Information Management

Telecommunications and Unified Capabilities

Headquarters Department of the Army Washington, DC 25 March 2013

UNCLASSIFIED

SUMMARY

AR 25-13 Telecommunications and Unified Capabilities

This new Department of the Army regulation, dated 25 March 2013--

- Assigns responsibilities to ensure the effective, efficient, and economical use of existing telecommunications equipment and services, in addition to unified capabilities (para 1-4).
- Includes authorized use and prohibitions for unified capabilities, including but not limited to telecommunications (strategic networks, base communications, long-haul, and deployable communications) and collaboration tools (chap 2).
- o Provides policy on satellite communication systems (chap 4).
- o Provides Army policy on commercial Internet service providers and global information grid waivers (chap 5).
- o Establishes policies for the management of telecommunications and unified capabilities (throughout).

Headquarters Department of the Army Washington, DC 25 March 2013

Effective 25 April 2013

Information Management

Telecommunications and Unified Capabilities

By Order of the Secretary of the Army:

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

Official:

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

History. This publication is a new Department of the Army regulation.

Summary. This regulation establishes policies and assigns responsibilities for the management of unified capabilities. 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 implements the provisions of Sections 2223 and 3014, Title 10, United States Code; 40 United States Code, Subtitle III, Clinger-Cohen Act; 44 United States Code, Chapters 35 and 36; DODD 8000.01; DODI 8100.04; DODD 5105.77; DODD 5105.83; and other related Federal statutes and directives. The full scope of Chief Information Officer responsibilities and management processes for telecommunications and unified capabilities are delineated throughout this regulation.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Portions of this regulation prescribe specific prohibitions that are punitive, and violations of these provisions may subject offenders to non-judicial or judicial action under the Uniform Code of Military Justice. 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 and identifies key internal controls that must be evaluated (see appendix C).

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 the Office of the Chief Information Officer/G-6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107 (CIOG6CIOPolicy@conus.army.mil).

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

Contents (Listed by paragraph and page number)

Chapter 1 Introduction, page 1 Purpose • 1–1, page 1 References • 1–2, page 1 Explanation of abbreviations and terms • 1–3, page 1 Responsibilities • 1–4, page 1 Architectures • 1–5, page 4

Contents—Continued

Chapter 2

Utilization Policies, page 4

Official uses of telecommunications and computing systems • 2–1, *page 4* Unauthorized use and prohibitions of telecommunications and computing systems • 2–2, *page 4* Communication monitoring and recording • 2–3, *page 5* Leasing of Government-owned telecommunications assets • 2–4, *page 5* Information technology support for telework • 2–5, *page 6* Military construction communication systems policy • 2–6, *page 6*

Chapter 3

Telecommunications Systems and Services, page 6

Applicability and policy • 3–1, page 6 Server moratorium • 3–2, page 6 Time-division multiplex equipment • 3–3, page 6 Asynchronous transport mode equipment • 3–4, page 7 Telephone systems • 3–5, page 7 Video services • 3–6, page 9 Commercial television service • 3–7, page 10 Multifunction mobile devices • 3–8, page 11 Wireless priority service and wireline Government Emergency Telecommunications Service • 3–9, page 12 Non-tactical radio systems • 3–10, page 12

Chapter 4

Satellite Communication Systems and Position Navigation and Timing, page 13

General • 4–1, page 13
Commercial satellite communication annual usage report • 4–2, page 13
Satellite communication requirements • 4–3, page 14
Use of wideband military satellite communications • 4–4, page 14
Satellite communication standardization • 4–5, page 14
Network Command operations of military satellite communication systems • 4–6, page 14
Army component command to United States Strategic Command • 4–7, page 14
International Maritime Satellite and Iridium • 4–8, page 15
Position navigation and timing global positioning system, precise positioning service, and standard positioning services • 4–9, page 15

Chapter 5

Long-haul and Deployable Telecommunications, page 15

General • 5–1, *page 15* Non-Department of Defense connections to the Defense Information System Network • 5–2, *page 17* Global information grid waivers • 5–3, *page 17* Military telecommunications agreements • 5–4, *page 18*

Chapter 6

Unified Capabilities, page 19 Introduction • 6–1, page 19 Policy • 6–2, page 19 Unified capabilities approved product list • 6–3, page 19 Voice services • 6–4, page 19 Video services • 6–5, page 21 Element management system • 6–6, page 21 Collaboration capabilities • 6–7, page 21 Installation information infrastructure • 6–8, page 22

