO/G–6 will support CIAV, which is designed to conduct end-to-end analysis of mission-based interoperability effectiveness of operational Coalition mission threads through validated operational and technical requirements. Coalition mission threads are the end-to-end sets of activities and data required to successfully execute an element of an operational mission, such as battlespace management and joint fire support. CIAV uses the full range of DOTMLPF–P solutions to properly validate information exchange effectiveness

3–33. Army data management

Data is a strategic asset and must be managed as such. The ADMP manages enterprise data through the Army Chief Data Officer, the Army Data Board, and the Army DS. The goal is to create and support a data-enabled environment that gives decisionmakers access to authoritative data in a timely and secure manner.

a. Army data management program. The ADMP provides governance needed to meet the Army's data management objectives. The programmatic objective is to integrate Army DM practices into a unified, consistent, and comprehensive body of DM guidance. For more information on the ADMP, see DA Pam 25–1–1 and https://www.milsuite.mil/wiki/portal:army Data Management Program.

b. Army data strategy. The ADMP implements the Army Data Strategy. The Army Data Strategy, aligned to the DOD Data Strategy, guides the Army towards ensuring data, information, and IT services adhere to VAUTI goals. System design (existing and new) will incorporate Army Data Strategy guidance.

c. Data governance. Army Data Governance consists of the ADB led by the CDO. The ADB is composed of Army DSs. The ADB fosters a collaborative governance environment for achieving Army Data Strategy goals, with active participation from across the Army.

(1) The ADB is the senior enterprise governance body responsible for Army DM and is chaired by the CDO. For more information regarding the ADB, see https://www.milsuite.mil/wiki/army_data_board. The ADB—

(a) Develops coordinated Army enterprise positions on data strategy, standards, and execution.

(b) Adjudicates Army enterprise data issues.

(c) Coordinates data sharing efforts across the Army enterprise.

(d) Recommends certification of data standards to the CDO.

(e) Collects and disseminates best practices and lessons learned for the data community.

(f) Serve as a certification/waiver approval authority for targeted standards as delegated by the CDO.

(2) The CDO serves as the senior advisor to the SECARMY and the CSA on data issues; reports to the CIO; and chairs the ADB. The CDO—

(a) Oversees the development and execution of the Army Data Strategy.

(b) Develops, implements, and matures the ADMP.

(c) Identifies Army DSs in areas as necessary, other than the Assistants Secretaries of the Army, DCSs, and ACOMs.

(d) Develops and coordinates the management and integration of data-related architecture and engineering products with operational, system, and technical architecture products for communities of interest and other data governance bodies.

(e) Provides direction to the Army DSs.

(f) Oversees the activities of the ADC.

(3) Army DSs are subject matter experts in their area's data, operational requirements, and processes. Under the direction of the CDO, the Army DSs are responsible for developing, implementing, and enforcing Federal, DOD, Army, and their organization's data standards, processes, and procedures. The Army DSs will—

(a) Serve as a voting member of the ADB.

(b) Convene data forums to oversee and manage data issues specific to their domain.

(c) Develop organizational Data Management Plans that implement the guidance and direction of the ADMP, the Authoritative Data Sources, and the AIA.

(d) Provide coordination, integration, and maintenance of other related data standards and products identified as critical to the success of achieving data interoperability.

(4) Authoritative Data Sources are recognized or official data-production sources with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers.

(a) Army organizations producing or maintaining data will identify, register, and publish ADSs in the data services environment (DSE) in accordance with DODI 8320.02, as the primary resource for searching for and identifying existing data services; and in accordance with DODI 8320.07 for registration of data engineering resources (DER) in the DSE.

(b) The ADB will review and approve all Army ADSs.

(c) Army organizations with a need for data will use registered and approved ADSs.

(5) Metadata—There are three types of metadata: structural, descriptive, and semantic. Structural metadata are data about the containers of data. Descriptive metadata use individual instances of application data or the data content. Semantic

metadata provides insight into the meaning and context of an asset to include content-related details such as data standards. Organizations producing and maintaining data will –

(a) Identify, register, and publish all required metadata (discovery, structural, and semantic) in the DSE to facilitate enterprise search, discovery, and use.

(b) Ensure discovery metadata conforms to the DISR Standards for all data assets posted to shared spaces.

(6) Army Data Quality Management—Organizations producing or maintaining authoritative data sources will incorporate a comprehensive data quality management program as part of their data-production and maintenance activities that advocates a "First Time Correct" strategy. The 'First Time Correct' strategy states data will be created correctly the first time (see International Standards Organization (ISO) 8000).

(7) Army Data Metrics – data metrics measure data, information, and IT Services performance and progress towards solutions needed in meeting the Army's strategic goals and objectives. Data metrics ensure data, information, and IT services meet the VAUTI goals. Data metrics help the Army determine the current level of data, information, and IT service solutions, and provide the ability to evaluate improvement over time. All Army DSs will establish a data metrics plan within their area of responsibility to effectively measure or monitor the progress of the Army Data Strategy objectives.

(8) Information Exchange Specifications (IES)—An IES is a set of materials that specifies how data are to be exchanged between software applications. An IES defines a particular data exchange and explains what developers must know to write code that produces or consumes an instance of that exchange.

(a) Army DSs are responsible for governing the information exchange specifications used within their area of responsibilities.

(b) Industry-standard IESs with commercial and open source implementations must take precedence over new IES development.

(c) Data exchanged between information systems conform to an IES.

(d) Army organizations will coordinate with other DOD Components and communities of interests to identify potential enterprise data and service standards, specifications, and DERs, including international, commercial, and Federal sources.

(9) National Information Exchange Model (NIEM)—a set of common, approved XML data elements and definitions vetted through the international, Federal, state, local, tribal, and private sectors developed to increase information-sharing between organizations.

(a) Army organizations will consider a "NIEM-First" strategy in accordance with DODI 8320.07 for new system and systems being modernized when developing an XML-based information exchange specifications.

(b) When NIEM is not the most efficient or effective means to address an information-sharing requirement, organizations will document the technical, fiscal, and operational reasons why the alternative approach is better and will submit a request for an exception to the "Consider NIEM-First" policy to the DOD–CIO, as described in DODI 8320.07.

(10) Unique identifiers—

(a) All major Army information and data assets will be assigned a globally unique identifier (UID) per DODI 8320.03.

(b) UIDs support data integration, referential integrity, and data interoperability by providing a single and consistent identifier with which to refer or designate a given Army asset.

(c) Army organizations will designate a role responsible for managing and assigning UIDs within the organization.

(11) Army data standards.

(a) Data Standards refer to any kind of documented guidance, practices, specifications, manuals, methodologies, procedures, or official "standards" that are developed and/or published by recognized Standards Development Organizations (for example, ISO, American National Standards Institute) that focus on data or data management topics. Thus, data standards underline all data management functional areas and are the collection in totality of all data management guidance artifacts across the Army.

(b) Data standards will be used to guide and govern the implementation of data-related IT capabilities established in the Army Data Strategy. Approved data standards are registered in the DISR. Data standards not found in DISR may be approved, applied/enforced, and managed in the ATGR and will not contradict, supersede, or duplicate DISR standards (see DA Pam 25–1–1).

(c) Army organizations will—

1. Implement applicable "Mandated" standards and specifications as cited in the DISR (accessible at https://gtg.csd.disa.mil), or any future DOD-designated registry for IT and data sharing standards in accordance with DODI 8320.02.

2. Validate that implementations of the data standard conform to the standard and maintain proof of conformance.

3. Provide feedback to the Army Standards Council and ADB.

(d) Army DSs will—

1. Ensure a standard does not exist before creating a new one to meet organization-local requirements.

2. Develop and approve a needed data standard as part of coalition of stakeholders (for example, a COI) with an interest in and need for the capability provided by the standard.

3. Thoroughly test and validate the capability provided by the standard prior to approval.

4. Submit approved standards to standards registry in the highest echelon at which the data standard may be needed (for example, DISR if DOD-wide applicability).

(12) RMF Data Requirements.

(a) All Army IT that receives, processes, stores, displays, or transmits Army information is subject to the Army implementation of the DOD RMF, in accordance with AR 25–2, DODI 8510.01 and the DA Pam 25–2-14's policy and procedures for assessing and managing risk per the Committee on National Security Systems and NIST issuances. Army IT is broadly grouped as information systems, PIT, IT services, and IT products. It includes IT in tactical environments, IT that supports research, development, test, and evaluation, and Army-controlled IT operated by a contractor or other entity on behalf of the Army.

(b) IT will be registered in accordance with AR 25–2 and DODI 8510.01 in the DOD-provided registry, the Enterprise Mission Assurance Support Service (eMASS), or its successors. Refer to US Army Component Workspace on the DOD RMF Knowledge Service (https://rmfks.osd.mil), for Army-specific implementation guidance.

(c) All Army system and data owners must be identified in accordance with AR 25–1 and the Army Data Board Information System.

3–34. Records management

a. Records management mission. The mission of records management is to capture, preserve, and make available evidence essential for Army decisions and actions; meet the needs of the American public; and protect the rights and interests of the Government and individuals.

(1) OMB and the National Archives and Records Administration (NARA) issued a joint Managing Government Records Directive (OMB M–12–18) mandating that agencies eliminate paper in favor of electronic means of recordkeeping. The elimination of paper will proliferate the accumulation of electronic data resulting in significant reduction in paper records storage costs to the Department of the Army.

(2) All Army organizations are encouraged to implement a disciplined and repeatable process that directs personnel to review electronic documents, identify records, and delete any information that is not required for business purposes or is a non-record. To the greatest extent possible, records should be identified at the time of creation.

(3) Additional guidelines for managing records are contained in DA Pam 25–403.

b. Records management regulation. The records management program is defined and described in AR 25–400–2.

3–35. Quality of publicly disseminated information

a. Freedom of information act. Information and the data from which information is derived are broadly categorized as public domain and nonpublic domain. Public domain data or information is Government-owned and is not personally identifiable, classified, subject to a Freedom of Information Act (FOIA) or Privacy Act (PA) exemption, or otherwise considered to be sensitive.

b. Army Freedom of Information Act and privacy office. The Army FOIA and Privacy Office is responsible for management oversight of the Armywide implementation of the FOIA, PA, and Quality of Information programs. Requests for nonpublic data from private individuals and organizations should be coordinated with and referred to the local FOIA or PA official for determination of whether or not the data are releasable. Refer to AR 25–55 for further information on the Army FOIA Program and to AR 25–22 for further information on The Army Privacy Program.

3–36. Army information technology standards

All Army IT systems will comply with the applicable IT standards contained in the DOD IT Standards Registry (DISR) (https://gtg.csd.disa.mil/disr/dashboard.html) and in the ATGR (https://www.kc.army.mil/trm_tool/)**.** Exceptions to this requirement are permitted only via a waiver or an approved CR as specified in DODI 8330.01. Architectures within the AEA must also conform to DOD IEA and Federal architecture policies and directives. The ATGR can also be accessed via the CIO/G–6 Enterprise Architecture website (https://ciog6.army.mil/architecuture/tabid146/default.aspx), as well as via ArCADIE's Magic Draw Teamwork Server.

a. Army information technology standards.

(1) IT Standard(s) are common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods, and related management systems practices. Standards include the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

(2) All Army IT systems will comply with the applicable IT standards contained in the Global Information Grid Technical Guide-Federated (GTG–F) portal (https://gtg.csd.disa.mil), DOD IT Standards Registry (DISR) and ATGR (https://www.kc.army.mil/trm_tool/) via ArCADIE's Magic Draw Teamwork Server. Exceptions to this requirement are permitted only via a waiver or an approved CR as specified in DODI 8330.01. Architectures must also conform to DOD IEA and Federal architecture policies and directives. The ATGR can also be accessed via the CIO/G–6 Enterprise Architecture website (https://ciog6.army.mil/architecuture/tabid146/default.aspx).

(3) The Army IT standards waiver and change request processes will be completed in accordance with Annex A, IT Standards Guidance to DODIN–A End-to-End Enterprise Architecture for all IT Standards (for example, data, cyber, system, performance, design, naming, or process).

b. Army data standards management.

(1) Data Standards. Data standards will be used to guide and govern the implementation of data-related IT capabilities established in the Army Data Strategy. Approved data standards are registered in the DISR. Data standards not found in DISR may be approved, applied/enforced, and managed in the ATGR and will not contradict, supersede, or duplicate DISR standards.

(2) Army organizations will—

(a) Implement applicable standards and specifications as cited in the DISR (accessible at https://gtg.csd.disa.mil), or any future DOD-designated registry for IT and data sharing standards in accordance with DODI 8320.02.

(b) Validate that implementations of the data standard conform to the standard and maintain proof of conformance.

(c) Provide feedback to the Army Standards Council and ADB.

(3) Army DSs will—

(a) Ensure a standard does not exist before creating a new one to meet organization-local requirements.

(b) Develop and approve a needed data standard as part of coalition of stakeholders (for example a COI) with an interest in and need for the capability provided by the standard.

(c) Thoroughly test and validate the capability provided by the standard prior to approval.

(d) Submit approved standards to standards registry in the highest echelon at which the data standard may be needed (for example DISR if DOD-wide applicability).

c. Information systems and software applications. See DA Pam 25–1–1 and the CIO/G–6 document "Application or Information System Determination: Definitions, Scenarios, Illustrations, and Decision Tree" (version 1.1, dated 23 January 2013).

3–37. Army enterprise architecture certification/compliance

AEA Certification/Compliance (AEACC) Policy Guidance and the ACA (see DA Pam 25–1–1) is a means for ensuring that all Army IT solution architectures and resulting systems comply with the rules put forth in the current DODIN–A Enterprise Architecture and associated Reference Architectures (RAs). The DODIN–A comprises the IT assets of all Army activities, agencies, and components. It is the Army's single, global, information enterprise that provides IT capabilities, services, and information securely to all Army users and allied organizations. The ACA results measure the level of compliance of Army IT solution architectures and resulting systems and will be used as part of the IT investment management/acquisition decisions.

3–38. Property book accountability

Hardware and software will be accounted for using the appropriate supply regulations that address property book and guidance that addresses IT asset accountability (see DA Pam 25–1–1). Decommission IT systems in the eMASS. IT systems that have been retired will remain active in eMASS unless deliberate action is taken to remove them.

3–39. Army standard for life cycle replacement of information technology assets

Army organization strategic planning must incorporate regular IT hardware life cycle replacement in accordance with ISO/IEC 19770–1 Information Technology-IT Asset Management, OMB A–130, OMB A–11, OMB M–16–09, and OMB M–16–12 guidance. Army organizations will include regular life cycle replacement cost into the organization annual budget planning cycle (OMB Circular A–11). Army organizations will use recommended industry standards business rules for IT hardware life cycle replacement categories to include End-User Devices, Applications, Compute, Storage, Integrated Communication, and Security, IT Management, Business Management and Physical/Facility equipment. (See DA Pam 25–1–1 for specific life cycle replacement guidelines and outer limits for equipment replacement.)

3–40. Redistribution and disposal of information technology assets

a. The screening, redistribution, and disposal of IT equipment are completed through the Defense Logistics Agency (DLA) Disposition Services. For further guidance and clarification on the processes and communications flow for the

disposal of excess IT equipment, the installation NEC should contact its installation property book officer for guidance on the reuse, transfer, and donation programs for excess IT equipment, or visit the DLA Disposition Services website at http://www.dla.mil/dispositionservices.aspx. See also DRMS Instruction 4160.14; DOD 4160.21; and DA Pam 25–1–1. For non-NEC units contact your local IMO for instructions.

b. DRMS supports EO 12999 through the DOD Computers for Learning Program. Refer to http://www.dla.mil/dispositionservices/offers/reutilization/cfl.aspx for more information on this program.

c. Army organizations will--

(1) Divest legacy IT equipment as it is replaced by new IT equipment and associated capabilities. Review the approved and removed products lists at the Defense Information Systems Agency's Approved Products List Tracking System website (https://aplits.disa.mil) to ensure that any new IT equipment is approved for use. Decommission unnecessary switches and routers.

(2) Terminate contracts for legacy hardware, software, or IT services that are no longer in use or that updated versions have replaced. 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.

(3) Make sure contract option years are not exercised for IT hardware, software, or services no longer in use.

(4) Ensure that hardware and software from existing contracts continue to meet current cybersecurity requirements and comply with Security Technical Implementation Guides for the duration of their use.

(5) Verify that operation and maintenance costs are not being paid on unused hardware or software, including applications and circuits.

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

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

(8) 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, DA Pam 25–1–1, and related IT security documents.

(9) Make sure procedures for disposition and data sanitization of IT follow the requirements in AR 25–2, DA Pam 25–1–1, and applicable cybersecurity best business practices available at https://www.milsuite.mil/wiki/portal:army_information_assurance. (CAC log-in required).

(10) Obtain and follow official disposition instructions from the Defense Logistics Agency as appropriate (go to http://www.dla.mil/dispositionservices.aspx).

(11) Disposition of SCI equipment containing data needs to be either returned to the data owner(s) or turned into National Security Agency (NSA) via their process for destruction. Additionally, the equipment is required to be sanitized in accordance with the current regulation for sanitization NSA/Central Security Service (CSS) PM 9–12 storage device declassification manual.

3–41. Waivers

a. The CIO/G–6 maintains an online directory of waivers to Army IT policies. The directory lists the types of waivers processed by CIO/G–6, provides a brief description of each waiver's purpose, names the policies associated with each type of waiver, displays relevant links to further information or instructions to request a waiver, and provides points of contact for each type of waiver. The waiver directory is CAC-enabled and is available at https://army.deps.mil/army/cmds/hqda_ciog6/pages/CIO_G-6-waivers.aspx.

b. Waivers processed by the CIO/G–6 include, but are not limited, to the following:

(1) ITAS Waiver: Provides exceptions to IT acquisition/procurement policies.

(2) Collaboration Waiver: Waives requirement to use enterprise collaboration tools for solutions judged not to duplicate existing enterprise capabilities.

(3) Non-.mil Domain Name Waiver: Waives the requirement for an Army website to use a .mil URL as specified in paragraph 4–6 of this document.

(4) Internet service provider and network temporary exception to policy (TEP): Waives the requirement to use an Army or DOD server or connection to the DODIN–A (Requires DOD–CIO approval).

(5) Non-DOD Waiver: Waives the requirement to use only DODIN connections for non-secure internet protocol routing network (NIPRNET) and SIPRNET access (Requires DOD–CIO approval).

(6) Journaling Justification: Waives the requirement for commands to use only Enterprise Email default journaling (which captures metadata of an email in route).

(7) DISR Waiver: Waives requirement for a military organization to use DISR standards where there are impacts to cost/schedule/performance.

(8) Army ISP Exemption: Waives the ISP requirement for technology that does not meet the definition of "Information Technology System."

(9) JITC Test Exemption: Waives the requirement for an Army IT system to meet the Joint IT System and Joint NSS interoperability certifications.

(10) OSD ISP Waiver to Policy: Waives the requirement to develop an ISP for any Army system designated as a Joint System (requires DOD–CIO concurrence).

(11) AIC Waiver: Waives the requirement for an Army IT system, NSS, or business system to meet interoperability certification standards.

(12) Acquisition Cybersecurity (Risk Management Framework) Strategy Waiver: Waives cybersecurity acquisition strategy requirements for systems not connected to the DODIN–A and not Mission Critical or Mission-Essential.

(13) Foreign Access to Information Systems Waiver: Waives security requirements for foreigners (for example exchange personnel) to access NIPR hard drives and other Army (non-email) systems and software.

(14) Identity and Access Management-CAC/Public Key Infrastructure (PKI) Waiver: Waives Public Key Enabled requirements, depending on circumstances.

Section VII

Evaluate

3–42. Information technology performance management

a. Capability and financial performance management are essential elements of mission accomplishment and a process to improve effectiveness and efficiency of the Army's Information Technology enterprise. Capability and financial performance management are required by both law and regulation (Government Performance and Results Act Modernization Act of 2010, DOD Agency Strategic Plan). Performance management is the process to identify an important end or outcome, adopt, or establish a performance expectation, or target and then measure performance against the expectation to ensure performance is within acceptable limits, or thresholds, frequently enough, usually monthly for headquarters activity, to allow managers to implement timely actions in order to adjust the level of performance. Performance management in support of Army Information Technology will adhere to the Army Management Framework as described in (see AR 5–1).

b. Army leadership has identified the importance of strategy and performance management reviews as a way to greater effective and efficient accomplishment to ensure alignment across components and measure capabilities and their performance (see AD 2016–16).

3–43. Information technology performance measurements

Measuring IT performance is the process of assessing transformational change and the effectiveness and efficiency of IT in support of achieving an organization's missions, goals, and quantitative objectives. Performance management is accomplished through the application of outcome-based, measurable, and quantifiable criteria compared to an established baseline.

a. Each organization will develop performance measures for each organizational C4IT initiative and investment (including business systems) before execution or fielding.

b. The performance measures will determine the value-added contribution of the IT initiative or IT investment to missions, goals, and objectives; and provide a clear basis for assessing accomplishments, aiding decisionmaking, and assigning accountability at each management level. These measures will directly support the metrics used in the Strategic Management System (SMS), the Army's IT Metrics Program, the ISR program, and Army Directives as issued.

c. Performance management in support of Army Information Technology will adhere to the Army Management Framework as described in AR 5–1.

d. All Army organizations will develop and report quantitative capability and financial performance measures for the year of execution activity that aligns with orders, directives, standing program guidance or agency strategic and campaign plans regarding network, information management and information resources in support of Army goals and objectives. Performance measures will meet the following criteria for acceptance by the CIO/G–6 (see DA Pam 25–1–1 for the complete guidelines).