Appendixes

A. References, page 23

B. Telecommunications Services Authorized for Specific Activities, page 26

Contents—Continued

C. Internal Control Evaluation Checklist, page 29

Glossary

Chapter 1 Introduction

1-1. Purpose

This regulation establishes Department of the Army (DA) policies and assigns responsibilities for the management of unified capabilities (UC). It implements the provisions of Sections 2223 and 3014, Title 10, United States Code (USC) (10 USC 2223 and 10 USC 3014); 40 USC Subtitle III, Clinger-Cohen Act (CCA); 44 USC 35 and 44 USC 36; DODD 5105.77; DODD 5105.83; DODD 8000.01; DODI 8100.04; and other related Federal statutes and directives. For Army tenant units residing on non-Army hosted installations or Joint bases, some local processes may vary from this regulation. Guidance and direction from this regulation will be used as the basis for input to local or Joint memorandums of agreement.

1-2. References

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

1-3. Explanation of abbreviations and terms

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

1-4. Responsibilities

a. Chief Information Officer/G-6. The CIO/G-6 will serve as senior Army authority for telecommunications and UC, to include the following:

(1) Joint Staff-controlled mobile and transportable telecommunications assets.

- (2) The Spectrum Certification Program.
- (3) Participant and voting member of the Military Communications-Electronics Board.
- (4) Participant and voting member of the Department of Defense (DOD) Unified Capabilities Steering Group.
- (5) Participant in the Department of Defense Unified Capabilities Industry Advisory Council.
- (6) Participant in the Defense Information Systems Network (DISN) Customer Forum.
- (7) Serve as Army lead for the Joint Transformation Communications Program.
- (8) Provide subject matter expertise in negotiations concerning recognized requirements.

(9) Integrate efforts to provide policy, oversight, and guidance to enable dominance in the Army information environment.

b. Army Cyber Command. Army Cyber Command will-

(1) Prescribe all infrastructure management activities, policies, processes, procedures, and protocols for the management of infrastructure assets such as Army networks, UC, telecommunications, installation facilities, data storage, information technology (IT) services continuity, and mid-range and mainframe computing.

(2) Prescribe security of telecommunications and UC for assigned fixed-station communications and Army contractor facilities.

(3) Provide for the protection of assigned fixed-station communications facilities, and the security of Army contractor telecommunications and UC.

(4) Execute Army leases of communications and UC services, and ensure that such services conform to DOD and National Communications Systems guidance.

(5) Formulate, manage, and approve Army military communications and UC exchange agreements between the United States, regional defense organizations, or friendly foreign nations. Coordinate the procedural details of the agreements with the commander of the theater of operations concerned.

(6) Support North Atlantic Treaty Organization (NATO) communication requirements for projects involving interfaces between non-DISN NATO and NATO member telecommunications systems and will—

(a) Provide subject-matter expertise in negotiations concerning recognized requirements.

(b) Manage system-to-system interfaces, unless otherwise directed by the Joint Staff.

(c) Fund validated projects that support U.S., NATO, and NATO-member telecommunications objectives and approved planned interfaces between non-DISN NATO, and NATO-member systems consistent with budget appropriations and the Secretary of Defense's consolidated guidance.

(d) Operate, maintain, and defend equipment, facilities, systems, and services that are required to support U.S., NATO, and NATO-member communications objectives as assigned.

(e) Assist the Defense Information Systems Agency (DISA) in representing U.S. interests within NATO communications forums.

(7) Submit validated or approved UC requirements to the DISA for coordination and implementation into the unified capabilities requirements (UCR).

c. Chief, Army Reserve. The CAR will-

(1) Serve as the designated lead agent for the Army Reserve Network II (ARNet II), including:

(a) Planning and programming resources to support ARNet II capabilities, as required by the Army CIO/G–6; Commanding General (CG), Army Cyber Command; and CG, Network Enterprise Technology Command (NETCOM).

(b) Directing all infrastructure management activities, policies, procedures, and protocols for management of the ARNet II.

(c) Exercising technical and configuration management authority for ARNet II, United States Army Reserve (USAR) specialized systems, and functional processing centers.

(d) Formulating, managing supporting and approval of written agreements, where applicable.

(2) Designate a single network enterprise center responsible for support all facilities and infrastructure.

d. Chief, National Guard Bureau. The CNGB serves as the channel of communications on all matters pertaining to the National Guard between the DA and the States and will—

(1) Collaborate with the National Guard Bureau (NGB), Army CIO/G–6, Army Cyber Command/2nd U.S. Army, NETCOM, and the Joint Forces Headquarters-State (JFHQs-States) on issues related to the Army National Guard's (ARNG) status as a component of the Army in the management of UC capabilities and services.