(1) Performance measures will have all supporting information for metric elements and adhere to the guidelines for Key Performance Indicators and Measures in DA Pam 25–1–1.

(2) The Army's enterprise-wide SMS is the repository and reporting tool for performance management actions.

(3) Army organizations will assign a performance management liaison to work with the CIO/G–6 and to carry out performance management responsibilities within the organization.

(4) Army agencies and commands will provide the staff section who has the responsibility for providing enduring liaison of performance management.

Chapter 4
Information Technology Solutions Implementation

Section I

Department of Defense Information Network—Army Operations and Cybersecurity

The IT solutions implementation chapter presents the common, integrated information computing and communications environment. It includes the computing infrastructure for the acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on enterprise network capacity, hardware, software operating systems, information transport, security, user services, and network operations, enterprise services, and hardware/software. This chapter contains policy for the management of IT investments. The EIEMA represents the common, integrated information computing and communications environment. The EIEMA includes computing infrastructure for the acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on enterprise hardware, software operating systems, information transport, security, and DODIN operations, enterprise services, and hardware/software. The EIEMA portfolio includes IT and national security systems, initiatives, programs of record, and other investments and resources that, individually or in combination, reach and serve users and enable capabilities across the MAs: BMA, WMA, and DIMA and EIEMA. Applications and platform or system-unique investments that exclusively or predominantly serve users or systems within a single domain (sub-portfolio) or a single MA are excluded as a rule, though such solutions may have a critical dependency upon the EIEMA.

4–1. General

See figure 4–1 below for mission areas and their domains within the Army.

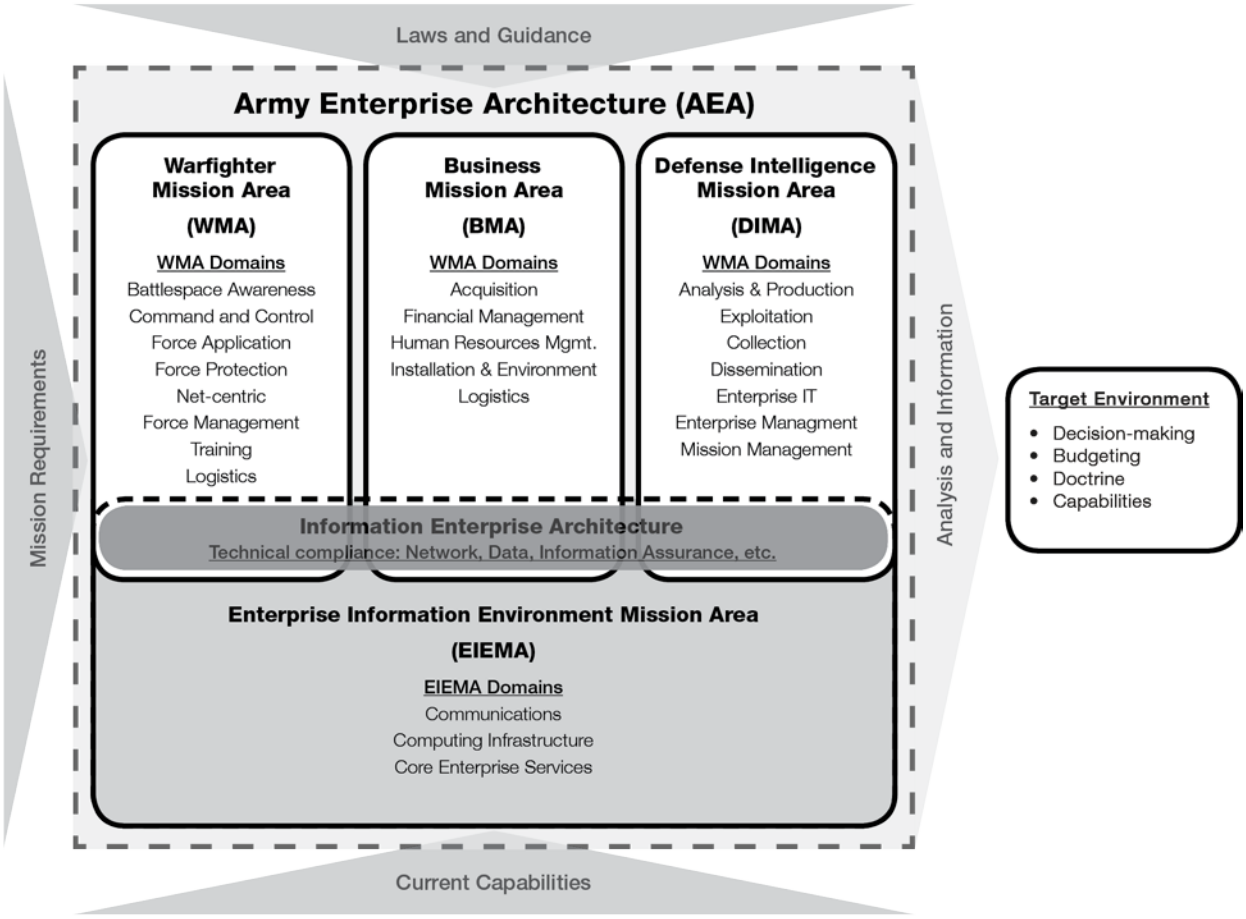

Figure 4–1. Mission Areas and their domains within the Army

4–2. Mission Areas

The Army categorizes IT investments within four MAs: WMA, BMA, DIMA, and EIEMA (see fig 4–1) to simplify and efficiently manage Army IT investments. The Army aligns IT investments with one of the four Army mission areas based on the functional process architecture of the IT investment and not on unit, command, or location.

a. Several authoritative documents direct managing IT capabilities and investments by functionally defined MA portfolios to include DODD 8115.01, DODI 8115.02, and SECARMY Memorandum, Subject: Army Information Technology Integration and Governance, dated 5 April 2017. Senior leader councils within each MA provide guidance and top-level governance.

b. Mission Area Organization.

(1) The BMA includes all IT investments characterize as DBSs. The USA as CMO is designated the lead for the Business portfolio. The ABC provides governance for the BMA and OBT is the HQDA lead for the BMA and the USA and the Army VCSA serve as the functional lead.

(2) The DIMA is a DOD-level MA, with the Army portion led by the Army DCS, G–2 responsible for Army-specific intelligence IT systems and Army equities in policy, operations, and investments at DOD-level. The ISIG provides governance for the DIMA. The U.S. Army Intelligence and Security Command is the command lead for the DIMA.

(3) The WMA includes all IT investments related to mission-command, warfighting operations, training, and readiness and is led by the Army DCS, G–3/5/7. The AWIC provides governance for the WMA. TRADOC is the command lead for the WMA.

(4) The EIEMA includes all IT investments that facilitate the implementation, operation, security, and enterprise services for the Army portion of the DODIN–A. The AENC provides governance for the EIEMA. The CIO/G–6 is the designated HQDA lead and ARCYBER is the command lead for the EIEMA.

4–3. Information transport

a. Internet service providers. Army computers, systems, and networks must access the Internet through a Defense Information Systems Network (DISN)-controlled and DISN-monitored connection. Army organizations that require direct connection to the commercial Internet must first obtain an Internet service provider and Network TEP waiver. For information on the Internet service provider and Network TEP waiver, see https://www.disa.mil/network-services/~/media/files/disa/services/disn-connect/references/disn_cpg.pdf, https://www.disa.mil/network-services/enterprise-connections/connection-approval, and https://snap.dod.mil.

b. Tactical use of the secure network on Army installations. Tactical units at their home station in the continental United States (CONUS) will connect tactical mission-command systems to the installation networks and sustain security posture in accordance with ARCYBER-published connection and registration TTPs. NECs will support connecting tactical units to the installation networks.

c. Telecommunications. Commanders at installation, ACOM, ASCC, and DRU levels will appoint in writing telephone control officers to accurately review and validate bills for toll-free service, pager services, cellular phone service, collect calls, and calling card usage; long-distance, sensitive but unclassified voice, Federal telecommunications, and all services associated with mobile devices in accordance with requirements of AR 25–13. Additionally, the telephone control officer is the only official other than the commander authorized to approve mobile device service initializations and all service level changes. Additional policy about the implementation and management of information transport and telecommunications can be found in AR 25–13.

4–4. Computing infrastructure

a. Department of Defense-provided processing services. DOD provides centralized information processing services (DISA's Defense Enterprise Computing Centers) available to all military departments and services on a fee-for-service basis and will be used to the greatest extent practicable.

(1) Fee-for-service rates will be coordinated among the requesting organization and the DOD service providers. ARCYBER will help Army activities resolve issues that involve the provisioning of, and funding for, services from DOD providers.

(2) Army organizations will coordinate with the supporting NEC or other service providers to determine requirements for centralized processing services. Installation requirements will be integrated and coordinated with the DOD service provider on behalf of all activities within their supported area (see DODI 4000.19 for procedures on service parameters and estimating annual fees).

(3) All software, firmware, applications, or web services using the DODIN–A must comply with the DOD RMF process. The RMF replaces the DOD Information Assurance Certification and Accreditation Process and eliminates the need for the previous Networthiness process (that is obtaining a Certificate of Networthiness). The RMF process is detailed in AR 25–2 and DA Pam 25–2–14.

(4) Army reporting entities and service providers will comply with the DOD financial improvement and audit readiness (FIAR) guidance. The Office of the Under Secretary of Defense (Comptroller) and the Office of the Chief Information Officer jointly issued a policy memo, subject "Enhanced Integration of Financial Management Requirements with the Risk Management Framework", which incorporates audit readiness requirements into the Department's RMF process. The updated guidance addresses the goals, priorities, strategy, and methodology for audit readiness. Moreover, it includes the responsibilities of reporting entities and service providers, as well as the processes they should follow for achieving audit readiness and sustainment for systems that impact internal controls over financial reporting. (Note, there are some common requirements between Federal Information System Controls Audit Manual and NIST 800–53 for which the FIAR Guidance provides a crosswalk for.)

b. Responsibility. OMB and the DOD–CIO prescribe strategic policy guidance for the employment of IT within the Federal Government and DOD respectively. The CIO/G–6, in coordination with ARCYBER and ASA (ALT), is the Army's executive agent for planning, resource management, budgeting, and execution of the DA's EIEMA, including oversight of networks, physical data centers as well as virtual data centers, end-user devices, and Army and DOD-approved Enterprise hosting environments.

c. The Army Data Center Consolidation Plan. The CIO/G–6 Army Enterprise Computing Division (SAIS–OAC) is responsible for implementing the Army Data Center Consolidation Plan (ADCCP) as described in AD 2016–38. The ADCCP applies to all ACOMs; ASCCs; DRUs; Army staff, including FOAs; data center owners; application owners; and IT portfolio and domain leads, whether or not they own or operate a data center. The intent of ADCCP is to support the Army's 2025 data center endstate; transition application hosting to enterprise environments; reduce the Army's data center and application footprint; enhance compute and store capabilities; improve cybersecurity; and increase fiscal and operational efficiencies of the Army's Information Technology environment. The Army's data center end-state includes a limited number of Army Enterprise Data Centers (AEDCs) and enduring data centers and communications nodes. The ADCCP

aligns the Army Cloud Strategy with the JIE data center architecture to include component enterprise data centers (CEDCs), Installation Service Nodes (ISNs), and special purpose processing nodes (SPPNs) and leverages the JIE Security infrastructure and architecture (Appendix A, Reference DOD Data Center Reference Architecture).

d. Enterprise hosting. The CIO/G–6 is undertaking a range of tasks necessary to rationalize and modernize IT systems and applications, migrate them to approved enterprise hosting environments and close or consolidate data centers. CIO/G–6, in collaboration with ASA (ALT) and ARCYBER, is responsible for developing and publishing the Approved list of enterprise hosting environments for Army organizations. The Army Application Migration Business Office (AAMBO) is the Army's source for cataloging enterprise hosting options, including commercial cloud service offerings (CSOs). Unless waived by the CIO/G–6, Army organizations are required to contact AAMBO for planning and facilitation of its application migrations to approved enterprise hosting facilities. The Army Cloud Computing Enterprise Transformation is the preferred vehicle for hosting in the commercial CSO's.

e. Governance. The MIRC is a 3-Star GO/SES Governance Forum, chaired by the Army Deputy Chief Information Officer/G–6 and the Deputy Chief Management Officer. Using the MIRC as an advisory body, the CIO/G–6 has oversight of the AD 2016–38 implementation plan through the AENC. The MIRC: (1) synchronizes the implementation plan across the Army, (2) adjudicates and elevates requests to deviate from the implementation plan, as required, (3) advises and recommends implementation plan changes, (4) validates compliance with the implementation plan and assess operational impacts of data center closures, and (5) reports Army compliance with the implementation plan to the AENC. The AENC Chair reports implementation progress to the Senior Review Group quarterly.

f. Resourcing. Army organizations are responsible for planning, programming, and funding for all data center consolidation and application migration requirements to include modernizing, virtualizing, and hosting systems or applications. Additionally, an ITAS Waiver is required prior to expenditure or commitment of funds related to data center IT investments, to include hosting services, hardware, software, storage, or other services in direct support of a data center before executing funds. This waiver is required regardless of whether or not the item is purchased through CHESS. Approved ITAS waivers are valid for one year and are reassessed annually.

g. Army Portfolio Management Solution applicability. 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 similar agreements, commercial cloud services provided directly through a hosting contract, or commercial cloud services provided through "other direct costs." Refer to the APMS Desk side Reference Manual for more information. CIO/G–6 will conduct periodic compliance reviews to ensure cloud data has been entered into APMS. Results will be reviewed in forums, including the MIRC.

h. Information technology support for military construction. Applicability. This section applies to all IT requirements related to all new, restoration and modernization (R&M) projects. MILCON requesting organizations will comply with AR 420–1, DA Pam 420–11, and DA Pam 25–1–1 which defines the IT requirements process in support of new and R&M MILCON projects. In addition, organizations will comply with the following: (a) the annual fiscal guidance from the DCS, G8's Technical Guidance Memorandum, which serves as an annex of the POM; (b) the Army Program Guidance Memorandum, which provides fiscal and programming guidance to the PEGs and program integrators regarding the allocation of Army resources during the Future Year Defense Plan; and (c) the ACSIM's Fiscal Investment Guidance Memorandum, which further defines each year's POM process. The MILCON requesting organization will document all their MILCON-related IT on DD Form 1391 (FY__ Military Construction Project Data) and load it into the US Army Corps of Engineer's Parametric Cost Engineering System (PACES). Army National Guard (ARNG) and U.S. Army Reserve (USAR) organizations will coordinate with their respective CIO/G–6 Army component for their MILCON IT requirements. For Repair and Restoration projects funded with Operation and Maintenance funds, conduct coordination with the garrison's respective CIO/G–6 as early as possible upon conception of the project. Two years is optimal to align with the budgeting cycles.

(1) Planning, designing, and monitoring MILCON projects. All MILCON project designs must comply with the standards set forth in the installation-information infrastructure architecture (I3A) technical criteria for non-NIPR systems. Medical MILCON projects have medically unique requirements. UFC 4–510–01 will take precedence over the I3A for medical MILCON projects (see UFC 4–510–01). Secure internet protocol router implementation must follow the guidelines set forth in the SIPRNET Technical Guide. The I3A Technical Criteria is available at https://www.us.army.mil/suite/folder/5745483. The SIPRNET Tech Guide is available at https://www.us.army.mil/suite/folder/5744948. ARCYBER and or its subordinate organizations will synchronize all IT planning, installation, and delivery of baseline IT services within the buildings or facilities at the installation for MILCON and medical MILCON. The Supporting NEC of the MILCON project must maintain close and continuous coordination with the supporting director of public works to ensure a complete awareness of all IT functional requirements

(including mission-related and base support) for inclusion in the Contracting Agency statement of work for real property construction.

(2) Requirements for information technology systems to include floor space. The supporting NEC will identify all proposed IT systems requirements for both outside and inside plant to their supporting signal brigade, who will then review the proposed requirements to ensure compliance with DOD and CIO/G–6 regulations and polices (for example DOD Data server consolidation and application migration timelines) and to ensure the NEC can support the real property requirements. The CIO/G–6 will coordinate with the real property requesting organization and the USAISEC, as appropriate, to validate the required real property IT requirements.

(3) Cost estimates and funding. The post, camp, and station's department of public works or equivalent will ensure the supporting NEC is included in any MILCON operation and maintenance real property project planning, designs, and contract negotiations for the information system technical requirements and communication systems for any MILCON projects or R&M projects. The supporting NECs will ensure that IT cost estimates for validated IT requirements are identified for each component supporting MILCON facilities. The appropriate supporting signal brigade will validate and approve the NEC's requirements and associated funding input to the DD Form 1391 prior to submission. The USAISEC must certify all DD Forms 1391 in PACES before the respective ACSIM's MILCON project review board in accordance with AR 420–1. IT funding and installation responsibilities are identified for inclusion to the DD Form 1391 in accordance with AR 420–1. The requesting organization and USACE will ensure the MUE IT requirements identified in the DD Form 1391 are submitted to the MILCON requesting organization's appropriate management decision execution package (MDEP) manager for programing in the POM process. The MDEP manager will associate the MDEP's MUE to the Programming Element, B3150.

(4) Host and tenant relationships. Supplemental service agreements and ISAs will include any IT support for MILCON.

(5) Installation-information infrastructure. MILCON IT requirements include information system connectivity for both voice and data.

(6) MILCON POM construction cost categories are as follows:

(a) Construction/Cost is developed in accordance with AR 429–1, information systems (INFOSYS) definitions.

(b) ACSIM programs for Congressional funding with the Installation Program Executive Group. IT requirements funded as part of the MILCON project (for example, fiber/copper cabling, wire raceway, racks, and so forth).

(c) Information Systems Cost/I cost. ACSIM programs with the Installation Program Executive Group. IT requirements used to deliver common services as identified in the DD1391 (for example, NIPR switches, local area network (LAN) connectivity, telephones, and so forth).

(d) Proponent/P cost also called MUE. The major command who own the new or R&M MILCON project MUE and programs the MUE with their respective PEG the IT requirements above the common level of services (for example, CENTRIX–K router, encryption, switches; JWICS network and audio and visual systems; and so forth). The command's G–8 will identify to the PEG the funds are MUE for a MILCON to ensure the PEG programs the requirement. INFOSYS has several Budget Line Item Number BB8650 used for Information System/I costs; BB1400 used for Army Enterprise Network requirements; BB8700 used for R&M MUE; B31510 used for Proponent/P MUE. Each year the command will review their MILCON requirements with the Mission-Unique Team, a subcommittee of ACSIM's integrated programming Team to ensure projects schedule and cost schedule are still on track.

(e) R&M MILCON projects tend to be Operations and Maintenance, Army funded. It is imperative that the garrison's NEC be involved in the planning of a proposed garrison or tenant R&M MILCON project to ensure the project's IT tails requirements and costs are accurately captured, and funding appropriately identified in accordance with AR 420–1. The NEC has the responsibility to initiate the request for any standard IT tails/ I cost for the R&M project. The NEC's requirements should be submitted through their chain of command for the project. The command that owns the project should submit their MUE requirements through their chain of command. If there are any questions to the MILCON INFOSYS process or have identified a MILCON IT-related requirement that cannot be funded by the NEC's chain of command, contact the CIO/G–6 Infrastructure Division (SAIS–NSI) for assistance and resolution.

(f) The Director of Public Works MILCON requesting organization will document all their MILCON-related IT on DD Form 1391 and load it into the U.S. Army Corps of Engineer's PACES. ARNG and USAR organizations will coordinate with their respective CIO/G–6 Army component for their MILCON IT requirements.

i. Development freeze for new and current data centers. Per OMB Data Center Optimization Initiative (DCOI) memo published on 1 Aug 16 (Appendix A – Reference OMB DCOI Memorandum), Army organizations are not authorized to build or allocate resources toward initiating a new data center or significantly expanding an existing data center without an approved waiver from the Office of the Secretary of Defense, DOD–CIO. To request a waiver, Army organizations must submit a written justification through the CIO/G–6 (SAIS–AOS) to the DOD–CIO for the OMB Office of the Chief Information Officer. Prior to submission, the waiver must be vetted by the MIRC. The waiver request must include an

analysis of alternatives (including opportunities for cloud services, inter-agency shared services, and third-party co-location) and an explanation of the net reduction in the agency's data center inventory that will be facilitated by the new or expanded data center (such as through consolidation of multiple existing data centers into a single new data center).

j. Energy conservation guidelines for information technology equipment.

(1) All computers, desktops, laptops, and tablets must have energy-saving features, such as ENERGY STAR® certification. These features, if configurable, shall be configured to be activated after no more than 30 minutes of inactivity (see DA Pam 25–1–1 for more information).

(2) Computer and peripheral devices used in conference rooms, video-teleconferencing, and kiosk environments, if configurable, will be configured to enter energy-saving mode (such as "sleep" or "standby"), after no more than 30 minutes after inactivity, or be turned off when not in use.

(3) General-purpose office equipment, copiers, printing devices, faxes, all-in-one devices, and similar equipment, if configurable, will be configured to enter energy-saving mode (such as "sleep" or "standby"), after no more than 30 minutes after inactivity, or be will be turned off at the end of every business day. Computer monitors and peripheral devices, such as speakers, scanners, and external drives, if configurable, will be configured to enter energy-saving mode (such as "sleep" or "standby"), after no more than 30 minutes after inactivity, or be will be turned off when not in use.

(4) Monitors and laptops displays will enter energy-savings mode after 15 minutes of inactivity.

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

k. Purchase of energy-efficient computer equipment. All purchases of microcomputers, including desktop and laptop personal computers, tablets, monitors, printers, and other peripheral equipment will meet the requirements of applicable laws and executive orders (see DA Pam 25–1–1 for more information).

l. Minimize employee information technology devices. Issuing employee IT devices (for example, desktops, laptops, cellular phones, smart phones, or tablet computers) is a command responsibility. Issuance will be based on the mission and assigned position, rather than grade or rank of the individual. The number of devices should be the least amount required to accomplish the assigned mission.

m. Data center energy metering and power efficiency. The OMB DCOI Memorandum (Appendix A, OMB DCOI Memorandum) requires all Federal agencies and departments install automated energy monitoring tools, and collect and report energy usage in their data centers to OMB. To comply with this OMB mandate, CIO/G–6, in coordination with ACSIM, ARCYBER, and ASA (ALT) will install automated energy metering tools and collect and report energy usage data in the designated AEDCs. The Army will also designate at least one certified Data Center Energy Practitioner to manage and report data center energy performance to CIO/G–6.

n. Data center infrastructure-management software. The OMB DCOI memo requires all Federal agencies and departments install infrastructure-management automated software in data centers to monitor and manage capacity and virtualization rates, energy utilization, and assets. CIO/G–6, in coordination with ARCYBER and ASA (ALT) will install data center infrastructure-management software in designated AEDCs.

o. Army input to Department of Defense Data Center Optimization Initiative strategic plan. The OMB DCOI memo requires all Federal agencies and departments to provide an annual report to OMB on their status of achieving stated data center optimization and closures metrics. Army is required to provide input to DOD to support this requirement and comply with DOD specified timelines. As necessary, Army will task subordinate commands to provide data to support the development of Army's input into DOD's strategic plan and designated AEDCs.

Section II

User Facing Services

4–5. Collaboration tools standards

a. Collaboration tools are defined as the wide range of structures, processes, procedures, and services necessary to enable two or more individuals who are not co-available to use an electronic synchronous or asynchronous environment to communicate.

b. All Army organizations investing in or implementing collaborative tools will use enterprise collaboration services and tools. ARCYBER maintains a list of enterprise collaboration tools and services on the approved product list at https://portal.army.mil/apps/networthiness/sitepages/home.aspx. If Army organizations have collaboration requirements that are not met by current capabilities, they are required to submit these requirements through CHESS for approval prior to implementing a collaboration solution (see DA Pam 25–1–1).

c. The Communications-Electronics Command is the Army focal point for technical matters and the Army interface with the DISA Configuration Management Office to address interoperability within Army systems. The CIO/G–6 will support only the new tools or the sustainment of existing collaborative tools that meet the DOD standards.

d. When using collaboration services and tools, Army commands will—

(1) Develop acceptable use policies.

(2) Develop local policies and procedures on access-control and management of information used in collaborative efforts.

(3) Comply with configuration management and IA vulnerability management policies.

(4) Leverage enterprise collaboration services.

e. All individual users of collaboration tools are responsible for—

(1) The information they create or share using collaboration capabilities.

(2) Adhering to applicable professional, ethical, and security guidelines.

(3) Maintaining the security of their credentials.

(4) Conforming to posting procedures and policy on the use of official and authorized telecommunications (see AR 25–13 for the UC policy).

(5) Following records management policy identified in paragraph 3–29 and AR 25–400–2.

4–6. Websites and services

a. Management of web domains. ARCYBER will manage the "army.mil" website and website assignment of subdomains and the web domain registration process. The web domain registry will include all of the web domain information for "army.mil" websites at the third-level domain, as well as any commercial websites being used.

b. Web domain registration. Army organizations that desire subdomains must register their domain through the registration processes and guidelines found at: https://www.us.army.mil/suite/page/600053/. All Army social-networking sites and social media sites must register at http://www.army.mil/.

c. Social-networking sites. For the use of social media sites, refer to paragraph 4–9 of this publication.

d. Use of the army.mil web domain. All Army public and nonpublic websites must be available on an "army.mil" or "disa.mil" domain, unless the CIO/G–6 waives that requirement. In accordance with DODI 8410.01, organizations must use the ".mil" domain as the Sensitive but Unclassified NIPRNET and ".smil.mil" for the SIPRNET, unless a waiver has been granted by the CIO/G–6. See https://www.milsuite.mil/wiki/non-mil Domain Waivers (CAC login required) for more information on non-.mil domain waivers and exceptions.

e. Web domain authorizations. HQDA principals, the USAR and ARNG, ACOMs, ASCCs, DRUs, PEOs, PMs, Service schools or centers, installations, division-level units, and special-Service organizations with third-level domain names (for example, arcyber.army.mil). Subordinate organizations with a requirement to provide web-based content should first seek to establish a web presence (for example, web pages) as part of a website owned by their respective parent organization rather than establish or maintain a separate website. The intent of this policy is to minimize the total number of Army websites.

f. Web management policy. Army website managers and maintainers must comply with the web management policy in this regulation, the DOD website administration policy available at: http://www.defense.gov/webmasters/, and subsequent DOD guidance and direction. Information contained on publicly accessible websites is subject to the policies and clearance procedures prescribed in AR 360–1 for the release of information to the public. Website managers and maintainers will—

(1) Ensure that only official Army information that is releasable and of value to the public is posted on the Army's public websites.

(2) Ensure that web servers are compliant with policy and security procedures (see AR 25–2 and related pamphlets).

(3) Comply with the Army Web Risk Assessment Cell (AWRAC) notifications for website security. For questions, contact AWRAC at usarmy.belvoir.arcyber.mbx.awrac@mail.mil.

(4) Apply appropriate privacy and security policies.

(5) Display a privacy and security notice in a prominent location on at least the first page of all major sections of each website. Each privacy and security notice must inform visitors to the site what information is collected, why it is collected, and how it will be used.

(6) Ensure surveys, questionnaires, and forms collecting information from members of the public or Federal personnel and contractors comply with AR 335–15.

g. Website reviews. In accordance with AR 530–1, the public affairs officer and operations security officer for each Army organization will review and approve the content and format for each of the organization' s public-facing websites before content is posted online. The designated certified reviewer(s) will conduct routine reviews of websites on a quarterly basis to ensure that each website is in compliance with applicable policies and that the content remains relevant and appropriate. The minimum review will include all of the website's internal control checklist questions (see DA Pam 25–1–1).

h. Assignment of webmaster and maintainer. Army organizations will assign a webmaster and maintainer for each of their websites and pages. Army organizations will provide their webmasters and maintainers sufficient resources and training on both technical and content matters. Resources are available at https://informationassurance.us.army.mil/. Online training is available at https://iatraining.us.army.mil/.

i. Electronic and information technology access for Army employees and members of the public. 40 USC 762 requires that agencies provide electronic and information technology (EIT) access to employees and members of the public with disabilities. The access must be comparable to the access available to individuals who do not have disabilities.

(1) Websites are required to comply with the provisions of Section 508 of the Rehabilitation Act Amendments of 1998. Websites must be equally accessible to disabled and non-disabled Federal employees and members of the public. Guidance on Section 508 standards concerning web-based information and applications is available at http://www.access-board.gov/. For procedures and exceptions (see DA Pam 25–1–1).

(2) EIT includes equipment or interconnected systems or subsystems of equipment that are used to create, convert, or duplicate data or information. More specific examples of EIT include, but are not limited to, telecommunication products (such as telephones), information kiosks and transaction machines, websites, multimedia, and office equipment (such as copiers and fax machines).

(3) Information managers will make all reasonable efforts to accommodate individuals with disabilities, consistent with the laws cited above and AR 600–7.

j. Private websites. Private websites are for DOD organizations to internally publicize projects and goals, and to share valuable information with the community for collaboration and coordination purposes. They are hosted on internal organizational web servers or other Army-approved hosting environments. Organizational website managers will install access-control mechanisms (see AR 25–2). All Internet-facing applications must be hosted within STIG-compliant NIPRNET DOD demilitarized zones (DMZs) or in DOD Provisionally Authorized cloud service offerings. Internet-facing applications must be registered with the Army IP Registration Authority.

k. Use of cookies. Use of cookies on Army websites will comply with the requirements found in OMB M–10–22. Persistent cookies that track users over time and across different websites to collect personal information are prohibited on public websites. The use of any other automated means to collect PII on public websites without the express permission of the user is prohibited. Third-party cookie generation will be disabled.

4–7. Web access blocking

The use of web access blocking or filtering tools is authorized for permanently blocking user access to inappropriate websites. Access to prohibited websites for mission support reasons is considered authorized use. Exceptions to this policy are described in AR 25–13.

4–8. Establish secure connections for all Army websites and web services

All Army organizations must deploy hyper text transfer protocol secure (HTTPS) on their domains using the following guidelines:

a. Newly developed websites and services at all Army domains or subdomains must use HTTPS at launch.

b. For existing websites and services, Army organizations must prioritize deployment of HTTPS using a risk-based analysis. Web services that involve an exchange of personally identifiable information, where the content is sensitive in nature, or where the content receives a high amount of traffic, should receive priority, and migrate as soon as possible.

c. Intranets must also use HTTPS to secure the websites.

d. All site administrators should follow the best business practices identified by OMB at https://https.cio.gov.

4–9. Other private websites (intranets and extranets)

a. Hosting. Army organizations must work with AAMBO during the planning phase. AAMBO provides assistance in defining requirements, recommending the most cost-effective hosting solution, and supporting system and application owners throughout the application migration process (see Memorandum, AD 2016–38).

b. Authentication. Web applications must be PKI-enabled. For more information on PKI requirements, standards, implementation, and exceptions, see https://portal.army.mil/apps/networthiness/sitepages/home.aspx.

c. Authentication. All NIPRNET and SIPRNET Intranets (private websites used for processing information limited to DOD users) will be configured to use DOD PKI certificates for server authentication, and client/server authentication. Owners of authorized Intranets must ensure that the secure sockets layer (SSL) is enabled and that PKI SSL encryption certificates are loaded on the servers. Use of IP restriction by itself is insufficient; such sites will be considered publicly accessible rather than private. PKI web server certificates may be obtained from ARCYBER regional cyber center.

d. Web application authentication. All intranet web applications will be enabled to use DOD PKI certificates for user access, unless waived by the CIO/G–6.

e. Extranet authentication. Unclassified extranets (private websites used for exchanging nonpublic domain information with members of the public and other individuals not authorized to use DOD PKI resources) may be operated to facilitate Army missions and functions. To ensure ease of access, organizations that collect sensitive but unclassified information from the general public as part of their assigned mission are authorized to purchase and use approved, commercially available certificates to provide SSL services. Extranet owners must select from the trusted and validated products lists on DISA's website at https://aplits.disa.mil/. All Internet-facing applications must be hosted within a STIG-compliant NIPRNET DOD DMZ. Internet-facing applications must be registered with the Army IP registration authority, ARCYBER.

4–10. Email services

a. Use of official Government email service. Army personnel will use only Government-provided email services to conduct official business unless otherwise authorized (see para 4–8b). Email services provided by a commercial service provider are prohibited for Army business communications containing sensitive information. Automatically forwarding from an official Government account to an unofficial (commercial service) is prohibited. "Auto-forward" default settings on email will restrict individuals from automatically forwarding their email messages to commercial (private) addresses. There is no prohibition for manually forwarding email messages, one at a time, after opening and reading the content to ensure that the information is not sensitive or classified.

b. Use of unofficial Government email service. Law and DOD policy are clear: "non-official electronic messaging accounts," including personal email accounts, must not be used to conduct official DOD communications, with very few exceptions, and intentional violations of this may be the basis for disciplinary action. Personal or other non-official email accounts may be used for official business only in those rare and extraordinary situations where an official email capability is not available (For example, an extraordinary circumstance could be when a DOD official is out of the office without access to official communication channels and must send an urgent DOD mission-related email). When this happens, the DOD official shall copy his official email account at the time of sending or forward the message to his official account within 20 days of sending the email. In doing so, the sender shall mitigate against transmitting non-public or controlled unclassified information. Classified information may never be transmitted over any unclassified networks, whether DOD or commercial.

c. Use of encryption. Army personnel will encrypt and digitally sign all emails containing sensitive data using an approved DOD PKI certificate, from an Army-owned, Army-operated, or Army-controlled system or account to maintain confidentiality. The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates. Sensitive information in email messages must be clearly labeled to show any sensitivity, such as "Sensitive-Privacy Act Information." A digital signature and encryption will be used to send information that is—

(1) Protected by 5 USC 552a (Privacy Act of 1974). The Privacy Act includes protection of PII.

(2) Identified as FOUO.

(3) Protected under HIPAA. (See also para 2–23*b* and appendix A.)

(4) Otherwise sensitive (as defined in the glossary).

d. Email records.

(1) Army policies for records management apply to email traffic. Designated records managers, records coordinators, and records custodians will monitor the application of records management procedures to email records. Email backup storage is not considered records archiving. Refer to AR 25–400–2 for more information on preserving email communications as records.

(2) Electronic messages generated by Army personnel (military and civilian) in their official capacity will not contain slogans, quotes, or other personalized information as part of the individual sender's signature block. Signature blocks within electronic messages will contain only the necessary business information, such as: the name of the organization (office, activity, or unit represented); official mailing address or unit information; name of individual; telephone numbers (Defense Switched Network, commercial telephone, cell phone number, or facsimile numbers); office email addresses or government websites (unit web or Facebook page); government disclaimer (Privacy Act Statement, Attorney Client Notice); unit historical motto (http://www.tioh.hqda.pentagon.mil); or any other information approved by HQDA.

e. Email administration. Local email procedures will provide for implementation of sound email account management consistent with guidance in this regulation and other Army security guidance. NECs will establish local procedures to ensure that—

(1) System administrators are assigned and trained.

(2) System administrators establish office accounts to receive organizational correspondence. All shared organizational accounts will use DOD-approved PKI certificates to ensure that email requiring data integrity, message authenticity, or nonrepudiation, is correctly identified and protected. Data owners must classify their data as public, public restricted, or

private. If data is classified as public restricted or private, then the data owner must restrict access to the information by using an approved, two-factor authentication access-control method such as CAC and PKI.

(3) Accounts are assigned only to individuals authorized to use Army-operated IT systems.

f. Bandwidth usage. Army service providers are required to develop local procedures on bandwidth usage to encourage the following behaviors to manage bandwidth demand:

(1) Only mission-essential attachments will be transmitted.

(2) When internally staffing documents within an organization, place the documents in internally accessible areas, shared drives, or approved organizational Intranets instead of sending documents via email.

(3) When sharing documents external to an organization, place documents in the aggregate on the enterprise portal or on an approved organizational web server, and provide the link or uniform resource locator (URL) where the documents are available. Activities will use the enterprise portal as the primary tools for collaboration.

4–11. Responsible use of internet-based capabilities

a. General. Internet-based capabilities (IbC) includes all the public information capabilities or applications available across the Internet from locations not directly or indirectly controlled by DOD or the Federal government (that is, locations not owned or operated by DOD or another Federal agency or by contractors or others on behalf of DOD or another Federal agency).

(1) Per DOD policy, the NIPRNET will be configured to provide access to internet-based capabilities across all DOD components. Commanders at all levels must continue to defend against malicious activity affecting Army networks. They therefore, may take actions to limit access to Internet-based capabilities on a temporary basis in order to ensure that a mission is safeguarded or to preserve operations security.

(2) IbCs are often deployed in an environment that is not under the Army's direct control. Commanders, Soldiers, and Civilians affiliated with the Army must follow the requirements outlined in this document and those found in DODI 8550.01 to ensure that Army networks and information are protected and that operations security is maintained.

b. Information manager.

(1) Decisions to collaborate, participate, or to disseminate or gather information via DOD Internet services or IbC requires that there be a balance between benefits and vulnerabilities. Internet infrastructure, services, and technologies provide versatile communication assets that must be managed to mitigate risks to national security, to the safety, security, and privacy of personnel, and to Federal agencies.

(2) DOD Internet services and IbC used to collect, disseminate, store, or otherwise process DOD information will be configured and operated in a manner that maximizes the protection (for example confidentiality, integrity, and availability) of the information, commensurate with the risk and magnitude of harm that could result from the loss, compromise, or corruption of the information.

(a) For use of DOD Internet services, this applies to both public and non-public DOD information.

(b) For use of IbC, this applies to the integrity and availability of public DOD information. IbC will not be used to collect, disseminate, store, or otherwise process non-public DOD information, as IbC are not subject to Federal or DOD cybersecurity standards, controls, or enforcement, and therefore may not consistently provide confidentiality.

(3) Army information systems hosting Army Internet services will be operated and configured to meet the requirements in AR 25–2 and certified and accredited in compliance with DODI 8510.01.

(4) Public Army websites will be operated in compliance with the laws and requirements cited in OMB Memorandum M–05–04. Detailed explanations and implementation guidance are provided at the web Manager's Advisory Council website at http://www.howto.gov/web-content/.

(5) Army Internet services and the information disseminated via these services, where appropriate, will be made available to Federal initiatives such as Data.gov, Recovery.gov, and USA.gov to reduce duplication and to foster greater participation, collaboration, and transparency with the public. Where feasible and appropriate, such Army information will be provided as datasets in raw (machine readable) format as defined in Deputy Secretary of Defense Memorandum, Subject: Support for the Open Government Initiative, dated 14 April 2010.

(6) All unclassified Army networks (for example Non-classified Internet Protocol Router Network (NIPRNET), the Defense Research and Engineering Network) will be configured to provide access to IbC across all the DOD Components.

(7) Authorized users of unclassified Army networks will comply with all laws, policies, regulations, and guidance concerning communication and the appropriate control of Army information regardless of the technology used. Furthermore, all personal use of IbC by means of Federal government resources will comply with DOD 5500.7–R.

c. Social media.

(1) Internet-based capabilities such as social-networking sites provide opportunities for adversarial groups, such as foreign intelligence services, to glean personal information for use in directly targeting Army and DOD users. All Army

personnel have a personal and professional responsibility to ensure that no information that might place Soldiers in jeopardy or be of use to adversaries (including local criminal elements) be posted to public websites. Sensitive organizational information, to include Controlled Unclassified Information, will not be discussed on any externally facing website. The following includes but is by no means a comprehensive list of, examples of information that should never be published on a public website:

(a) Classified information.

(b) Casualty information before the next-of-kin has been formally notified by the Service concerned.

(c) Information protected by the Privacy Act.

(d) Information regarding incidents under investigation.

(e) Information considered Essential Elements of Friendly Information.

(f) For Official Use Only information.

(g) Information identified on the current Critical Information List.

(h) Personally Identifiable Information (PII).

(i) Sensitive acquisition or contractual information.

(2) Current policies, implementation plans, and best practices specific to social media can be found at http://www.defense.gov/socialmedia and http://www.army.mil/media/socialmedia.

d. Protecting information from unauthorized disclosure. It is imperative that operations security, and Information Security regulations be followed in accordance with AR 25–2, AR 530–1, and AR 380–5. Army personnel must safeguard classified and sensitive information in all communications and must understand that online communications expose operations to risk; communication outside of official channels (such as .com domains) increase risk.

e. Specific external official presence requirements.

(1) External official presence (EOP) includes official public affairs activities conducted on IbC.

(2) EOP activities must be conducted in compliance with sections 4–2, as workable. Additional requirements, specific to EOP are:

(a) Approval will be obtained from the responsible DOD Component Head before establishing EOP.

(b) Official branding will be used in accordance with DODD 5535.09 and other guidance that may be issued by the Office of Public Affairs.

(c) Clear identification that a DOD Component provides the content for the EOP will be provided.

(d) The Army organization under which the EOP is managed, the mission of that organization, and the purpose of the EOP will be provided, as workable.

f. Use of internet-based capabilities.

(1) Internet-based capabilities, including social media sites and web-based interactive technologies not under the control of DOD, can be valuable tools to assist Army components in providing important information to military and civilian personnel in both official and unofficial capacities. All information disseminated via IbC should be approved for consumption by an audience external to DOD and used for purposes deemed necessary in the interest of the U.S. Army (for example, public communication, recruitment, marketing). Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, will not be disclosed.

(a) Non-public 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. For detailed instruction regarding the collection, dissemination, storage, and processing of unclassified information via IbC, please refer to DA Pam 25–1–1.

g. Use of public Army internet services.

(1) Public Army Internet services can be used for collection, dissemination, storage, or processing of information that has been cleared and authorized for release to the public via Federal-owned, operated or controlled Internet Services. Public Army Internet Services can be useful for communicating with key stakeholder groups external to the Army, for purposes including public affairs, recruiting, research, collaboration, and outreach to the general populations.

(a) Information disseminated via these services require mandatory content review and approval procedures for information posted to publicly accessible websites as outlined in DODI 5230.29.

(b) Guidance for managing a Public Army Internet service on an unclassified network to collect, disseminate, store, and otherwise process unclassified Army information is provided in DA Pam 25–1–1.

h. Use of private Army internet services. Private Army Internet services are used to provide both DOD-wide and local information to an audience internal to the Federal Government (for official use only (FOUO)/Unclassified). Guidance for organizations to establish, operate, and/or maintain a Private Army Internet service on an unclassified network to collect, disseminate, store, and otherwise process non-public information to specific audiences is provided in DA Pam 25–1–1 and 4–7 of this document.