(2) Designate the Director, ARNG as the lead agent for the Army National Guard Network (GuardNet).

(3) Appoint the Director, ARNG as the designated approval authority (DAA) for GuardNet.

(4) Oversee organizations that operate and maintain GuardNet, a separate network providing Land Warrior Network (LandWarNet) services to States, territories, and the District of Columbia, and that also connects the ARNG to the DISA global information grid (GIG). This includes, but is not limited to—

(*a*) Planning and programming UC resources to support NGB and JFHQ–States UC requirements, as required by the CNGB; Army CIO/G–6; CG, Army Cyber Command; CG, NETCOM; Adjutants General of the States and Territories; and the Commanding General of the District of Columbia.

(b) Exercising technical authority and configuration management authority for GuardNet, NGB specialized systems, and functional processing centers; and providing guidelines and direction for GuardNet IT configuration management.

(c) Prescribing all infrastructure management activities, policies, processes, procedures, and protocols for the management of the following: networks, telecommunications, UC facilities, data storage, IT services continuity, and midrange and mainframe computing operations within the GuardNet.

(d) Providing technical and administrative guidance, direction, and resources to the JFHQs-States that assume direct responsibility for the communications and UC services operating within their State boundaries.

(e) Executing ARNG leases of communications and UC capabilities and services to ensure that such services conform to NGB, Army CIO/G–6, Army Cyber Command, and NETCOM guidance in collaboration with the JFHQs-States, where applicable.

(f) Formulating, managing, supporting, and approving ARNG military communications and UC exchange agreements between the U.S. Army, other Joint Services, JFHQs-States, State Government, and first-response agencies in collaboration with the JFHQs-States where applicable.

(g) Providing subject-matter expertise in negotiations and collaborations with the NGB, Army CIO/G-6, Army Cyber Command, NETCOM, and JFHQs-States concerning recognized requirements.

(h) Managing GuardNet-specific, system-to-system interfaces between the States and the DA in collaboration with the JFHQs-States where applicable.

(*i*) Identifying and validating unique, critical communications requirements considered vital to the NGB and ARNG in collaboration with the JFHQs-States where applicable; and submitting these requirements to the Army CIO/G–6, Army Cyber Command, and NETCOM.

(*j*) Collaborating with the JFHQs-States directorates of information management, which have Network Enterprise Center (NEC)-like responsibilities within their respective states as outlined in this regulation.

e. U.S. Army Network Enterprise Technology Command. The NETCOM will-

(1) Submit validated or approved UC requirements to DISA for coordination and implementation.

(2) Formulate Army military communications and UC exchange agreements between the U.S. and regional defense organizations or friendly foreign nations, and coordinate the procedural details of the agreements with the commander of the theater of operations concerned.

(3) Support NATO communication requirements for projects involving interfaces between non-DISN NATO and NATO-member telecommunications systems and will—

(a) Participate in negotiations concerning recognized requirements.

(b) Provide overall U.S. management of system-to-system interfaces, unless otherwise directed by the Joint Staff.

(c) Fund validated projects that support U.S., NATO, and NATO-member telecommunications objectives and approved planned interfaces between non-DISN NATO and NATO-member systems to the extent such projects are consistent with budget appropriations and the Secretary of Defense's consolidated guidance.

(4) Operate required equipment, facilities, and systems or services supporting U.S., NATO, and NATO-member communications objectives as assigned.

(5) Assist DISA in representing U.S. interests within NATO communications forums as appropriate.

(6) Identify and validate unique critical communications circuit requirements considered vital to the Army and submit them to the Joint Staff.

f. Assistant Secretary of the Army for Acquisition, Logistics and Technology. The ASA (ALT) will-

(1) Maintain an accurate telecommunications and UC inventory. This inventory will be continuously updated and maintained for asset visibility.

(2) Incorporate an engineering-based approach to determine current and future bandwidth requirements for circuits that connect installations to the GIG.

g. Commanders and activity heads of Army Commands, Army Service Component Commands, and Direct Reporting Units. Commanders and activity heads of ACOMs, ASCCs, and DRUs will—

(1) Establish procedures to ensure—

(a) All data, video, and voice-switching hardware and software are on the UC approved product list (APL) 25252532 found at https://aplits.disa.mil/processAPList.do; or available on the Computer Hardware, Enterprise Software and Solutions (CHESS) program catalog before procuring these items.