4–12. Visual information management

a. Visual information. VI addresses the acquisition, creation, storage, transmission, distribution, and disposition of still and motion imagery; and linear or nonlinear multimedia, with or without sound, for the purpose of conveying information. VI includes the exchange of ideas, data, and information, regardless of formats and technologies used (see DODI 5040.02). VI will be viewed and used as an essential information resource and a supporting capability for strategic communication. Army activities will make, acquire, or create VI, appropriately distribute VI gathered, and preserve VI obtained following procedures detailed in DODI 5040.02.

b. Defense imagery management operations center. All Army VI activities will participate in the Army Documentation Program by making daily submissions of record VIDOC to the Defense Imagery Management Operations Center (DIMOC) for accessioning. The capture and submission of record VIDOC will be considered high priority by all VI activities.

(1) Historically significant visual information documentation products. DRUs, COMCAM teams, and local VI activities will submit historically significant VIDOC products directly to DIMOC. Provide noncurrent VI records having historical or long-term value to DIMOC for accessioning into the DOD VI records holdings or the National Archives and Records Administration.

(2) Tactical documentation. COMCAM teams obtain record VIDOC during theater-level Army and Joint wartime operations, contingencies, exercises, or humanitarian operations. COMCAM teams will electronically forward imagery, with embedded captions, to DIMOC for distribution to operational decisionmakers and other customers. COMCAM teams will provide original source materiel to DIMOC for accessioning.

c. Visual information activities responsibilities.

(1) All multimedia/visual information (M/VI) activities will use DD Form 2858 (Visual Information Activity Profile) to review, update, and certify compliance with their defense visual information activity number (DVIAN) and the C4IM services list annually, no later than 30 September of each odd-numbered fiscal year (see DA Pam 25–91 for procedural information). Regardless of cost and without exception, all Army productions will be documented using the online DD Form 1995 (Visual Information (VI) Production Request and Report). Approval will be obtained prior to commencing production. If no suitable production exists in the Content Discovery and Access Catalog, complete section 1 of DD Form 1995 in coordination with the supporting VI activity to establish the production requirement. DD Form 1995 initiates the production process and remains with the production through its life cycle.

(2) AMVID supports the requirements in DODI 5040.02 by operating and maintaining VI activity authorized to support the Office of the Secretary of Defense, the Office of the Chairman of the Joint Chiefs of Staff, Headquarters Department of the Army and other major commanders, and other Federal Agencies in the NCR as required. AMVID includes a specialized VI activity to procure total productions and other VI end products from commercial sources to support the Army, other DOD Component requirements as established in resourcing agreements. AMVID is the Army's component coordinating point, which is a central designated point in the Army for the coordination of imagery for transmission to the DIMOC records holdings in accordance with DODI 5040.02.

d. The enterprise multimedia center. Enterprise multimedia centers (EMCs) support the realignment of VI resources, functions, and facilities for the transforming institutional Army. The EMC will be designed to support mission products and services as defined in the C4IM services list and connected to an Armywide network. The EMC will provide products and services classified as "above-baseline" or "mission-funded" on a fee-for-service basis and documented in an SLA. All requests received on an installation for above-baseline mission services and products will be forwarded to the EMC for production or approval for local installation production. The EMC will provide in-house production of multimedia and VI in support of Army, DOD, other military departments, and other Government agency requirements. Each installation Multimedia/VI activity will be connected to an EMC for support from a single location. For more information on EMC's, see DA Pam 25–91.

e. Visual information procedures. For more information on the Visual Information Systems Program, certifications of VI assets, and the VIDOC program, see DA Pam 25–91.

f. Visual information records management. Original local or non-local Army multimedia VI productions and VI products, with their associated administrative documentation, are controlled as official records throughout their life cycle, and disposal in accordance with General Records Schedule 21, DODI 5040.02, this regulation, and DA Pam 25–91. For VI housekeeping files, refer to AR 25–400–2. Refer to Table 4–1 for required VI forms.

g. Customer self-help. Unless an exception or waiver is submitted through the ACOM and granted by CIO/G–6, training support centers will provide the full suite of customer self-help support, which includes the production of simple products (for example, briefing charts, sign-out boards, flyers, or flip charts).

h. Recording events. All M/VI products and services are for official use only. As a general rule, social events such as military balls and hails and farewells are unofficial and considered entertainment except where nationally or historically significant.

Table 4–1
Required visual information forms

Form	Purpose
DA Form 4103 (Visual Information (VI) Product Loan Order)	To record media loans.
DA Form 3903 (Multi-Media/Visual Information (M/VI) Work Order)	To identify and capture all work associated with a customer request for products and services.
DA Form 5695 (Information Management Requirement/Project Document)	To document all requirements for VI items (excluding expendables and consumables) with an end item cost over $25,000.
DD Form 1367 (Commercial Communication Work Order)	To submit a commercial communication work order against an existing consolidated contract when acquiring telecommunications services for the installation. Ordering officers, appoint in writing 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 exceeding the ordering officer's threshold to the ARCYBER contracting officer.
DD Form 2537 (Visual Information Caption Sheet)	To maintain a system for numbering individual product items based on DODI 5040.02 requirements. Still photographs, motion picture footage, video recordings (excluding those assigned a personal identification number), and audio recordings, if retained for future use, will be assigned a VI re- cord identification number. All VI material retained for future use will be captioned.
DD Form 1995 (Visual Information (VI) Production Request and Report)	To manage the life cycle of VI productions.

4–13. Publishing and printing

a. Functional proponent. AR 25–30 designates the AASA as the functional proponent for the APP. The APP consists of development, production, and dissemination of all official DA publications. The APP also provides oversight of printing, reproduction, self-service copying, and related equipment and operations.

b. Management. The AASA provides centralized control and management of the Army's departmental publishing and distribution system, to include distribution of hard copy and electronic editions of DA publications and blank forms.

c. Statutory restrictions for publications and requirements for printing. Refer to AR 25–30 for policy on restrictions in publishing, printing, and distribution of materials and requirements for all printing and duplicating work.

d. Requisitioning printing.

(1) All Army printing and duplicating (including compact disc-read only memory replication) will be prescribed in accordance with policies in AR 25–30.

(2) Army organizations will consider effective and economic printing options when determining whether in-house or commercial resources will be used in accomplishing mission objectives.

(3) Functional managers at all levels of command will conserve printing, duplicating, and self-service copying resources (including personnel, funds, material, and equipment) consistent with conducting operations essential to mission support.

(4) In the event of and during the initial stages of mobilization, authority is granted to the field to produce any departmental publication (including blank forms) necessary for mission requirements. This automatic authority will remain in effect until otherwise notified by AASA (SAAA (APP)), 105 Army Pentagon, Washington, DC 20310–0105.

e. Self-service printing device management.

(1) All discussions about printing devices in this publication, unless otherwise specified, refer only to printing devices that are self-service devices.

(2) Exclusions. Specialty equipment for graphics shops (high-definition/high-resolution, high-color fidelity devices), topography printers, psychological operations printers, other technical printers (blueprint/large bed), and equipment in authorized Army field printing plants and reproduction facilities.

(3) Functional managers will—

(a) Manage printing devices.

(b) Develop, monitor, and enforce departmental policies, regulations, and instructions governing self-service printing devices.

(c) Advise organizational leadership regarding acquisition, operation, accountability, consolidation, and disposition of printing device equipment and operations as warranted.

(d) Maximize use of networked multi-function devices (MFDs), and phase out print-only devices when possible.

(e) Assist tenant and satellite activities as needed in relocating and justifying printing devices and related equipment.

(f) Collect and analyze production data for all printing devices.

(g) Oversee compliance for the procurement and maintenance of printing devices and printing device supplies (except paper). Responsibilities include, but are not limited to—

1. Determine the print capacity needed by the requesting organization or activity, in accordance with mission need and DOD guidance, by assessing the average number of documents produced in a specific time period by the activity. The printing device inventory must be capable of handling that number of reproductions in that time period, with minimal overcapacity.

2. Manage inventory of printing devices and supplies. Increase or decrease the number of devices within an organization's printing environment to achieve balanced deployment of these devices. Conduct an assessment to determine the existing printing device inventory and actual needs in terms of printing device numbers and sizes. Adjust the inventory accordingly.

3. Ensure use of CHESS to purchase or lease all printing and copying devices. For printing and copying devices used in CONUS, consider use of enterprise contracts, enterprise license agreements, or blanket purchase agreements available via CHESS. OCONUS activities will use appropriate procurement vehicles.

4. Obtain ITAS approval to purchase or lease printing and copying devices from a non-CHESS vendor. This requirement applies to both CONUS and OCONUS activities.

5. Coordinate with the local NEC and/or local service provider to ensure that printing devices connected to the Army network are connected and configured correctly. This requirement is applicable to the classified and unclassified networks. The NEC will apply the DISA STIG for all printing devices on the Army network.

6. Utilize network printing devices to the fullest extent. Most printing devices in the inventory should be connected to the Army network, regardless of how many personnel a particular device supports. Networked printers can be monitored centrally, which facilitates better overall inventory management.

7. Enforce the optimization of cost-efficient printing and copying features, using duplex printing and efficient print quality. The NEC can help to maximize printing device efficiency.

8. Maintain records listed in paragraph 4–11*g*. Make these records available to CIO/G–6 upon request.

9. Monitor the number of service calls on specific printing devices to determine when printers, copiers, and MFDs should be taken out of service or replaced. Dispose of devices in accordance with established property disposal and security procedures.

10. Require requesting organizations to obtain approval for their stated requirements by preparing and submitting an administrative request memorandum (an example may be found in DA Pam 25–1–1) and DA Form 4951 (Lease/Purchase Analysis for Copying/Duplicating Machines) for validation/technical review by the functional manager prior to acquisition.

11. Conduct analyses of administrative request memoranda and DA Form 4951 to ensure the correct type and number of printing devices are acquired.

f. Self-service printing device acquisition.

(1) Commands and agencies will purchase or lease printing devices through CHESS (unless they are granted an approved ITAS waiver). CHESS has two buying periods per year – January to March and June to September – and it offers a selection of printers that can be leased or purchased. The consolidated buy is the most cost-effective way for Army organizations to purchase IT products.

(2) Conduct a cost-benefit analysis using DA Form 4951 to clearly document that the chosen service option (lease or purchase) is the most cost-effective option prior to entering into a service contract. The cost-benefit analyses must document that consideration was given to—

(a) Using existing self-service printing device equipment or service contracts already available through the local functional printing device manager.

(b) The cost of exercising any buyout options on existing equipment.

(c) The useful life of owned equipment prior to initiating a separate self-service printing device contract.

(3) Submit an administrative request memorandum (see DA Pam 25–1–1) and a completed DA Form 4951 to the functional manager for validation/technical review prior to acquisition.

(a) At a minimum, one alternate proposal from a different vendor must be considered in the selection process.

(b) Army organizations will not acquire printing devices for the primary purpose of circumventing the use of in-house printing or reproduction facility, or Defense Logistics Agency Document Services.

g. Self-service printing device records.

(1) Army organizations will maintain consolidated annual statistics for owned, leased, or contract service copy devices in accordance with AR 710–2 and DA Pam 710–2–1. Such records will be made available to CIO/G–6 upon request. Records maintained by the command or agency must include—

(a) Equipment brand, model number or name, and serial number.

(b) Type of procurement (lease/purchase/cost per copy) and installation date.

(c) Location of equipment (organization, building, and room number.)

(d) Purchase price (if owned).

(e) Equipment characteristics, such as production speed, accessories, or special features.

(f) Record of repair and maintenance.

(g) Number of copies produced monthly and annually.

(h) Total annual depreciation.

(i) Total annual rental cost.

(j) Total annual maintenance cost.

(k) Total annual cost of supplies (except paper).

(l) Total annual cost of all components.

(m) Cost per copy per self-service printing device (except paper).

(n) Completed DA Form 4951 (reflecting the information required in para 4–11g, above).

4–14. Morale, welfare, and recreation activities and non-appropriated fund instrumentalities

40 USC 762 requires that agencies provide EIT access to employees and members of the public with disabilities. The access must be comparable to the access available to individuals who do not have disabilities.

a. Information technology access

(1) The law applies to all Federal agencies that develop, procure, maintain, or use EIT. Section 508 of the Rehabilitation Act Amendments of 1998 was enacted to eliminate barriers in IT, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

(2) Unless an exception applies (see DA Pam 25–1–1), all Federal or DOD acquisitions of EIT must meet the applicable accessibility technical standards or the functional performance criteria (36 CFR 1194) as established by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board). For more information, see http://www.access-board.gov/.

(3) EIT includes equipment or interconnected systems or subsystems of equipment that are used to create, convert, or duplicate data or information. More specific examples of EIT include, but are not limited to, telecommunication products (such as telephones), information kiosks and transaction machines, web sites, multimedia, and office equipment (such as copiers and fax machines). Review website at http://www.section508.gov for further information and training about the laws and regulations pertaining to Section 508 and how to support its implementation. Section 508 is applicable to—

(a) All contracts for EIT supplies and services. Except for indefinite-delivery contracts, it is applicable to all delivery orders or task orders for EIT.

(b) All procurement actions for EIT processed by Government contractors, regardless of the customer being supported.

(4) Information managers will make all reasonable efforts to accommodate individuals with disabilities, consistent with the laws cited above and AR 600–7. At no cost to individual activities, the Computer/Electronic Accommodations Program (CAP), at 5111 Leesburg Pike, Suite 810, Falls Church, VA 22041–3206, provides assistive technology accommodations and services to persons with disabilities at the DOD. The CAP operates a Technology Evaluation Center to match people

with specific technologies. Funding is available to provide such things as interpreters, readers, personal assistants, telecommunications devices, telephone amplifiers, listening devices, and closed-captioned decoders and visual signaling devices for those with hearing problems. For more information, see DA Pam 25–1–1 and http://www.cap.mil/.

b. Morale, welfare, and recreation activities.

(1) Use of appropriated funds (APF) is required to support executive control and essential command supervision activities, including telephones, computers, and communications for all MWR Category A, B, and C programs as defined by AR 215–1. Expending NAF for these activities requires a certificate of non-availability of APF before procuring. All items that are authorized APF funding must comply with this regulation.

(2) Use of APF on a non-reimbursable basis is authorized to provide communications and data automation support to—

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

(b) Temporary duty, permanent change of station, and military treatment facility lodging programs as outlined in DODI 1015.12.

(c) Medical holdover (MH) members residing in DOD housing are authorized to use a television with cable or satellite service, Internet service, and telephone service. MH members are responsible for any charges associated with premium cable, satellite service, and long-distance calls. Excludes Initial Entry Training both Basic Combat Training and Advanced Individual Training members assigned to MH units who typically live in barracks that do not have TV, cable, telephone, internet service in those rooms, as they would have in operational units.

(d) All other Non-appropriated Fund Instrumentalities (NAFIs) as outlined in DODI 1015.15 (Army and Air Force Exchange Service, civilian welfare and restaurant funds, and so on).

(3) NAF programs and activities and NAFI entities will comply with AR 70–1 and this regulation for acquisition and management of MWR systems authorized or obtained with APF.

(4) NAFI requiring NEC-provided IT support will comply with this regulation and those procedures promulgated by the installation NEC (see AR 25–13).

4–15. Telework

Authorized individuals may telework according to DOD and Army policy (see DODI 1035.01).

Section III

Department of Defense Information Network Operations and Cybersecurity

4–16. Department of Defense Information Network Operations and Cybersecurity

The Army closely coordinates and ensures unity of effort between cybersecurity and DODIN operations. Cybersecurity activities (see AR 25–2) predominately originate as policy and doctrine and guide execution of DODIN operations, with a primary focus on the action to protect the network. This integration and linkage between cybersecurity and DODIN operations directly informs and supports the broader mission of cyberspace operations (CO), as well as, enabling nearly every aspect of total Army operations by allowing the Army to have confidence in the confidentiality, integrity, and availability of the DODIN and Army information to make decisions. Specifically related to CO, the coordination of cybersecurity and DODIN operations forms the foundation of cyberspace situational awareness, including current and predictive knowledge of all factors affecting friendly and adversary cyberspace forces, as well as, maintaining the network as a critical communication channel to commanders. Additionally, the integration of cybersecurity and DODIN operations provide the network that enables CO commanders to execute defensive cyber operations and offensive cyber operations cyberspace missions. Refer to AR 25–2 for policy, roles, responsibilities, and procedures for managing cybersecurity risk and safeguarding IT and information.

4–17. Maintaining the Army's Hardware and Software Baseline

This section identifies the certifications that must be obtained before a software or hardware change can be made to the Army's approved network baseline. Prior to operational use, system developers and operators must ensure that all systems and enabling components have been assessed as to their utility, risk of network disruption, and risk of introducing vulnerabilities; and have been properly certified for operations as a component of the approved Army network baseline.

a. File transfer protocol. File transfer protocol sites in the public domain are not authorized and will not be used in the place of authorized public websites.

b. Internet protocol management.

(1) Internet protocol address space management. ARCYBER is designated the Army IP management and registration agent and will lead the execution of the Army's IP management policy. ARCYBER is the only Army organization authorized to obtain IP address space from the DOD Network Information Center and will control allocation and assignment of IP address space within the Army (see chap 2 for roles and responsibilities).

(2) Internet Protocol version 6 (IPv6). IPv6 provides many capabilities, including increased address space, quality-of-service, and mobility enhancements. Army organizations and agencies will upgrade public- and external-facing servers and services (for example, web, email, domain name system, Internet service provider services, and so forth) to use dual-stack (internet protocol version 4 (IPv4)/IPv6 in accordance with data center consolidation, applications migration, and DOD/Army IPv6 transition program requirements; internal-client applications that communicate with public Internet servers and supporting enterprise networks to use dual-stack IPv4/IPv6 in accordance with DOD/Army IPv6 transition program requirements). Army organizations and agencies with internal network backbones that interface with the NIPRNET must be IPv6-capable to synchronize with the NIPRNET core transition as defined by the DOD. Specifically, any new IP product or system developed, acquired, or produced must—

(a) Be compliant with IPv6 for all application and product features.

(b) Have contractor or vendor IPv6 technical support available for development and implementation and fielded product management.

(c) Apply all of the requirements above to all IP-related acquisition systems.

(3) Procurement considerations. During the procurement process, organizations must assess if a product is IPv6- capable or can be made IPv6-capable. Factors to be considered are the following:

(a) Interoperability in heterogeneous environments with IPv4 systems or components.

(b) Vendor certification that—

1. The vendor commits to upgrade as the DISR IPv6 standard profiles evolve.
2. The vendor commits to provide IPv6 technical support.
3. Product has JITC certification and is included on the DOD UC Approved Products List.

c. Use of internet protocol restrictions. Public websites are considered unrestricted or restricted. A website that is intended to be accessible from the Internet to anyone and authentication is not required for access, is considered a public unrestricted website. A website that is intended to be accessible from the Internet, but access is restricted to authorized users and authentication is required, is considered a public restricted website.

d. Voice over internet protocol and voice over secure internet protocol. Organizations that have a requirement to use voice over internet protocol (VoIP) or voice over secure Internet protocol to perform their missions will implement solutions in accordance with DODI 8100.04, CJCSI 6211, and CIO/G–6 guidance. Organizations must use only authorized products listed on the UC Approved Products List at https://aplits.disa.mil/. This requirement applies to both VoIP equipment and the associated LAN. Organizations with a requirement to implement VoIP must first submit their request through the local installation NEC. The request will then be processed through the appropriate signal command and forwarded to the CIO/G–6/SAS–AOI, 107 Army Pentagon, Washington, DC 20310–0107 for approval. Organizations not available on an installation with a NEC will forward their requirement via the appropriate chain of command, who will then forward the requirement through ARCYBER for forwarding to CIO/G–6. The package submitted to CIO/G–6 must include the following: a detailed justification; an operational need statement; architecture; supported organizations or entire installation; impact statement describing results of not receiving an approved waiver; a Bill of Materials; the location where the equipment will be installed or where construction or renovation will take place; an approved requirements document; and, a General Officer or Senior Executive Service endorsement.

4–18. Army's Risk Management Framework

All Army IT hardware, software, firmware, applications, or web services that receive, process, store, display, or transmit Army information is subject to the Army implementation of the DOD RMF in accordance with AR 25–2 and DA Pam 25–2–14 procedures for assessing and managing risk. The RMF replaces the DOD Information Assurance Certification and Accreditation Process and eliminates the Networthiness processes (that is obtaining a Certificate of Networthiness).

4–19. Identity and access management

Army will use DOD Identity and Access Management data to populate and maintain strategic and tactical directories, applications, systems, and Global Address List with a single set of trust identity credentials. All Army email and web servers that host sensitive information will be configured to use certificate-based client authentication using only DOD PKI-approved certificates. Issuance of the CAC will serve as the authoritative source for account provisioning. For policy on Identity and access management, please refer to AR 25–2.

4–20. Privacy Impact Assessment

Army organizations must observe Federal, DOD, and Army policies for protecting personal information contained in government records and systems, including information obtained through electronic collection portals, such as websites.

a. A privacy impact assessment (PIA) is an analysis of how PII is handled in electronic form by information system/electronic collection (ISEC). An ISEC collects, maintains, uses, and/or disseminates PII about members of the public, DOD personnel (government civilians, members of the military and non-appropriated fund employees), contractors, or foreign nationals employed at U.S. military facilities.

(1) A PIA determines the risks and effects of ISECs that collect, maintain, and disseminate information in identifiable electronic form.

(2) A PIA examines and evaluates protection and alternative processes for handling information to mitigate potential privacy risks.

(3) A PIA conforms to applicable legal, regulatory, and policy requirements regarding privacy.

b. If ISEC has the ability to retrieve an individual's name, date of birth, social security number and contains a personal identifier of an individual, then the ISEC will require a System of Records Notice. The System of Records Notice identifier must be documented on the PIA. Refer to AR 25–22 for information regarding system of records notices.

c. Procedures for submitting a PIA are delineated in the DA Pam 25–1–1 (see DODI 5400.16 and DD Form 2930 (Privacy Impact Assessment (PIA))).

d. All PIAs that identify information collected from members of the general public and Federal personnel and/or contractors will be displayed on the CIO/G–6 website at http://ciog6.army.mil/privacyimpactassessments/tabid/71/default.aspx.

e. A PIA is required on new information technology, electronic collections, and/or when changes create new privacy risks, including significant system management changes, significant merging, new public access, incorporation of commercial sources, new interagency uses of data, and/or alterations in character of data, such as the addition of health or financial information.

f. A PIA should be performed on information systems and electronic collections including those supported through contracts with external sources.

4–21. Electromagnetic spectrum operations

a. Spectrum management is planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. The Army Spectrum Management Program, executed in accordance with procedures outlined in AR 5–12, is aligned with DOD directives and instructions, the National Telecommunications and Information Administration, United States Code, and other Federal Department statutes.

b. The Army will 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 boundary of a sovereign nation 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 C2 relationships will apply in OCONUS locations. NECs coordinate, plan, program, and fund for the management of the electromagnetic spectrum as outlined in AR 5–12, the C4IM services list, and this publication. The NEC ensures emitter usage on the installation complies with AR 5–12 and operates within the scope of the specific frequency assignment. This responsibility cannot be delegated unless authorized by the Army Spectrum Manager. The installation NEC or other designated individual in the area or region provides spectrum management support. Commands will—

(1) Ensure that the installation frequency coordinator is trained through a military department spectrum manager’s course. Frequency coordination constitutes dealing with international and national laws on a regular basis in addition to safety of life issues. Assigning this function as an additional duty or temporary assignment to untrained personnel could have severe repercussions.

(2) Conduct ongoing review of frequency assignments for deletion or amendment. In CONUS, U.S. Government policy requires Army users to revalidate each permanent frequency assignment to delete or modify the record, normally every 5 years. OCONUS, Army records require a similar review under Allied Communications Publication 190(D) US SUPP–1(D) or per combatant command directives.

(3) Promote awareness of the operating parameters (power level, antenna type, height, gain, authorized operational use, area of operation, and so on) of assigned frequencies.

(4) Coordinate with installation directorates and tenant organizations to ensure that spectrum-dependent equipment (for example, fire alarms, paging systems, handheld radios, and barcode readers) being developed or procured for use on the installation is fully supportable.

(5) Establish a program in which each tenant and/or supported organization that uses spectrum-dependent emitters perform positive radio control duties as identified in AR 5–12.

Appendix A

References

Section I

Required Publications

AGO 2017–01
Assignment of Functions and Responsibilities Within Headquarters, Department of the Army (Cited in para 2–10*a*.)

AR 25–2
Army Cybersecurity (Cited in para 1–1*a*.)

AR 25–22
The Army Privacy Program (Cited in para 3–36*b*.)

AR 25–30
Army Publishing Program (Cited in title page.)

AR 70–1
Army Acquisition Policy (Cited in para 2–3.)

AR 71–9
Warfighting Capabilities Determination (Cited in para 2–3*k*(5).)

AR 215–1
Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities (Cited in para 4–14*b*(1).)

AR 215–4
Nonappropriated Fund Contracting (Cited in para 2–33*h*.)

AR 380–5
Department of the Army Information Security Program (Cited in para 1–1*a*.)

AD 2016–38
Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers (Cited in para 3–31*b*(4)(*b*).)

CJCSI 5123.01H
Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS) (Cited in para 3–26*b*.)

CJCSI 5128.01
Mission Partner Environment Executive Steering Committee (MPE ESC) Governance and Management (Cited in para 2–10*d*(12).)

DA Pam 25–1–1
Army Information Technology Implementation Instructions (Cited in para 2–1*f*.)

DA Pam 25–91
Visual Information Procedures (Cited in para 2–10*d*(17).)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read the publication to understand this regulation.

ACP 123
Common Messaging Strategy and Procedures

ACP 190 US SUPP–1(D)
Allied Communications Publication – US Supplement 1-(D) - Guide to Frequency Planning

AFARS, Part 5139
Acquisition of Information Technology

AGO 2006–01
Transfer and Reassignment of the U.S. Army Records Management and Declassification Agency

AGO 2017–07
Designation of the USARCYBER Command as an ASCC, alignment of the Army's portion of the Department of Defense Information Network roles and responsibilities, reassignment of United States Army NETCOM to USARCYBER Command, and discontinuation of Second Army

AR 5–1
Management of Army Business Operations

AR 5–11
Management of Army Models and Simulations

AR 5–12
Army Use of the Electromagnetic Spectrum

AR 5–20
Competitive Sourcing Program

AR 5–22
The Army Force Modernization Proponent System

AR 11–2
Managers' Internal Control Program

AR 12–1
Security Assistance, Training, and Export Policy

AR 15–1
Department of the Army Federal Advisory Committee Management Program

AR 25–6
Military Auxiliary Radio System and Amateur Radio Program

AR 25–13
Army Telecommunications and Unified Capabilities

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 25–58
Publishing in the Federal Register

AR 25–59
Office Symbols

AR 25–400–2
The Army Records Information Management System (ARIMS)

AR 27–26
Rules of Professional Conduct for Lawyers

AR 27–60
Intellectual Property

AR 34–1
Multinational Force Interoperability

AR 71–32
Force Development and Documentation

AR 73–1
Test and Evaluation Policy

AR 190–53
Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 195–2
Criminal Investigation Activities

AR 215–7
Civilian Nonappropriated Funds and Morale, Welfare, and Recreation Activities

AR 335–15
Management Information Control System

AR 350–1
Army Training and Leader Development

AR 360–1
The Army Public Affairs Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–40
Safeguarding and Controlling Communications Security Material (U)

AR 380–53
Communications Security Monitoring

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 420–1
Army Facilities Management

AR 500–3
U.S. Army Continuity of Operations Program Policy and Planning

AR 525–27
Army Emergency Management Program

AR 530–1
Operations Security

AR 550–1
Processing Requests for Political Asylum and Temporary Refuge

AR 600–7
Nondiscrimination on the Basis of Handicap in Programs and Activities Assisted or Conducted by the Department of the Army

AR 640–30
Official Army Photographs

AR 690–950
Career Program Management

AR 700–127
Integrated Product Support

AR 700–131
Loan, Lease, and Donation of Army Materiel

AR 700–142
Type Classification, Materiel Release, Fielding, and Transfer

AR 710–2
Supply Policy Below the National Level

AR 735–5
Property Accountability Policies

AR 750–1
Army Materiel Maintenance Policy

AD 2016–16
Changing Management Behavior: Every Dollar Counts

CIO/G–6 Memorandum
Army Information Technology Service Management (ITSM) Policy

CJCSI 3170.01I
Joint Capabilities Integration and Development System (JCIDS)

CJCSI 5128.02
Mission Partner Environment Executive Steering Committee; Coalition Interoperability Assurance and Validation Working Group

CJCSI 6211.02D
Defense Information Systems Network (DISN) Responsibilities

CJCSI 6285.01D
Mission Partner Environment Information Sharing Requirements Management Process

CNSSI 4009
National Information Assurance (IA) Glossary

CTA 50–909
Field and Garrison Furnishings and Equipment

DA Memo 25–51
Records Management Program

DA Pam 25–1–2
Information Technology Contingency Planning

DA Pam 25–2–14
Risk Management Framework for Army Information Technology

DA Pam 25–40
Army Publishing Program Procedures

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 70–3
Army Acquisition Procedures

DA Pam 700–142
Instructions for Type Classification, Materiel Release, Fielding and Transfer

DA Pam 710–2–1
Using Unit Supply System (Manual Procedures)

DCID 6/3
Protecting Sensitive Compartmented Information within Information Systems

Defense Message System GENSER Message
Security Classification, Categories, and Marking Phrase Requirements

Defense Supplement to the Federal Acquisition Regulations Subpart 208.74
Enterprise Software Agreements

Deputy Secretary of Defense Memorandum
Guidance Regarding Cyberspace Roles, Responsibilities, Functions and Governance within the Department of Defense

DESMF, Edition III
DOD Enterprise Service Management Framework

DFAS–IN 37–1 Regulation
Finance and Accounting Policy Implementation

DFAS–IN Manual 37–100–FY
Army Management Structure (AMS)

DISAC 310–130–1
Submission of Telecommunications Service Requests

DOD 5015.02–STD
Electronic Records Management Software Applications Design Criteria Standard

DOD 5500.07–R
Joint Ethics Regulation (JER)

DOD 5400.07
DOD Freedom of Information Act (FOIA) Program

DOD FMR 7000.14–R
Department of Defense Financial Management Regulations (FMR)

DOD Agency Strategic Plan
FY 2015–2018 DOD Agency Strategic Plan

DOD DTM 08–037
Policy for Department of Defense (DOD) Interactive Internet Activities

DOD Information Enterprise Architecture
Core Data Center Reference Architecture

DODD 3020.26
DOD Continuity Policy

DODD 5000.01
The Defense Acquisition System

DODD 5105.83
National Guard Joint Force Headquarters – State (NG JFHQS-State)

DODD 5144.02
DOD Chief Information Officer (DOD–CIO)

DODD 5230.09
Clearance of DOD Information for Public Release

DODD 5400.11
DOD Privacy Program

DODD 8000.01
Management of the Department of Defense Information Enterprise (DOD IE)

DODD 8100.02
Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)

DODD 8115.01
Information Technology Portfolio Management

DODI 1000.15
Procedures and Support for Non-Federal Entities Authorized to Operate on DOD Installations

DODI 1015.10
Military Morale, Welfare, and Recreation (MWR) Programs

DODI 1015.12
Lodging Program Resource Management

DODI 1015.15
Establishment, Management, and Control of Non-appropriated Fund Instrumentalities and Financial Management of Supporting Resources

DODI 1035.01
Telework Policy

DODI 4000.19
Support Agreements

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 5000.76
Accountability and Management of Internal Use Software (IUS)

DODI 5040.02
Visual Information (VI)

DODI 5040.07
Visual Information (VI) Productions

DODI 5230.24
Distribution Statements of Technical Document

DODI 5230.29
Security and Policy Review of DOD Information for Public Release

DODI 5400.16
DOD Privacy Impact Assessment (PIA) Guidance

DODI 8100.04
DOD Unified Capabilities (UC)

DODI 8110.01
Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DOD

DODI 8310.01
Information Technology Standards in the DOD

DODI 8320.02
Sharing Data, Information, and Technology (IT) Services in the Department of Defense

DODI 8320.03
Unique Identification (UID) Standards for Supporting the DOD Information Enterprise

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 8440.01
DOD Information Technology (IT) Service Management (ITSM)

DODI 8500.01
Cybersecurity

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT)

DODI 8530.01
Cybersecurity Activities Support to DOD Information Network Operations

DODI 8550.01
DOD Internet Services and Internet-Based Capabilities

DODI 8551.1
Ports, Protocols, and Services Management (PPSM)

DODI 8560.01
Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing

DODI 8582.01
Security of Unclassified DOD Information on Non-DOD Information Systems

DODM 4160.21
Defense Materiel Disposition Manual

DODM 5200.01, Volume 1
DOD Information Security Program Marking of Classified Information

DODM 5200.02
Procedures for the DOD Personnel Security Program (PSP)

DRMS Instruction 4160.14
Operating Instructions for Disposition Management

EO 12845
Requiring Agencies to Purchase Energy Efficient Computer Equipment

EO 12958
Classified National Security Information

EO 12999
Educational Technology: Ensuring Opportunity for all Children in the Next Century

EO 13103
Computer Software Piracy

EO 13514
Federal Leadership in Environmental, Energy, and Economic Performance

EO 13589
Promoting Efficient Spending

EO 13693
Planning for Federal Sustainability in the Next Decade

FAR
Federal Acquisition Regulation

FIAR 2017
DOD Financial Improvement and Audit Readiness Guidance for 2017

FISMA 2014
Federal Information Security Modernization Act of 2014

FM 6–02
Signal Support to Operations

GAO "Green Book"
GAO standards for Internal Control in the Federal Government (the "green Book")

General Records Schedule 21
Audiovisual Records, Transmittal No. 8, December 1998

HQDA G–3/5/7 EXORD 080–17
Alignment of Army DODIN Operational Roles and Responsibilities

HQDA G–3/5/7 EXORD 209–11
Army Data Center Consolidation Plan (ADCCP)

HSPD 12
Policy for a Common Identification Standard for Federal Employees and Contractors

ISO 9001:2015
International Standards Organization, 4th Edition

JP 1–0
Joint Personnel Support

JP 1–02
Department of Defense Dictionary of Military and Associated Terms

JP 3–12
Cyberspace Operations

JP 3–13
Information Operations

JP 6–0
Joint Communications System

JTR
Joint Travel Regulations

Memorandum, Deputy Secretary of Defense
Conducting Official Business on Electronic Messaging Accounts, 16 January 2018

Memorandum, Secretary of the Army
Support to the Army Request for Information Technology (ARFIT) Process, 28 June 2012

Memorandum, Secretary of the Army
Army Request for Information Technology (ARFIT) Policy, 16 April 2013

Memorandum, Secretary of the Army
Army Information Technology Integration and Governance, 5 April 2017

Memorandum, Secretary of the Army and Chief of Staff of the Army
Army Knowledge Management (AKM) Guidance Memorandum: Capabilities-Based Information Technology (IT) Portfolio Governance, 20 July 2015

NIST SP 800–47
Security Guide for Interconnecting Information

NSA/CSS PM 9–12
NSA/CSS Storage Device Sanitization Manual

OMB Cir A–11
Preparation, Submission, and Execution of the Budget

OMB Cir A–76
Performance of Commercial Activities

OMB Cir A–123
Managements Responsibility for Enterprise Risk Management and Internal Control

OMB Cir A–130
Management of Federal Information Resources

OMB DCOI Memorandum Cir M–16–19
Data Center Optimization Initiative (DCOI)

OMB Manual M–12–18
Managing Government Records Directive

OMB Manual M–16–02
Category Management Policy 15–1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops

OMB Manual M–16–12
Category Management Policy 16–1: Improving the Acquisition and Management of Common Information Technology: Software Licensing

OMB Memorandum 10–22
Guidance for Online Use of DOD Web Measurement and Customization Technologies

PL 104–208
Omnibus Consolidated Appropriations Act, 1997

PL 107–314
Bob Stump National Defense Authorization Act for Fiscal Section Year 2003

RCS CSIM–46
Information Management Requirement/Project Document

RCS CSIM–59
VI Annual Workload and Cost Data Report

SB 700–20
Army Adopted/Other Items Selected for Authorization/List of Reportable Items

Social Media Handbook
The United States Army Social Media Handbook

STIG
Security Technical Implementation Guide

UFC 4–510–01
United Facilities Criteria Design: Military Medical Facilities

5 CFR 2635
Standards of Ethical Conduct for Employees of the Executive Branch

36 CFR Chapter 7
Library of Congress

36 CFR 1194
Electronic and Information Technology Accessibility Standards

36 CFR 1237
Audiovisual, Cartographic, and Related Records Management

67 FR 36
Volume 67, Federal Register, p. 36

2 USC Subtitle F
The Health Insurance Portability and Accountability Act (HIPAA) of 1996

5 USC 552
Freedom of Information Act

5 USC 552a
Privacy Act of 1974

10 USC 1588
Authority to accept certain voluntary services

10 USC 2222
Defense business systems: business process reengineering; enterprise architecture; management

10 USC 2223
Information Technology: Additional Responsibilities of Chief Information Officers

10 USC 2667
Leases: non-excess property of military departments and defense agencies

10 USC 2686
Utilities and Services: Sale; Expansion and Extension of Systems and Facilities

10 USC 3014
Office of the Secretary of the Army

17 USC 101
Definitions

17 USC 501
Infringement of Copyright

18 USC 701
Official Badges, Identification Cards, Other Insignia

31 USC 1341
Limitations on expending and obligating amounts

32 USC
National Guard

40 USC 762
Public Buildings, Property, and Works (PL 100–542, Telecommunications Accessibility Enhancement Act of 1988.)

40 USC 11101 to 11704
Information Technology Management

40 USC 11312
Capital Planning and Investment Control

40 USC Subtitle III
Clinger-Cohen Act

44 USC Chapter 35
Coordination of Federal Information Policy

44 USC Chapter 36
Management and Promotion of Electronic Government Services

44 USC 3311
Destruction of Records Outside of Continental United States in Time of War or When Hostile Action Seems Imminent; written report to Archivist

44 USC 3501
Paperwork Reduction Act of 1995

44 USC 3506
Federal agency responsibilities

44 USC 3601
Definitions

47 USC 225
Telecommunications services for hearing-impaired and speech-impaired individuals

47 USC 611
Closed-captioning of public service announcements

Section III

Prescribed Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (https://armypubs.army.mil); DD forms are available from the Secretary of Defense website (http://www.esd.whs.mil/directives/forms/.)

DA Form 3903
Multi-Media/Visual Information (M/VI) Work Order (Prescribed in table 4–1.)

DA Form 4103
Visual Information (VI) Product Loan Order (Prescribed in table 4–1.)

DA Form 4951
Lease/Purchase Analysis for Copying/Duplicating Machines (Prescribed in para 4–13*e*(3)(*g*)(10).)

DA Form 5695
Information Management Requirement/Project Document (Prescribed in table 4–1.)

DD Form 1367
Commercial Communication Work Order (Prescribed in table 4–1.)

DD Form 1995
Visual Information (VI) Production Request and Report (Prescribed in para 4–12c(1).) (Available on Defense Automated Visual Information System (DAVIS).)

DD Form 2537
Visual Information Caption Sheet (Prescribed in table 4–1.)

DD Form 2858
Visual Information Activity Profile (Prescribed in 4–12c(1).) (Available at http://dodimagery.afis.osd.mil/.)

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) website (https://armypubs.army.mil); DD forms are available from the Secretary of Defense website (http://www.esd.whs.mil/directives/forms/.)

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 1391
FY__ Military Construction Project Data

DD Form 2930
Privacy Impact Assessment (PIA)

Appendix B

Internal Control Evaluation

B–1. Function

The function covered by this evaluation is the administration of Army IM and IT organizations. This includes key controls for CIO management, command senior IM officials, IA, C4IT support and services, VI management, records management, and publishing management.

B–2. Purpose

The purpose of this evaluation is to assist HQDA, FOAs, ACOMs, ASCCs, DRUs, PEOs, PMs, and managers associated with systems and data, and installations in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.

B–3. Instructions

Answers must be based on the actual testing of internal controls (such as document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least once every five years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions

a. Responsibilities (chapter 2). Have C4IT plans, programs, and requirements been coordinated with the appropriate IM and IT managers? (All)

b. Information Technology Governance and Investment Management (chapter 3).

(1) Are the duties and responsibilities of the senior information management official clearly designated in the organization's mission and function? (HQDA, region, ACOM, ASCC, and DRU)

(2) Has the installation clearly established a NEC who has the sole responsibility of implementing the installation's IM and IT program? (ASA (ALT) and ARCYBER)

(3) Has the organization analyzed (and documented the analysis of) its mission and revised mission-related and administrative work processes, as appropriate, before making significant IT investments in support of those processes? (HQDA, ACOM, ASCC, and DRU)

(4) Does the organization have a strategic plan that is linked to its mission? Is it periodically updated? (ACOM, ASCC, and DRU)

(5) Has a forum been established to develop and implement C4IT procedures, requirements, and priorities? (ASCC and DRU)

(6) Does the organization have a clearly defined process for submitting and screening new IT investment proposals for management consideration? (HQDA, ACOM, ASCC, and DRU)

(7) Does the IT investment-screening process include addressing the questions in this evaluation, resolving all issues prior to making an IT investment, and initiating any process analysis or improvement? (HQDA, ACOM, ASCC, and DRU)

(8) Does the process support core or priority mission functions? (HQDA, ACOM, ASCC, DRU, and FOA)

(9) Can the process be eliminated? (HQDA, ACOM, ASCC, and DRU)

(10) Can the process be accomplished more effectively, efficiently, and at less cost by another Government source (for example, DOD or other Federal agency) or the private sector? (HQDA, ACOM, ASCC, and DRU)

(11) Does the IT investment process clearly establish who in the organization has the responsibility and authority for making final IT-related investment decisions? (HQDA, ACOM, ASCC, and DRU)

(12) Are exceptions to the IT investment-screening process clearly documented? (HQDA, ACOM, ASCC, and DRU)

(13) Does the organization require that management evaluations for the IT investment-screening process, as well as scoring, ranking, and prioritization results, be documented (either manually or through the use of automated applications such as a decision support tool)? (HQDA, ACOM, ASCC, and DRU)

(14) Has the organization determined the financial statement impact of its IT portfolio as part of the respective system authorization?

(15) For systems determined to have a financial statement impact and/or process financial transactions, has the organization conducted assessments of those systems in accordance with the April 21, 2016 OUSD(C) and CIO memo titled, "Enhanced Integration of Financial Management Requirements with the Risk Management Framework"?

(16) Is there an overall framework and structure for maintaining an effective internal control documentation and monitoring process for efficient and effective operations, reporting reliable information, and compliance with applicable laws and regulations?