(b) Procurements of networked IT comply with Federal Acquisition Regulation (FAR) requirements for use of the U.S. Government version 6 (USGv6) profile and test program for the completeness and quality of Internet Protocol version 6 (IPv6) capabilities.

(c) Users of computers, Army telecommunications, and UC are familiar with the types and purposes of available communications, services, and systems.

(d) Information managers (or designated telephone control officers (TCOs)) review and validate monthly bills, which are certified by the users for toll-free service, multi-function mobile device, pager service, cellular phone service, calling card usage, long-distance commercial calls, and commercial lines.

(e) The review and revalidation of DOD physical inventory includes an analysis of leased and Government-owned long-haul telecommunications circuits, services, and equipment. NETCOM, in conjunction with the NECs, will review and revalidate all expired communications service authorizations (CSAs) regardless of user. Review and revalidation must include voice, video, data, and bandwidth utilization of internet protocol (IP) services (for example, non-secure Internet protocol router network (NIPRNET) and secure Internet protocol router network (SIPRNET), Voiceover Internet Protocol (VoIP), Voiceover Secure Internet Protocol (VoSIP) and Joint Worldwide Intelligence Communication System (JWICS)). DISA submits CSAs for validation, and the information is used to determine if the circuit is still required. Refer to Army Regulation (AR) 25–2 for applicable information assurance (IA) processes and governance.

(f) Organizational telecommunications and UC inventory are updated on an annual basis and verified accurate.

(2) Review long-haul, common-user transmission requirements and forward all requirements not needing combatant command, Joint Staff, or Office of the Secretary of Defense (OSD) approval to NETCOM for development of a technical solution, coordination, and implementation. In accordance with DISA's criteria, systems requirements must be identified far enough in advance to ensure a timely acquisition of network components to satisfy the operational date.

(3) Review and submit, as delegated by the supported combatant commander, requirements for service with the information prescribed in Defense Information Systems Agency Circular (DISAC) 310–130–1.

(4) Program, budget, fund, and provide support for assigned portions of the DISN through the planning, programming, budgeting, and execution process, including approved contractor and foreign Government systems.

(5) Provide sufficient local distribution capability to meet the combatant commanders' validated connectivity requirements. These systems must be capable of supporting the operational requirements of the Army as well as Joint Task Force contingencies.

(6) Ensure that information security, communications security, emissions security (formerly known as TEMPEST), physical security measures, and installation requirements conform to the Army and DISN security policy.

(7) Ensure that approved systems use DISN services to meet mission requirements, and ensure compliance with the Army and DISN policy and procedures.

(8) Coordinate with the theater commander and DISA before submitting long-range requirements for DISN access within a geographic region of responsibility of a theater command. Conflicting views among the requesting activity, DISA, and the concerned combatant commander will be forwarded to the Joint Staff for resolution.

(9) Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits in accordance with DISA's criteria and provide representatives, as required, to Joint-chaired or DISA-chaired working groups on related topics.

(10) Provide requisite site support for DISN equipment located on their respective posts, installations, or the equivalent. Site support requirements will be specified by DISA in appropriate procedural documentation and coordinated with the Services and defense agencies. Support required will include, but is not limited to, providing power, physical security, floor space, and on-site coordination for the DISN data networks points of presence located on their respective posts, installations, or equivalent.

(11) Manage DISN sub-networks when authorized by the Director, Joint Staff.

1-5. Architectures

Approved DOD and Army architecture documents will be used to establish architectural procedures, implementation plans, and requirements. Army architectures must be IA compliant, interoperable, defendable, and in line with the CIO/G–6 Strategic Goals and Guidance. Army architecture documents will be in line with the following documents: Unified Capabilities Requirements 2008; UC Master Plan; Army CIO/G–6 Strategy for "End State" Army Network Architecture–Tactical; Technical Criteria for the Installation Information Infrastructure Architecture; and applicable Security Technical Implementation Guides (STIGs).