(17) Are IT investment decisions a part of the organization's integrated capital planning process or are IT projects separated out? (HQDA, ACOM, ASCC, and DRU)

(18) Does the organization have a process in place to conduct periodic reviews (in-house or via outside consultant or expert) of its current IT investment portfolio to assess alignment with mission needs, priorities, strategic direction, or major process reengineering? (HQDA, ACOM, ASCC, and DRU)

(19) Does the organization have a process for documenting and disseminating results of this review? (HQDA, ACOM, ASCC, and DRU)

(20) Are process analysis and improvements for Warfighting processes documented in the initial capabilities document using the DOTMLPF–P requirements methodology as defined by the Army requirements generation process in AR 71–9? (HQDA, ACOM, ASCC, and DRU)

(21) Have web-enabling status and future web-enabling plans been reported within the APMS? (All)

(22) Have functional managers developed a set of goals and objectives (with performance measures) to gauge overall functional mission improvement? Have accomplishments been reported to enterprise-level managers? (All)

(23) Have performance measures been developed for each IT investment that supports the organizational mission before execution of that investment? (HQDA, ACOM, ASCC, DRU, PEO, and PM)

(24) Have IT investments been synchronized to overall DOD and Army mission priorities? (HQDA, ACOM, ASCC, DRU, PEO, and PM)

(25) Is all IT accounted for in APMS? Are all IT and IT personnel assigned to a specific registered APMS system to account for them properly? (HQDA, ACOM, ASCC, and DRU)

(26) Are C4IM services only being done by the NEC or being provided for by a NEC contract? Does the NEC have a contract to perform baseline, enhanced baseline or above-baseline services? (HQDA, ACOM, ASCC, and DRU)

(27) Are all communication circuits, including commercial circuits accounted for? Are all contracts for IT executed in accordance with HQDA CIO/G–6 guidance? (HQDA, ACOM, ASCC, and DRU)

(28) Are performance measures linked to management-level goals, objectives, and measures? (All)

(29) Are requirements being developed in harmony with the Army's goal of creating an end-state strategy of implementing an enterprise resource planning business solution throughout a fully integrated Army logistics environment? (HQDA and ACOM)

(30) Are financial, logistics, facilities, human resources, contractors, and other senior Army leaders held accountable for ensuring business processes comply with financial audit standards? (HQDA)

(31) Are current Information Technology Commitment Item Codes, Elements of Expense, and Elements of Resource codes being used in accordance with the annually updated IT Purchasing Desk Side Standard Operating Procedures disseminated by the Army Budget Office for IT-related financial transactions? If corrections are required, are they being performed in a timely manner? (All)

(32) Has the organization published a policy on the issuance of IT devices to employees based upon mission and assigned position rather than the grade or rank of the individual? Does the policy minimize the number of IT devices per employee and provide the least amount required for the assigned mission? (All)

c. Cybersecurity. See AR 25–2.

*d. Information Technology Solutions Implementation (*chapter 4*).*

(1) Does the mission guidance include the responsibilities of the VI manager, to include organization structure and responsibilities of all components of the organization, and does it state that this VI manager provides overall policy, plans, and standards for all VI operations? (HQDA)

(2) Is the VI manager the single staff manager for all VI functions on the installation? (HQDA)

(3) Are all VI services and equipment, except those specifically exempted by the HQDA, consolidated for centralized VI management? (HQDA)

(4) Do all VI activities under the theater-level signal command's purview have a (DVIAN)? (HQDA)

(5) Does the VI manager approve all VI equipment required by AR 25–1, chapter 4? (HQDA)

(6) Is VI policy being followed for M/VI productions? (For example, DD Form 1995 is used, funds identified up front, personal identification number registers maintained, Content Discovery and Access Catalog searches conducted, service support contracts awarded for less than 50 percent of the total production cost, non-local Content Discovery and Access Catalog entries, and using Joint Visual Inspection System contracting facility.) (FOA and installation)

(7) Is a production folder maintained for the life cycle of local productions? (HQDA, FOA, and installation)

(8) Has your VI activity developed and implemented a standard level of agreement document, to including a standard operating procedure? (installation)

e. Records management. See DA Pam 25–403.

f. Publishing and printing management. See AR 25–30.

g. Enterprise architecture (chapter 3). (All, as applicable)

(1) Has the organization developed the appropriate architectures for the AEA to support the DOTMLPF–P components as mapped to net-centric data and services?

(2) Has the organization developed the appropriate architectures for the mission-command architecture that supports JCIDS, acquisition of system-of-systems and Family of systems, force development, and lessons learned from operations?

(3) Has the organization developed the necessary architectures for the business mission-command architecture that aligns to the appropriate BMA functional domains; and aligns with the requirements of the BCAC, as appropriate?

h. Installation-information technology services and support.

(1) Is a process in place for acquiring IT and ensuring all required licensing and registration are accomplished? (NEC)

(2) Is the NEC the single organization responsible for the oversight and management of installation IT? (NEC.)

(3) Are quarterly reviews of current IT within the APMS– Army IT Registry being conducted and have the users verified that they are still required and meeting users' needs? (HQDA, ACOM)

(4) Are evaluations being conducted of existing systems for obsolescence? (HQDA, ACOM)

(5) Has a business capability acquisition been performed prior to implementing the thin client concept? (NEC)

(6) Is an accurate inventory being maintained and validated annually for IT equipment? (NEC, IMO)

(7) Are COOP plans and procedures documented, distributed, and tested at least annually? (ACOM, NEC)

(8) Has guidance been provided to ensure all software is checked for viruses before being loaded? (NEC)

(9) Are existing capabilities and assets considered prior to upgrading, improving, or implementing LANs? (Theater-level signal command and NEC)

(10) Are uneconomical IT service contracts identified and terminated? (All)

(11) Has the NEC coordinated the acquisition of licenses with the CHESS office prior to entering into an agreement with a COTS vendor? (NEC)

(12) Are spare capacity and functional expansion of IT being considered or used when new requirements are identified? (All)

(13) Has the NEC reported the server consolidation status for all of its Army tenants to the CIO/G–6? (NEC)

(14) Are measures being taken to ensure that hard drives are disposed of properly? (NEC)

(15) Are criteria established for justifying and approving the acquisition of cellular phones and pagers? (signal command (theater), and NEC)

(16) Has guidance been provided to review and revalidate cellular telephones and pagers every 2 years? (Theater- level signal command, and NEC)

(17) Do procedures require the establishment of a reutilization program to identify and turn in cellular phones and pagers that are no longer required or seldom used? (NEC)

(18) Is there a requirement for cellular phones and pagers to be recorded in the property book? (NEC)

(19) Has the NEC implemented accountable billing procedures? (NEC)

(20) Have maintenance and support strategies been devised to minimize overall systems life cycle cost at an acceptable level of risk? (PEO, PM, and ACOM)

(21) Have program managers, project managers, and IT MATDEVs coordinated their system architectures and fielding plans with the gaining commands and DRUs, Theater-level signal command, and installation NECs prior to fielding systems? (PEO and PM)

(22) Do safeguards exist to ensure that computer users do not acquire, reproduce, or transmit software in violation of applicable copyright laws? (theater-level signal command, NEC, and IMO)

(23) Are private-sector service providers made aware that written assurance of compliance with software copyright laws may be required? (theater-level signal command, NEC, and IMO)

(24) Does website require HTTPS in accordance with paragraph 4–6? (NEC and website owners)

(25) Are existing portals being migrated to AKO and AKO–SIPRNET? (All)

(26) Does each website contain a clearly defined purpose statement that supports the mission of the organization? (All)

(27) Are users of each publicly accessible website provided with privacy and security notice prominently displayed or announced on at least the first page of all major sections of each web information service? (All)

(28) If applicable, does the website contain a disclaimer notice for links to any site outside of the official DOD web information service (usually the .mil domain)? (All)

(29) Is the website free of commercial sponsorship and advertising? (All)

(30) Is the website free of persistent cookies or other devices designed to collect PII about web visitors? (All)

(31) Is each website made accessible to disabled users in accordance with Section 508 of the Rehabilitation Act? (All)

(32) Is the operational information identified below purged from publicly accessible websites? (All)

(a) Plans or lessons learned that would reveal military operations, exercises, or vulnerabilities.

(b) Sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

(c) Personal information about U.S. citizens, DOD employees, and military personnel, to include the following: Social Security numbers; dates of birth; home addresses; directories containing name, duty assignment, and home telephone numbers; names; locations; or any other identifying information about Family members of DOD employees or military personnel.

(d) Technological data such as weapon schematics, weapon system vulnerabilities, electronic wire diagrams, and frequency spectrum data.

(33) Does the information system or electronic collection collect, maintain, use, or disseminate PII?

(34) Does the information system or electronic collection collect, maintain, use, or disseminate social security numbers in any format?

(35) Does the information system or electronic collection collect information from members of the public?

(36) Does the information system or electronic collection retrieve data using a personal or unique identifier?

(37) Are operational security tip-off indicators in the following categories purged from the organization's publicly accessible website? (All)

(a) Administrative. Personnel travel (personal and official business), attendance at planning conferences, commercial, support contracts, and FOUO information.

(b) Operations, plans, and training. Operational orders and plans; mission-specific training; exercise and simulations activity; exercise, deployment, or training schedules; unit relocation or deployment information; inspection results, findings, and deficiencies; unit vulnerabilities or weaknesses.

(c) Communications. Spectrum emissions and associated documentation; changes in activity or communications patterns. Use of Internet and email by unit personnel (personal or official business); availability of secure communications; hypertext links with other agencies or units; and Family support plans, bulletin board postings, or messages between Soldiers and their Family members.

(d) Logistics and maintenance. Supply and equipment orders and deliveries; transportation plans; mapping; imagery and special documentation support; maintenance and logistics requirements; and receipt or installation of special equipment.

(38) Has the website reviewer performed a key word search for any of the following documents and subsequently removed sensitive personal or unit information from publicly accessible websites? (Document review of deployment schedules; duty rosters; exercise plans; contingency plans; training schedules; inspection results, findings, and deficiencies; biographies; Family support activities; phone directories; and lists of personnel) (All)

(39) Are existing infrastructure capabilities and assets considered prior to upgrading, improving, or modernizing? (HQDA and ACOM)

(40) Is the fully qualified domain name (for example, https://www.us.army.mil or http://www.apd.army.mil) for Army sites registered with the Government Information Locator Service at http://defense.gov/registeredsites/submit-link.aspx/ and the contact information updated annually?

(41) Are the web servers IAVA-compliant and placed behind a reverse proxy server?

(42) Did the command program their MILCON project's MUE with their PEG? (All)

(a) Provide a List of Material: IT equipment list and its associated cost. (All)

(b) Identify needed Labor: Who is installing the IT-fit out? Is the work a turnkey solution? (Contractor buying and installing the IT equipment for completed package. Equipment and labor separate) (All)

(c) Develop a Cost schedule: Time line of when the funds are due contracting, contract schedule? (All)

(d) Develop a Project schedule: Identify Schedule changes, project changes? When is Soldier Readiness Date and Building Occupancy Date? (All)

(e) Are the IT requirements and cost reasonable and accurate? (All)

B–5. Supersession

This evaluation replaces the evaluation for the administration of Army IM and IT previously published in AR 25–1, dated 25 June 2013.

B–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to CIO/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (usarmy.pentagon.hqda-cio-g-6.mbx.policy-inbox@mail.mil).

Glossary

Section I

Abbreviations

A&A
assessment and authorization

AAMBO
Army Application Migration Business Office

AASA
Administrative Assistant to the Secretary of the Army

ABC
Army Business Council

ACA
Architecture Compliance Assessment

ACAT
acquisition category

ACOM
Army command

ACP
Army Campaign Plan

ACSIM
Assistant Chief of Staff for Installation Management

AD
Army Directive

ADB
Army Data Board

ADC
Army Data Council

ADCCP
Army Data Center Consolidation Plan

ADMP
Army Data Management Program

ADS
authoritative data source

AEA
Army Enterprise Architecture

AEACC
Army enterprise architecture certification/compliance

AEDC
Army Enterprise Data Center

AENC
Army Enterprise Network Council

AESM
Army Enterprise Service Management

AESMF
Army Enterprise Service Management Framework

AGO
Department of the Army General Order

AIA
Army Information Architecture

AIC
Army Interoperability Certification

AICFB
Army Interoperable Certified Fielded Baseline

AKO
Army Knowledge Online

AMC
U.S. Army Materiel Command

AMVID
Army Multimedia and Visual Information Directorate

APF
appropriated funds

APMS
Army Portfolio Management Solution

APP
Army Publishing Program

AR
Army regulation

ArCADIE
Army Capabilities and Architecture Development and Integration Environment

ARCYBER
U.S. Army Cyber Command

ARFIT
Army Request for Information Technology

ARFIT–MI
Army Request for Information Technology-Military Intelligence

ARIMS
Army Records Information Management System

ARNG
Army National Guard

ARSTAF
Army Staff

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASA (FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

ASC
Army Standards Council

ASCC
Army service component command

ATEC
U.S. Army Test and Evaluation Command

ATGR
Army Technical Guidance Repository

ATP
acceptance test procedure

AWIC
Army Warfighting Integration Council

AWRAC
Army Web Risk Assessment Cell

BCAC
Business Capability Acquisition Cycle

BEA
business enterprise architecture

BMA
Business mission area

C4
command, control, communications, and computers

C4IM
command, control, communication, and computers for information management

C4IT
command, control, communication, and computers for information technology

CAC
common access card

CAP
Computer/Electronic Accommodations Program

CCA
Clinger-Cohen Act

CDC
core data center

CDO
Chief Data Officer

CEDC
component enterprise data center

CENTRIX
Combined Enterprise Regional Information Exchange

CFBL
Combine Federated Battle Laboratories

CG
Commanding General

CHESS
Computer Hardware, Enterprise Software and Solutions

CHS
common hardware systems

CIAV
Coalition Interoperability Assurance & Validation

CIO
Chief Information Officer/G–6

CJCSI
Chairman, Joint Chiefs of Staff Instruction

CM
configuration management

CMO
Chief Management Officer

CO
cyberspace operations

COE
common operating environment

COMCAM
combat camera

COMSEC
communications security

CONOPS
concept of operations

CONUS
continental United States

COOP
continuity of operations

COTS
commercial, off-the-shelf

CP
Career Program

CPIC
capital planning and investment control

CR
change request

CSA
Chief of Staff of the Army

CSO
cloud service offering

CSS
Central Security Servic**e**

CSSP
cybersecurity service provider

CTSF
Central Technical Support Facility

DA
Department of the Army

DAG
Defense Acquisition Guidebook

DARNG
Director, Army National Guard

DAVIS/DITIS
Defense Automated Visual Information System/Defense Instructional Technology Information System

DBC
Defense Business Council

DBS
defense business system

DCIM
Data Center Inventory Management

DCOI
Data Center Optimization Initiative

DCS
Deputy Chief of Staff

DER
data engineering resources

DESMF
DOD Enterprise Service Management Framework

DIMA
Army portion of the DOD portion of the Intelligence Mission Area

DIMOC
Defense Imagery Management Operations Center

DISA
Defense Information Systems Agency

DISN
Defense Information Systems Network

DISR
DOD Information Technology Standards Registry

DLA
Defense Logistics Agency

DM
data management

DMZ
demilitarized zone

DOD
Department of Defense

DODAF
DOD Architecture Framework

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODIN
Department of Defense Information Network

DODIN–A
Army portion of the Department of Defense Information Network

DODM
Department of Defense manual

DOTMLPF–P
doctrine, organizations, training, materiel, leadership and education, personnel, facilities-Policy

DR
disaster recovery

DREN
Department of Defense Research and Engineering Network

DRU
direct reporting unit

DS
Data Steward

DSE
data services environment

DVIAN
defense visual information activity number

EB
Executive Board

EIE
enterprise information environment

EIEMA
Enterprise Information Environment mission area

EIT
electronic and information technology

ELA
enterprise license agreement

eMASS
Enterprise Mission Assurance Support Service

EMC
enterprise multimedia center

EO
Executive Order

EOP
external official presence

ESA
enterprise service agreement

ESI
enterprise software initiative

FaNS
federated net-centric sites

FAR
Federal Acquisition Regulation

FIAR
financial improvement and audit readiness

FISMA
Federal Information Security Modernization Act

FOA
field operating agency

FOIA
Freedom of Information Act

FORSCOM
U. S. Army Forces Command

FRCS
Facility-related control systems

FY
fiscal year

GAO
Government Accountability Office

GOSC
General Officer Steering Committee

GTG–F
Global Information Grid Technical Guide-Federated

HIPAA
Health Insurance Portability and Accountability Act

HQDA
Headquarters, Department of the Army

HSPD
Homeland Security Presidential Directive

HTTPS
hyper text transfer protocol secure

I3A
installation-information infrastructure architecture

IA
information assurance

IbC
internet-based capabilities

IE
information enterprise

IEA
information enterprise architecture

IES
information exchange specifications

IM
information management

IMO
information management officer

INFOSYS
information systems

INSCOM
U.S. Army Intelligence and Security Command

IP
internet protocol

IPR
in-process review

IPT
integrated process team

IPv4
internet protocol version 4

IPv6
internet protocol version 6

IRM
information resource management

IS
information system

ISA
interconnection security agreement

ISEC
information system/electronic collection

ISG
Interoperability Steering Group

ISIG
Intelligence Senior Initiatives Group

ISN
Installation Service Node

ISO
International Standards Organization

ISP
information support plan

ISR
installation status report

ISR–MC
installation status report-mission capacity

ISR–S
installation status report-services

IT
information technology

ITAS
Information Technology Approval System

ITIM
information technology investment management

ITOC
Information Technology Oversight Council

ITSMO
Information Technology Service Management Office

IUS
internal use software

JCIDS
Joint Capabilities Integration and Development System

JFHQ
Joint Forces Headquarters

JIE
Joint Information Environment

JIIM
joint, interagency, intergovernmental, and multinational

JITC
Joint Interoperability Test Command

JS
Joint Staff

JWICS
Joint Worldwide Intelligence Communication System

LAN
local area network

LWN
LandWarNet

M/VI
multimedia/visual information

MA
Mission Area

MARS
Military Auxiliary Radio System

MATDEV
materiel developer

MDA
milestone decision authority

MDEP
management decision execution package

MEDCOM
U.S. Army Medical Command

MFD
multi-function device

MH
medical holdover

MI
Military Intelligence

MILCON
military construction

MIP
Military Intelligence Program

MIRC
Migration Implementation and Review Council

MOA
memorandum of agreement

MPE
mission partner environment

MSC
major subordinate command

MTOE
modified table of organization and equipment

MUE
mission-unique equipment

MWR
morale, welfare, and recreation

NAF
non-appropriated funds

NARA
National Archives and Records Administration

NCR
National Capital Region

NEC
Network Enterprise Center

NGB
National Guard Bureau

NIEM
National Information Exchange Model

NIP
National Intelligence Program

NIPRNET
non-secure internet protocol routing network

NR–KPP
net-ready key performance parameters

NSA
National Security Agency

NSS
National Security Systems

OBT
Office of Business Transformation

OCONUS
outside the continental United States

OMB
Office of Management and Budget

OSD
Office of the Secretary of Defense

PA
Privacy Act

PACES
Parametric Cost Engineering System

PED
portable electronic device

PEG
Program Evaluation Group

PEO
program executive office

PEO EIS
Program Executive Officer Enterprise Information Systems

PfM
portfolio management

PIA
privacy impact assessment

PII
personally identifiable information

PIT
platform information technology

PKI
Public Key Infrastructure

PM
project manager

POM
program objective memorandum

PP&E
property, plant, and equipment

PPBE
planning, programming, budgeting, and execution

R&M
restoration and modernization

RA
reference architectures

RDT&E
research, development, test, and evaluation

RIG
Resource Integration Group

RMF
Risk Management Framework

RRS-A
Army Records Retention Schedule-Army

SAP
Special Access Program

SATCOM
satellite communications

SC
Signal Command

SCI
sensitive compartmented information

SCOP
Senior Component Official for Privacy

SECARMY
Secretary of the Army

SIPRNET
secure internet protocol router network

SLA
service level agreement

SMS
Strategic Management System

SoNA
statement of non-availability

SPPN
special purpose processing node

SSL
secure sockets layer

STIG
Security Technical Implementation Guide

SV
system view

T&E
test and evaluation

TA
Technical architecture

TDA
table of distribution and allowances

TEP
temporary exception to policy

TRADOC
U.S. Army Training and Doctrine Command

TTP
tactics, techniques, and procedures

UC
Unified Capabilities

UID
unique identifier

USA
Under Secretary of the Army

USACE
U.S. Army Corps of Engineers

USAISEC
U.S. Army Information Systems Engineering Command

USAR
U.S. Army Reserve

USASOC
U.S. Army Special Operations Command

USC
United States Code

USCYBERCOM
U.S. Cyber Command

VAUTI
visible, accessible, understandable, trustable, and interoperable

VCSA
Vice Chief of Staff of the Army

VI
visual information

VIDOC
visual information documentation

VoIP
voice over internet protocol

WMA
Warfighter Mission Area

Section II

Terms

Acquisition
The acquiring of supplies or services (including construction) with appropriated funds and for the use of the Federal Government through purchase or lease; whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established; and includes the description of requirements to satisfy agency needs, solicitation, and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

Activity
An Army organization. Within the context of the AEA, a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes in support of accomplishing tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element.

Administrative work processes
Enabling activities that support mission and mission-related processes and functions (for example, manage legal process, performance assessment, combat health support, Family support, and so on).

Application
Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, or facilitating email. For purposes of reporting in APMS, applications may be reported as a separate investment or included in an information system registration. If reported as a separate investment, applications will identify in the dependency tab, the system it is part of as the parent information system. Otherwise, identify the hosting environment in the infrastructure tab as directed.

Appropriated Funds
Refers to moneys allocated by legislation passed by Congress and signed by the President. Appropriated Funds are usually specified in Congress’s yearly budget or continuing resolution. However, funds can be allocated in any bill passed by Congress. This money comes primarily from Federal Income Tax and other Federal taxes. Appropriated Funds may only be used for the purpose they have been appropriated for. Agencies can incur penalties and employees can face legal charges for misappropriating funds

Architecture
See enterprise architecture and Army enterprise architecture.

Army application migration business office
The Program Executive Office Enterprise Information Systems (PEO EIS), in coordination with the CIO/G–6, established AAMBO to serve as the Army's single point of contact for system and application owners. AAMBO provides assistance in defining requirements, recommending the most cost-effective hosting solution, and supporting system and application owners throughout the application migration process.

Army business enterprise architecture
The Army BEA is the enterprise architecture for the DOD BMA and reflects DOD business transformation priorities; the Business capabilities required to support those priorities; and the combinations of enterprise systems and initiatives that enable those capabilities. It also supports use of this information within an end-to-end (E2E) framework. The purpose of the BEA is to provide a blueprint for DOD business transformation that helps ensure the right capabilities, resources, and materiel are rapidly delivered to the force. The BEA guides and constrains implementation of interoperable DBS solutions

as required by USC 2222. It also guides IT investment management to align with strategic business capabilities as required by the Clinger-Cohen Act, and supports the OMB and Government Accountability Office (GAO) policies.

Army enterprise architecture
See also enterprise architecture. The AEA transforms operational visions and associated required capabilities of the business and warfighting missions into a blueprint for an integrated and interoperable set of information systems and NSS that implement horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA supports the DODIN–A and is the combined total of all the Army's operational, technical, and system architectures.

Army Enterprise Data Center
The Army Enterprise Data Center (AEDC) meets the required DOD/NIST standards/specifications as a DOD defined component enterprise data center (CEDC). AEDCs are intended to provide capabilities at the Army enterprise level. AEDCs will be built to the specifications necessary to deliver the technical and mission capabilities required by the owning Component. AEDCs must be registered as a CEDC within the DOD's SNaP IT Data Center Inventory Management (DCIM) system database. AEDC requirements include: Facility Infrastructure, Computing & Storage Infrastructure, Capability Delivery and Standardized Operations and Processes to include automated DCIM capabilities. AEDCs delivering services across installation boundaries to other entities must be built to meet mission requirements of affected parties. AEDCs will meet DOD standards for cybersecurity.

Army enterprise infrastructure
The systems and networks that comprise the DODIN–A.

Army interoperability certification
Certification from CIO/G–6 that the candidate system has undergone appropriate testing and that the applicable standards and requirements for compatibility, interoperability, and integration have been met.

Army knowledge management
The process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. Within the context of Army IT, it is the Armywide strategy to transform the Army into a network-centric and knowledge-based force to improve information dominance by our warfighters and business Stewards. It includes, but is not limited to, improving processes, technology, and work culture to collaborate, catalog, store, find, and retrieve information; and share this information with Joint, coalition, and international partners as mission needs dictate.

Army net–centric data management program
Establishes policy, guidance, and instruction about the set of data standards, business rules, and data models required to govern the definition, production, storage, ownership, and replication of data.

Army recordkeeping systems management
Cost-effective organization of Army files and records contained in any media so that records are readily retrievable. Ensures that records are complete; facilitates the selection and retention of permanent records; and accomplishes the prompt disposition of noncurrent records in accordance with National Archives and Records Administration approved schedules.

Army records information management system
The Army's automated recordkeeping system used to properly manage information from its creation through final disposition, according to Federal laws and Army recordkeeping requirement. The Federal Records Act of 1950, as amended, contains the statutory authority for the ARIMS program.

Army website
A collection of hypertext markup language pages, graphics, images, video, audio, databases, or other media assets at a URL, which is made available for distribution or is distributed or transmitted (with or without limitation) via the world wide web for reception and display on a computer or other devices including but not limited to mobile phones, personal digital assistants or interactive television; and whose content is controlled, authorized, or sponsored by an Army organization or representative.

Armywide enterprise architecture
Defined by the DoD Information Enterprise Architecture (IEA) (see http://dodcio.defense.gov/inthenews/dodinformationenterprisearchitecture.aspx). The EIEMA is responsible for the Infrastructure services and as a result is the Enterprise Integrator for Shared Services across all MAs. Each of the four MAs: BMA, WMA, EIEMA, and DIMA will be responsible for their architecture.

Attribute
A property or characteristic of one or more entities (for example, race, weight, or age). Also, a property inherent in an entity or associated with that entity for database purposes.

Authentication
A security service that verifies an individual's eligibility to receive specific categories of information.

Authoritative data source
A recognized or official data-production source (with a designated mission statement, source, or product), which publishes reliable and accurate data for subsequent use by customers. An ADS may be the functional combination of multiple, separate data sources.

Automation
Conversion of a procedure, process, or equipment to automatic operation. When allied to telecommunications facilities, automation may include the conversion to the automatic operation of the message processing at an exchange or remote terminal.

Bandwidth
The rate at which an amount of data can be sent through a given transmission channel.

Benchmark
A procedure, problem, or test that can be used to compare systems, components, processes, and so forth to each other.

Beneficial occupancy date
Construction complete; user move-in dates.

Broadcast
The transmission of radio, television, and data signals through the air waves or fiber optic cable.

Business and functional process improvement
A systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes in order to achieve improvements in performance in areas important to customers and stakeholders (see also DODD 8000.01).

Business enterprise architecture
The BEA is the enterprise architecture for the DOD BMA and reflects DOD business transformation priorities; the business capabilities required to support those priorities; and the combinations of enterprise systems and initiatives that enable those capabilities. It also supports use of this information within an end-to-end (E2E) framework. The purpose of the BEA is to provide a blueprint for DOD business transformation that helps ensure the right capabilities, resources, and materiel are rapidly delivered to the force. The BEA guides and constrains implementation of interoperable DBS solutions as required by USC 2222. It also guides IT investment management to align with strategic business capabilities as required by the Clinger-Cohen Act, and supports the OMB and GAO policies.

Capability
In the context of the AEA framework, a capability satisfies a requirement, specifically an IT requirement. For example, an Army headquarters element has the requirement to know the location of all friendly and enemy units in its area of operations. Situational awareness is the capability that satisfies this requirement.

Capital planning and investment management
The capital planning and investment management process is to develop C4IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4IT expenditures across all functional domains. The capital planning and investment management process is collaborative among C4IT stakeholders, with a focus on C4IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets.

Closed–circuit television
Point-to-point signal transmission by cable or directional radiation where the audience is limited by physical control or nonstandard transmission.

Cloud computing
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Cloud services provider/cloud service offering
A cloud service provider is an organization that provides cloud services. These services come in a variety of service and deployment models, but their characteristics involve one or more of the following: on-demand self-service, resource pooling, rapid elasticity, measured service, and broad network access. The cloud service offering is a specific set of services the cloud service provider makes available to cloud consumers.

Coalition interoperability assurance and validation
Services provided by the U.S. CIAV Team to combatant commands and their mission partners to resolve process, training, and technical capability gaps hampering efficient information exchange.

Command and control
Exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. These functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures that are used by a commander to plan, direct, coordinate, and control forces and operations for the accomplishment of the mission.

Command and control system
Any system of facilities, equipment (including hardware, firmware, and software), communications, procedures, and personnel available to commanders at all echelons and in all environments; and essential to plan, direct, and control operations conducted by assigned resources.

Command, control, communications, and computer systems
Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications, and computers.

Command, control, communications, and computers for information management services list
The source document that defines the Army Enterprise baseline and mission IT services provided or supported by the NEC. This list of service definitions is the foundation for the development and publishing of the customer-facing DODIN–A [the Army's portion of the DODIN (Department of Defense Information Network)] services catalog. The C4IM services listed as baseline are core or common-user services that are the responsibility of the Army to centrally fund. Those services listed as "Mission" are the responsibility of the ACOMs/mission commanders to resource. These services are not in the baseline, but are required based on the mission (for example, cell phones, pagers, personal digital assistants) and are grounded by the business processes that enable mission execution in a more efficient and effective manner.

Common–use
Services, materiel, or facilities provided by a DOD agency or a military department on a common basis for two or more DOD agencies, elements, or other organizations as directed.

Communications
See telecommunications.

Communications network
A set of products, concepts, and services that enables the connection of computer systems for the purpose of transmitting data and other forms (for example, voice and video) among the systems.

Communications security
Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto-security, transmission security, emission security, and physical security of COMSEC material.

Communications systems
A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

Communities of interest
The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes; and who therefore must have a shared vocabulary for the information they exchange.

Community of practice
A community of practice (CoP) is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice. CoPs cut across formal organizational structures and increase individual and organizational agility and responsiveness by enabling faster learning, problem solving, and competence building; greater reach to expertise across the force; and quicker development and diffusion of best practices. CoP structures range from informal to formal and may also be referred to as structured professional forums, knowledge networks, or collaborative environments.

Compatibility
The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

Compliance
A system that meets, or is implementing an approved plan to meet, all applicable TA mandates.

Component
One of the subordinate organizations that constitute a Joint force. Normally, a Joint force is organized with a combination of Service and functional components. An assembly or any combination of parts, subassemblies, and assemblies mounted together in the manufacture, assembly, maintenance, or rebuild.

Component Enterprise Data Center
See Army Enterprise Data Center (AEDC).

Computer network defense
(Joint) Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks (see JP 6–0).

Concept
A document or theory that translates a vision or visions into a more-detailed, but still abstract, description of some future activity or end-state, principally concerned with a 3- to 15-year time-frame.

Configuration
An expression in functional terms (that is, expected performance) and physical terms (that is, appearance and composition).

Connection fee
The charge, if any, imposed on a subscriber by the cable television franchisee for initial hookup, reconnection, or relocation of equipment necessary to transmit the cable television signal from the distribution cable to a subscriber's receiver.

Content discovery and access catalog
An online, unrestricted, full-text searchable, standard DOD-wide database containing content description, production, acquisition, inventory, distribution, currency status, archival control, and other data on VI productions and distance learning center products typically used in military training. Formerly DAVIS/DITIS.

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.

Cookie
A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. Cookies are embedded in the hypertext markup language information flowing back and forth between the user's computer and the servers. They allow user-side customization of web information. Cookies normally expire after a single session.

Core Data Center
Within the Joint Information Environment (JIE) A core data center (CDC) is a fixed DOD data center meeting DOD standards for facility and network infrastructure, cybersecurity, technology, and operations and adhering to enterprise governance. Functions and services delivered by current DISA Defense Enterprise Computing Centers, Component Enterprise Data Centers, and Component Installation Data Centers will be consolidated to the greatest extent possible.

Cost–effective
Describes the course of action that meets the stated requirement in the least-costly method. Cost-effectiveness does not imply a cost savings over the existing or baseline situation; rather, it indicates a cost savings over any viable alternative to attain the objective.

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 (see DODI 8500.01).

Cyberspace
A global domain consisting of the interdependent network of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (see JP 1–02 and National Security Systems Instruction 4009). The 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 (see DODI 8500.01).

Cyberspace operations
The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace operations consist of three (3) functions: offensive cyberspace operations; defensive cyberspace operations; and DOD information network operations.

Data
The representation of facts, concepts, or instructions in a formal manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities to which meaning is, or might be, assigned (see JP 1–02).

Data element
In electronic recordkeeping, a combination of characters or bytes referring to one separate item of information, such as name, address, or age (see JP 1–0).

Data engineering resource
A specification that is expressed in a formal syntax that is registered in the DSE. A data engineering resource may convey the data structure and validation constraints for an information exchange, has the program logic to translate between different representations, has the controlled vocabulary whose terms will be used in data exchanges or metacards, or describes the inputs, outputs, and operations for a web service, or an information system. Examples of DERs are XML schemas, schematron documents, stylesheets, Web Services Description Language documents, taxonomies, ontologies, and conformant samples.

Data management
The process of creating a basis for posting, sorting, identifying, and organizing vast quantities of data available to DOD.

Data model
A graphical and textual representation of data needed by an organization to represent achievement of its mission, functions, goals, objectives, and strategies. A data model is represented by its entities, attributes, and relationships among its entities. In the relational model of data, entities are tables, attributes are columns, and relationships are primary and foreign key pairs. Data models may be enriched beyond data structures with both constraints and embedded processes.

Data services environment
An enterprise capability that enables a holistic view of DOD data sources, their relationships, and their responsible governance authorities. It is a web-enabled interface with streamlined ADS registration and discovery capabilities that support the visibility of DOD data needs and the attribution of those needs to one or more authoritative bodies responsible for meeting or otherwise fulfilling those needs. For more information, see http://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/832007p.pdf.

Data standards
A documented agreement on representation, format, definition, structuring, tagging, transmission, manipulation, use, and management of data.

Data Steward
A subject matter expert who is under the direction of the Chief Data Officer and is responsible for developing, implementing, and enforcing Federal, Army, and their respective organization's data standards, processes, and procedures.

Database
A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications.

Defense business system
An information system that is operated by, for, or on behalf of the Department of Defense, including any of the following: (i) A financial system, (ii) A financial data feeder system, (iii) A contracting system, (iv) A logistics system, (v) A planning and budgeting system, (vi) An installations management system, (vii) A human resources management system, (viii) A training and readiness system.

Defense telephone system
A centrally managed system that, in accordance with its charter, provides telephone service to all DOD activities in the area.

Defensive Cyberspace Operations
(DOD) Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (see JP 1–02).

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, software (including applications), data, security services, other associated services, and national security systems. (Source: JP 6–0 and approved for inclusion in JP 1–02; JP 3–12). The DODIN includes DOD IT (for example, DOD-owned or DOD-controlled information systems (ISs), PIT systems, IT products and services) as defined in DODI 8500.01; and control systems and industrial control systems [as defined in National Institute (NIST) Special Publication (SP) 800–82] that are owned or operated by or on behalf of DOD Components (see DODI 8530.01).

Department of Defense information network – Army
The Army's portion of the DODIN is a universally accessible, standardized, protected, and economical network enterprise. DODIN–A seamlessly delivers network capabilities and services supporting the Army's Joint, interagency, intergovernmental, multinational operations, and business missions.

Department of Defense information network operations
Actions to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the security of the DODIN.

Department of Defense information technology standards registry
DISR is a Joint effort to identify and mandate IT standards for use in the acquisition and development of DOD systems. It focuses on the inter-operability and standardization of information technology and supports net-centric operations and warfare.

Department of Defense operational viewpoint
DOD Architecture Framework (DODAF)-described "models on the operational viewpoint" describe the tasks and activities, operational elements, and resource flow exchanges required to conduct operations. A pure operational model is materiel independent. However, operations and their relationships may be influenced by new technologies, such as collaboration technology, where process improvements are in practice before policy can reflect the new procedures. There may be some cases, as well, in which it is necessary to document the way activities are performed, given the restrictions of current systems, to examine ways in which new systems could facilitate streamlining the activities. In such cases, operational models may have materiel constraints and requirements that need to be addressed. For this reason, it may be necessary to include some high-level system architectural data to augment information onto the operational models.

Direct reporting unit
An operational command that reports to and is under the direct supervision of an HQDA element. A DRU executes its unique mission-based upon policy established by its HQDA principal.

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
Collections of similar capabilities that are grouped at a high level in order to support decisionmaking, capability delegation, and analysis.

Electronic business (e–business)
A way of performing enterprise activities involving the use of electronic technologies, such as facsimile, email, World Wide Web software, electronic bulletin boards, electronic funds transfer, purchase cards, and electronic data interchange.

Electronic government (E–Gov)
The use of web-based applications and other information technologies, combined with processes that implement these technologies, to: a) enhance access to and delivery of Government information and services to the public, other agencies, and other Government entities; or b) bring about improvements in Government operations that may include effectiveness, efficiency, service quality or transformation.

Electronic mail (email)
An information dissemination and retrieval service accessed through distributed user workstations normally provided through an office automation initiative.

Embedded information technology
Any IT item (hardware or software) which when removed from a device renders the IT item inoperable and the device nonfunctional for its intended purpose. Under this definition, the firmware in a smartphone and the guidance system in a missile are both examples of embedded IT. An example of IT that is not embedded is a laptop bolted down in a tank; the tank is able to operate without the laptop and the laptop is able to function without the tank

Enterprise
The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise architecture
A strategic information asset base, that defines the mission, information, and technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. An EA includes a baseline architecture, a target architecture, and a sequencing plan (see 44 USC 3601).

Enterprise data
Data shared across systems, applications, and processes by organizations, branches, divisions, and other sub-units in the enterprise.

Enterprise information environment
The common, integrated computing and communications environment of the DODIN–A. The EIE is composed of DODIN–A assets that operate as, or assure, LANs, campus-area networks, tactical networks, operational-area networks, metropolitan-area networks and wide-area networks. The EIE is also composed of DODIN–A organizational, regional, or global-computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the DODIN–A. The EIE included a common set of enterprise services, called Core Enterprise Services, which provide awareness, and delivery of information on the DODIN–A.

Enterprise information environment mission area
The EIEMA represents the common, integrated information computing and communications environment of the DODIN–A. The EIE is composed of DODIN–A assets that operate as, provide transport for, and/or assure LANs, campus-area networks, tactical operational and strategic networks, metropolitan-area networks, and wide-area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DOD enterprise hardware, software operating systems, and hardware/software support that enable the DODIN–A. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the DODIN–A.

Enterprise multimedia and visual information service center
The VI activity that provides general support to all installation, base, facility, or site organizations or activities. It may include motion picture, still photo, television, and audio recording for nonproduction documentary purposes, their laboratory support, graphic arts, VI libraries, and presentation services.

Enterprise network
The connection of all components, departments, organizations, and locations into a single standardized, compatible, interoperable, and secure intra-Army network. The single intra-Army network (Army enterprise network) integrates all systems in the Army (and all systems outside the Army requiring data exchange with the Army) to provide seamless information superiority that supports the Army's Joint, interagency, intergovernmental, multinational operations, and business missions. This translates to system-wide engineering, common strategy and architecture, and a single concept of operation and authority for DODIN–A operations. The Army's enterprise is prescribed by the CIO.

Environment
The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.

Exhibit documents
Exhibit 53s and 300s are reporting requirements established by the Office of Management and Budget for an agency's IT investment portfolio.

Extensible markup language
A tagging language used to describe and annotate data so that the data can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension.

Extranet
Similar to Government Intranet, an Extranet includes outside organizations, vendors, industry partners, and individuals outside the DOD information network (DODIN) to facilitate inter-business transactions, such as placing and checking orders, tracking merchandise, and making payments. Extranets require access-control via authorized external certificates.

Facsimile
A system of telecommunications for the transmission of fixed images with a view to their reception in a permanent form. These images include typewritten and handwritten documents, fingerprint records, maps, charts, operations overlays, sketches, and low-resolution photographs.

Federal personnel
Officers and employees of the Government of the United States, members of the Uniformed Services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DOD dependents are considered members of the general public.

Federated architecture
An approach for EA development, which is comprised of a set of coherent but distinct entities or architectures, or the architectures of separate members of the federation. The members of the federation participate to produce inter- operable, effectively integrated EA. The federation sets the overarching rules of the federated architecture, defining the policies, practices, and legislation to be followed; as well as the inter-federated procedures and processes, date interchanges, and interface standards to be observed by all members of the federation. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission (see AR 25–13).

Franchise
Authorization, or renewal thereof, issued by a franchising authority; whether such authorization is designated as a franchisee, permit, license, resolution, contract, certificate, agreement, or otherwise, which authorizes the construction or operation of a cable system.

Franchisee
Any individual or partnership, association, joint stock company, or trust corporation who owns or controls, is owned or controlled by, or is under common ownership or control with such person.

Function
Within the context of the AEA framework, a synonym for activity.

Functional proponent
Commander or chief of an organization or staff element that is the operative agency charged with the accomplishment of a particular function(s) (see AR 5–22).

Government office equipment/services
Equipment and/or systems purchased, leased, and/or owned by the government. This includes, but not limited to, IT equipment, pagers, Internet services, Email, Library resources, telephones, portable electronic devices (PED), Smartphones, facsimile machines, photocopiers, and office supplies.

GuardNet
The IT infrastructure of the National Guard securely supporting the NGB Joint team using nationwide information systems and a mission-command network spanning 11 time zones, 54 States and territories, and the District of Columbia at approximately 3,000 separate locations. GuardNet provides ARNG access to the DODIN–A [the Army's portion of the DODIN (Department of Defense Information Network)] and Joint access to Air Force network services in those States.

Hardware
The generic term dealing with physical items as distinguished from the capability or function, such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. In data automation, the physical equipment or devices forming a computer and peripheral components (see also software).

Imagery
A pictorial representation of a person, place, thing, idea, or concept, either real or abstract, used to convey information.

Information
Any communication or representation of knowledge, such as facts, data, or opinion; in any medium or form including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information enterprise
The holistic, end-to-end approach of a variety of IT activities and tasks, which include infrastructure-management, DM, networking, system engineering, database and software design, and management, and the administration of entire systems resulting in an Armywide capability that covers the entire life cycle of information and knowledge. IE includes matters involving information technology, network defense, and network operations contributing to the DODIN–A [the Army's portion of the DODIN (Department of Defense Information Network)]. The Army's IE is the core domain of the CIO/G–6, which includes the people, processes, and technology that resource and deliver IT services and support Armywide.

Information exchange specification
A narrowly scoped data model that facilitates data exchange and interoperability between COIs.

Information management
Planning, budgeting, manipulating, and controlling information throughout its life cycle.

Information management office or officer
The office or individual responsible to the respective commander, director, or chief responsible for coordinating service definition, management oversight, advice, planning, and funding coordination of all IT and IM requirements (business and mission) for the organization. The IMO assists the commander, director, or chief in exercising responsibility to effectively manage the organization's IT and IM processes and resources that enable the organization's business and mission processes.

Information Operations
Information operations (IO) is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own (see JP 3–13).

Information requirement
The expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or recordkeeping systems, whether manual or automated.

Information resources management
The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, maintenance, utilization, dissemination, and disposition of information, regardless of media. Includes the management of information and information-related resources and systems, whether manual or automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information; and the acquisition and use of automatic data processing, telecommunications, and other IT.

Information support plan
A set of information supporting interoperability test and certification. Entered through the GTG–F portal, the ISP contains or links to the NR–KPP along with supporting architectural data (see DODD 4630.05, DODI 4630.8, and CJCSI 5123.01H).

Information system
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS, the terms "application" and "information system" are both IT investments describing a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see JP 1–02). The application of IT to solve a business or operational (tactical) problem creates an information system.

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 executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency, which 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. [Reference 40 USC Subtitle III (Clinger-Cohen Act of 1996)].

Information technology architecture
An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency's strategic and information resources management goals (see 40 USC Subtitle III: Information Technology Management §11315 Agency Chief Information Officer).

Information technology equipment
Any equipment, interconnected systems or subsystems of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. IT equipment includes, but is not limited to, CG Standard Workstation desktops or laptops, PEDs, Smartphones, related peripheral equipment, and software.

Information technology investments
The development and sustainment resources needed in support of IT or IT-related initiatives. These resources include, but are not limited to: research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund.

Information technology portfolio
A grouping of IT capabilities, systems, services, systems support services (for example, IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal.

Information technology standards
An established norm to be used in an information system or across the enterprise. It is a formal document that establishes uniform engineering methods, technical criteria, and processes and practices. An IT standard falls under the jurisdiction of a standards body. IT standards developed by DOD should have traceability to a standards body. An IT standard is proposed by a DOD or IC organization with a vested interest in that standard or technology (for example agencies, services, acquisition programs of record, capability portfolio managers, communities of interest, and so forth). It is a formal document that establishes uniform engineering methods, technical criteria, procedures and practices associated with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of information.

Infrastructure
The shared computers, ancillary equipment, software, firmware, and similar procedures; and services, people, business processes, facilities (such as building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format (including audio, video, imagery, or data) whether supporting IT or national security systems as defined in the CCA.

Installation
Geographic area subject to the control of the installation commander, including Government-owned housing or supported activities outside the perimeter of the military installation that depend on the installation for support.

Installation Services Node
An Installation Service Node (ISN) provides the minimum basic network and communications functionality to the installation in the event it becomes disconnected from the enterprise. The ISN's limited store and compute capabilities are in direct support of that basic functionality. Potential services may include read only Active Directory (AD) servers, print servers, Domain Name System servers, Assured Compliance Assessment Solution servers, Host Based Security System , Installation/Base/Building Access Systems, and Traffic Control Systems. In addition, ISNs may also host Unified Capabilities (UC) that must remain on the Installation to enable emergency services (Emergency Notification Systems, E911 Systems).

Integrated information technology
Modular IT that can operate independently or on multiple platforms.

Integration
The process of making or completing, by adding or fitting together into an agreed framework (architecture), the information requirements, data, applications, hardware, and systems software required to support the Army in peace, transition, and conflict.

Integrity (of information)
Assurance of protection from unauthorized change.

Interface
A boundary or point common to two or more similar or dissimilar telecommunications systems, subsystems, or other entities where necessary information flows take place.

Interim certificate to operate –
A temporary authorization to proceed to connection without completing full interoperability certification. Issued by the ISG to PMs who have an urgent need to operate IT, have not completed interoperability certification, but are making satisfactory progress towards that goal (as determined by the ISG).

Internal use software (IUS)
Software that includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program. Most often, software is an integral part of an overall system(s) having interrelationships between software, hardware, personnel, procedures, controls, and data.

Internet
An electronic communications network that connects computer networks and organizational computer facilities around the world.

Internet protocol version 4 interoperable
An IPv6-capable system, or product capable of receiving, transmitting, and processing IPv4 packets.

Internet protocol version 6–capable
A system or product meeting the minimal set of DISR-mandated requirements (appropriate to the product class) necessary to be interoperable with other IPv6-capable products in DOD deployments.

Internet protocol version 6–enabled
IPv6-capable systems or products with the IPv6 functionality turned on–implying that IPv6 packets can be properly processed by that system, product, or component.

Internet service provider
An organization that provides other organizations or individuals with access to, or presence on, the Internet. Most Internet service providers also provide extra services including help with the design, creation, and administration of websites; training; and the administration of Intranets.

Interoperability
The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.

Interoperability steering group
Forum to coordinate policy and provide oversight and direction across DOD organizations in ensuring the interoperability of IT and NSS

Intranet
A computer network that functions like the Internet. Uses web browser software to access and process the information that employees need, and is available on computers within the organization or enterprise. A firewall is usually used to block access from outside the Intranet. Intranets are private websites.

Joint information environment
A secure environment composed of shared IT infrastructure, enterprise services, and a single security architecture designed to achieve full spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. The JIE is operated and managed in accordance with the Unified Command Plan, using enforceable standards and specifications, and common tactics, techniques, and procedures.

Joint interoperability test command
DOD's Joint Interoperability Certifier and only non-Service Operational Test Agency for Information Technology (IT)/NSS. JITC provides risk-based Test Evaluation & Certification services, tools, and environments to ensure Joint Warfighting IT capabilities are interoperable and support mission needs

Life cycle
The total phases that an item progresses through from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

Management decision evaluation package
A nine-year package of dollars and manpower to support a given program or function. The management decision evaluation package justifies the resource expenditure.

Measure
One of several measurable values that contribute to the understanding and quantification of a key performance indicator.

Message (telecommunications)
Recorded 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; information about data; or descriptive information about an organization’s data, data activities, systems, and holdings.

Metrics
The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.

Mission
A group of tasks and their respective purposes, which are assigned to military organizations, units, or individuals for execution.

Mission area
A defined area of responsibility 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 the allocation of resources).

Morale, welfare, and recreation programs
Military MWR programs (exclusive of private organizations as defined in DODI 1000.15) available on DOD installations or on property controlled (by lease or other means) by DOD or furnished by a DOD contractor, which provide for the mission sustainment and community support of authorized DOD personnel.

Multimedia
The synchronized use of two or more types of media, regardless of the delivery medium.

National security system
Any telecommunications or information system operated by the United States Government. The function, operation, or use of which involves: 1) intelligence activities; 2) cryptologic activities related to national security; 3) C2 of military forces; 4) equipment that is an integral part of a weapon or weapons system; or 5) matters critical to the direct fulfillment of military or intelligence missions (see the CCA).

Negotiation
The communication (by any means) of a position or an offer on behalf of the United States, DOD, or any office or organizational element thereof; to an agent or representative of a foreign Government (including an agency, instrumentality, or political subdivision thereof); or of an international organization in such detail that the acceptance in substance of such position or offer would result in an international agreement. The term also includes any communication conditional on subsequent approval by higher authority, but excludes mere preliminary, exploratory, or informal discussions or routine meetings conducted with the understanding that the views communicated do not and will not bind any side. (Normally, the approval authority will authorize the requesting command to initiate and conduct the negotiation.)

Net–ready key performance parameters
NR-KPPs identify operational, net-centric requirements in terms of threshold and objective values for measures of effectiveness and measures of performance. The NR–KPP covers all communication, computing, and EM spectrum requirements involving information elements among producer, sender, receiver, and consumer. Information elements include the information, product, and service exchanges. These exchanges enable successful completion of the warfighter mission or joint business processes.

Network operations
The DOD-wide operational, organizational, and technical capabilities for operating and defending the DODIN.
NetOps is the discipline within signal operations focused on planning, engineering, installing, operating, maintaining, controlling, and defending the network in support of both the generating force and the operational Army. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with DODIN–A situational awareness to make informed C2 decisions. DODIN–A situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical).

Network security
Any activity designed to protect the usability and integrity of the network and associated data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on the network.

Non–appropriated fund instrumentalities
Every NAFI is legally constituted as an "instrumentality of the United States." Funds in NAFI accounts are Government funds, and NAF property, including buildings, is Government property. However, NAF are separate from APF of the U.S. Treasury. They are not commingled with APF and are managed separately, even when supporting a common program or activity.

Non–appropriated fund(s)
Cash and other assets received from sources other than monies appropriated by the U.S. Congress (NAF must be resources of an approved NAFI). NAF are U.S. Government funds, but they are separate and apart from funds that are recorded in the books of the U.S. Treasury. NAF are used for the collective benefit of the authorized patrons who generate them.

Nonpublic data and information
Data and information that is personally identifiable, subject to the Privacy Act, classified according to the National Security Act, subject to a FOIA exemption, or sensitive.

Objectives
Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.

Offensive Cyberspace Operations
(Joint) Offensive cyberspace operations intended to project power by the application of force in or through cyberspace (see JP 1–02).

Operational architecture
Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.

Operational requirement
A formally established, validated, and justified need for the allocation of resources to achieve a capability to accomplish approved military objectives, missions, or tasks.

Operational viewpoint (architecture)
Department of Defense Architecture Framework (DODAF)-described Models in the Operational Viewpoint describe the tasks and activities, operational elements, and resource flow exchanges required to conduct operations. A pure operational model is materiel independent. However, operations and their relationships may be influenced by new technologies, such as collaboration technology, where process improvements are in practice before policy can reflect the new procedures. There may be some cases, as well, in which it is necessary to document the way activities are performed, given the restrictions of current systems, to examine ways in which new systems could facilitate streamlining the activities. In such cases, operational models may have materiel constraints and requirements that need to be addressed. For this reason, it may be necessary to include some high-level system architectural data to augment information onto the operational models.

Organizational messaging
Correspondence used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies official position, or issues official guidance is considered an organizational message.

Performance management
The use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet goals, and report on the success in meeting goals.

Performance measure
A quantitative or qualitative characterization of performance.

Performance measurement
The process of assessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of outputs (how well they are delivered to clients and the extent they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives).

Persistent cookies
Cookies that can be used to track users over time and across different websites to collect personal information.

Personally identifiable information
Information that can be used to distinguish or trace an individual's identity (for example, their name, social security number, and biometric records), or when combined with other personal or identifying information that is linked or linkable to a specific individual (for example, date and place of birth, mother's maiden name).

Planning, programming, budgeting, and execution process
The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Platform
A weapon system, system-of-systems, or support system designated by a DOD component as the basis for analyzing core capability requirements.

Platform information technology
Refers to computer resources, both hardware and software, which are physically a part of, dedicated to, or essential in real time to the mission performance of special-purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility-distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

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 in not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

Platform information technology
Information technology, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems.

Portfolio management
The management of selected groupings of IT investments using integrated strategic planning, integrated architectures, performance measures, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with PfM are binning, criteria development, analysis, selection, control, and evaluation.

Printing
The processes of composition, platemaking, presswork, and binding (including micropublishing) for the production of publications.

Privacy impact assessment
An analysis of how personal information is handled to: (a) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (b) determine the risks and effects of collecting, maintaining and disseminating personal information in an information system; and (c) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA process provides a way to ensure compliance with applicable laws and regulations governing privacy.

Process
A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place, which also has a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process owners
HQDA functional proponents, ACOMs, and others who have responsibility for any mission-related or administrative work process.

Procurement and contracting
Purchasing, renting, leasing, or otherwise obtaining supplies or services from non-Federal sources. Includes description (but not determination) of supplies and services required, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration. Does not include making grants or cooperative agreements.

Proponent
An Army organization or staff that has been assigned primary responsibility for materiel or subject matter in its area of interest.

Public
The people or a citizen of the United States not affiliated with the Government.

Public key infrastructure
An enterprise-wide service (for example, 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. Includes the generation, production, distribution, control, and accounting of public key certificates. PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key, and are issued by a reliable certification authority.

Public website on the internet
Army website with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet or anyone who can access a website through a browser.

Publications
Items of information printed or reproduced, whether mechanically or electronically, for distribution or dissemination to a predetermined audience. The items are generally directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by and for the Army.

Publishing
Actions involved in issuing publications. Involves creating, preparing, coordinating, approving, processing, printing, and distributing or disseminating publications.

Record
All books, papers, maps, photographs, machine readable items (such as, disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical-recording media, film slides, transparencies, or other documentary materials regardless of physical form or characteristics) made or received by any entity of the DA as

evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data.

Records centers
Locations established in CONUS to receive and maintain records with long-term or permanent value, pending their ultimate destruction or accession into the National Archives.

Records management
The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with information creation, information maintenance and use, and information disposition in order to achieve adequate and proper documentation of the policies, transactions, and effective and economical management of DA operations.

Records management program
A program that includes elements concerned with the life cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information Act and Privacy Act.

Satellite communications
DOD use of military-owned and military-operated SATCOM space systems that use Government frequency bands, and commercial SATCOM systems provided by commercial entities using commercial frequency bands. SATCOM is further defined to include DOD's use of other allied and civilian SATCOM resources as appropriate (see CJCSI 6250.01).

Sensitive compartmented information
Classified national intelligence concerned with or derived from intelligence sources, methods, or analytical processes, which are required to be protected within formal access-control systems established and overseen by the Director of National Intelligence.

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.

Servomechanism
An electronic control system in which a hydraulic, pneumatic, or other type of controlling mechanism is actuated and controlled by a low-energy signal.

Signal operations
The employment and ordered arrangement of Signal forces in a supporting role to provide DODIN–A across the range of military operations. Core competencies of Signal Operations include network transport and information services, spectrum management operations, visual information operations, DODIN–A operations, network management and enterprise system management, cybersecurity, and information dissemination management

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.

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, and circuit diagrams); usually contrasted with hardware.

Spam
Widely disseminated "junk" email.

Special purpose processing nodes
A special purpose processing node (SPPN) is a fixed data center supporting special-purpose functions that cannot (technically or economically) be supported by CDCs or CEDCs due to its association with non-severable infrastructure or equipment tethered to non-IT hardware (for example sensors, medical, modeling & simulation, test ranges, classrooms, RDT&E, and so forth). A "litmus" test for a data center to be categorized as an SPPN is for it to be truly non-severable from infrastructure or facility. An SPPN will not provide general-purpose computing or provide compute/storage capabilities to any applications or systems beyond those needed to support the non-severable equipment or facility requirements for the designated mission type.

Spectrum Management Operations
The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operational environment during all phases of military operations.

Standard
Within the context of the AEA, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also establish requirements for the selection, application, and design criteria for materiel.

Standards view (architecture)
The standards view is the set of rules governing the arrangement, interaction, and interdependence of parts or elements of the architecture description.

Strategic management plan
The DOD Strategic Management Plan sets forth the DOD strategy for delivering effective business operations to support and enable the warfighter by aligning and improving business functions across the Department's business functions.

Strategic planning
A continuous and systematic process whereby guiding members of an organization make decisions about the organization's future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured.

Subscriber
Any person, group, organization (including concessionaire), or appropriated or NAF activity that procures services made available pursuant to the terms of the franchise agreement.

Support agreement
An agreement to provide recurring common-use IT services to another DOD or non-DOD Federal activity.

Synchronization
Coordinating and aligning the development of the AEA in both timing and direction for mutual reinforcement and support. See data synchronization.

System
An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JP 1–02). Within the context of the AEA, systems are people, machines, and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; or produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry, the terms "application" and "system" are used synonymously–a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (for example, the application of IT).

System owner
The system proponent and the agency or organization that establishes the need for the IT system. Develops requirements, provides funding, designates who will manage data entry, and aligns requirements with APMS standards.

System view (architecture)
A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. The system view defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms, and specifies system and component-performance parameters. It shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems.

Systems architect
Responsible for the integration and oversight of architecture for IT and NSS from a systems perspective.

Systems architecture
Descriptions, including graphics, for systems and interconnections providing for or supporting functions.

Task
A discrete event or action that is unspecific to a single unit, weapon system, or individual; and that enables a mission or function to be accomplished by individuals or organizations.

Technical architecture
The technical architecture provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed.

Telecommunications
Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

Telework
Working at an alternative site via electronic means.

TEMPEST
An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment. These investigations are conducted in support of emanations and emissions security.

The Army plan
This plan is a 16-year strategic planning horizon that includes the 6-year span of the program, plus an additional 10 years. The Army Plan presents comprehensive and cohesive strategic, midterm planning and programming guidance that addresses the Army's enduring core competencies over this time period.

Thin client
The use of client-server architecture network that depend primarily upon the central server for processing activities that focus on conveying input and output between the user and the remote server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server. Many thin client devices run only web browsers or remote desktop software, which means that all significant processing occurs on the server.

Third–party cookies
Cookies placed on a user's hard drive by Internet advertising networks. The most common third-party cookies are placed by various companies that oversee the banner ads that appear on many websites.

Tiered data center
Tiered data centers are defined as those that utilize each of the following: 1) a separate physical space for IT infrastructure; 2) an uninterruptible power supply; 3) a dedicated cooling system or zone; and 4) a backup power generator for prolonged power outages. All other data centers will be considered non-tiered data centers according to OMB.

Uniform resource locator
A web address that a person uses to direct a browser program to a particular Internet resource (for example, a file, a web page, an application, and so on). All web addresses have a URL.

Unique identification
A system of establishing globally unique identifiers within DOD, and serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships.

Unique identifier
A character string, number, or sequence of bits assigned to a discrete entity or its associated attribute, and serves to uniquely distinguish it from other like and unlike entities. Each unique identifier has only one occurrence within its defined scope of use.

User
Any person, organization, or unit that uses the services of an information processing system. Specifically, it is any table of organization and equipment or TDA command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, or otherwise applying DOTMLPF–P products for the accomplishment of a designated mission.

User fee
The periodic service charge paid by a subscriber to the franchisee for service.

Video
Pertaining to bandwidth and spectrum position of the signal that results from television scanning and is used to produce an electronic image.

Video–teleconferencing
Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video. Includes full-motion video, compressed video, and sometimes freeze (still) frame video.

Vision
A description of the future; the most abstract description of the desired end-state of an organization or activity at an unspecified point in the future.

Visual information
Information in the form of visual or pictorial representations of person(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog, digital, and high-definition video recordings; hand-generated or computer-generated art and animations that depict real or imaginary person(s) or thing(s); and related captions, overlays, and intellectual control data.

Visual information activity
An organizational element or a function within an organization in which one or more individuals are classified as VI specialists, or whose principal responsibility is to provide VI services. VI activities include those that expose and process original photography; record, distribute, and broadcast electronically (video and audio); reproduce or acquire VI products; provide VI services; distribute or preserve VI products; prepare graphic artwork; fabricate VI aids, models, and displays; and provide presentation services or manage any of these activities.

Visual information documentation
Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, and are usually not controlled by the recording crew.

Visual information equipment
Items capable of continuous or repetitive use by an individual or organization to record, produce, reproduce, process, broadcast, edit, distribute, exhibit, and store visual information. Items otherwise identified as VI equipment, which are an integral part of a non-VI system or device (existing or under development), will be managed as a part of that non-VI system or device.

Visual information functions
The individual VI processes, such as production, documentation, reproduction, distribution, records preservation, presentation services, VI aids, fabrication of model and displays, and related technical services.

Visual information library
A VI activity that loans, issues, and maintains an inventory of motion media, imagery, or equipment.

Visual information management office
Staff office at command, FOA, or other management level established to prescribe and require compliance with VI policies and procedures, and to review operations.

Visual information materials
A general term that refers collectively to all of the various VI still and motion films, tapes, discs, or graphic arts. Includes the original, intermediate, and master copies, and any other recorded imagery.

Visual information production
The combination of motion media with sound in a self-contained, complete presentation, developed according to a plan or script for purpose of conveying information to, or communicating with, an audience. A production is also the end item of the production process. Used collectively, VI production refers to the functions of procurement, production, or adoption from all sources, such as in-house or contract production, off-the-shelf purchase, or adoption from another Federal agency.

Visual information products
VI media elements such as motion picture and still photography (photographs, transparencies, slides, film strips); audio and video recordings (tape or disc); graphic arts (including computer-generated products); models; and exhibits.

Visual information records
VI materials, regardless of format, and related captions and intellectual control data.

Visual information resources
The personnel, facilities, equipment, products, budgets, and supplies that comprise DOD visual information support.

Visual information services
Those actions that 1) result in obtaining a visual information product; 2) support the preparation of a completed VI production such as photographing, processing, duplicating, sound and video recording, instrumentation recording, and film-to-video transferring, editing, scripting, designing, and preparing graphic arts; 3) support existing VI products such as

distribution and records center operations; and 4) use existing VI products, equipment, maintenance, and activities to support other functions such as projection services, operation of conference facilities, or other presentation systems.

Warfighter
A common Soldier, sailor, airman, or marine by trade, from all Services who joins in a coordinated operation to meet a common enemy, a common challenge, or a common goal.

Warfighting requirements
Requirements for ACAT I–IV systems or IT capabilities in direct use by or support of the Army warfighter in training for and conducting operational missions (tactical or other), or for connecting the warfighter to the sustaining base.

Weapon System
A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

Web portals
Websites that serve as starting points to other destinations or activities on the web. Initially thought of as "home base" web pages, portals attempt to provide all of a user's Internet needs in one location. Portals commonly provide services such as email, collaboration centers, online chat forums, searching, content, newsfeeds, and other.

Website
A location on the Internet; specifically it refers to the point of presence location in which it resides. All websites are referenced using a special addressing scheme called a URL. A website can mean a single HTML file or hundreds of files placed on the Internet by an enterprise.

Worldwide web
A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses; also referred to as the "web."

Section III

Special Abbreviations and Terms

This section contains no entries.