Chapter 2 Utilization Policies

2-1. Official uses of telecommunications and computing systems

a. The use of DOD and other government telephone systems, electronic mail (email), and other systems and services (including the Internet) are limited to the conduct of official business or other authorized uses. Commanders and supervisors at all levels will make all users of government telecommunications and UC systems aware of permissible and unauthorized uses. Local policies and procedures will be promulgated, as necessary, to avoid disruptions to telecommunications systems. The Joint Ethics Regulation, Section 2–301, serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and disruptions to Army communications systems.

b. All communications users must be aware of security issues and provide their consent to being monitored for all lawful purposes, including restrictions on transmitting classified information over unsecured communications systems, prohibitions regarding release of access information such as passwords, and the need to encrypt transmissions containing unclassified sensitive information (see paragraph 2-3 for additional information on communications monitoring).

c. Army-funded IT and information management (IM) products, including intellectual property, will follow appropriate statutory, regulatory, and Cooperative Research and Development Agreements, and other policies consistent with national and departmental security objectives, including the Defense Federal Acquisition Regulations.

d. Official business calls, email, and text messages are defined as those necessary in the interest of the Government (for example, communications directly related to the conduct of DOD business or having an indirect impact on DOD's ability to conduct its business).

e. Official use includes health, morale, and welfare (HMW) communications by military members and DOD employees deployed on official DOD business to remote or isolated locations for extended periods of time. HMW calls will be made via the sensitive but unclassified (SBU) voice network (formerly the defense switched network (DSN)). When authorized by the theater combatant commander, the theater commander will institute local procedures to authorize HMW calls may be made only during non-peak, non-duty hours and will not exceed 15 minutes once per week. The commander may authorize calls that exceed this limit and frequency on a case-by-case exception basis (see paragraph 3–8 of this publication for guidance on acquiring and using cellular telephones).

f. Commanders will recover toll charges, as practical, for unauthorized personal telephone calls placed on official telephones by personnel within their organizations. Charges may also apply to misuse of Government communications through modems or other connections (see Department of the Army Pamphlet (DA Pam) 25-1-1).

g. Authorized use of communication systems includes brief communications made by DOD employees while they are traveling on Government business to notify Family members of transportation or schedule changes. Authorized use also includes personal communications from the DOD employee's usual workplace that are most reasonably made while at the workplace (such as, checking in with spouse or minor children; scheduling doctor, auto, or home repair appointments; brief Internet searches; and emailing directions to visiting relatives). Restrictions on communications are described at http://ciog6.army.mil/Policy/tabid/64/Default.aspx.

h. The Joint Travel Regulations provide guidance for telephone calls while at a temporary duty location.

i. Requests for leased commercial phone service are submitted by memorandum to the installation NEC. The memorandum must be reviewed by and have the original signature of the unit's TCO before submission. The user will submit requirements to the NEC at least 90 days (120 days for 1–800 service) in advance of the required service date (see DA Pam 25-1-1).

2-2. Unauthorized use and prohibitions of telecommunications and computing systems

a. Administrative, criminal, and adverse actions. Unauthorized use or abuse of DOD and Army telecommunications, UC, and computing systems (including telephone, email systems, DOD mobile devices, Web services, or other systems) may subject users to administrative, criminal, or other adverse action.

b. Use of Department of Defense-owned information technology. Connecting or installing non-DOD-issued IT hardware or software to the LandWarNet is prohibited. The organization's DAA must approve exceptions prior to

connecting to the network. This includes the use of employee-owned assets that connect to the network at the worksite. Use of employee-owned assets to process unclassified Army-related work off of the Government worksite must comply with the provisions of AR 25–2.

c. Prohibitions in communications usage. Prohibitions in the use of Army communications systems include the following:

(1) Use of communications systems, including Web services, which adversely reflect on DOD or the Army. Examples include uses involving sexually explicit email or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images; chain email messages; unofficial advertising, solicit-ing, or selling via email; or subversive and other uses that are incompatible with public service.

(2) Use of communications systems for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DOD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or laws. This may include, but is not limited to, violation of intellectual property and copyright laws, gambling, support of terrorist or subversive activities, and sexual or other forms of harassment.

(3) Political transmissions, to include transmissions that advocate the election of particular candidates for public office.

(4) Actions that result in the theft of resources or the abuse of computing facilities. Such prohibitions apply to email services and include, but are not limited to, the unauthorized entry, use, transfer, and tampering with the accounts and files of others; interference with the work of others; and interference with other computing facilities.

(5) Use of communications systems that could reasonably be expected to cause, directly or indirectly, the congestion, delay, or disruption of service to any computing facilities; a denial of service; or cause the unwarranted or unsolicited interference with others' use of communications. These types of interferences are described at http://ciog6. army.mil/Policy/tabid/64/Default.aspx.

(6) Use of communications systems to open, send, or forward items known or suspected of being malicious (such as spam, phishing, viruses, and Trojan horses).

2–3. Communication monitoring and recording

a. Army policy permits communications monitoring or recording, provided that the information to be acquired is necessary for the accomplishment of the Army mission. Lawful monitoring and recording of Army telecommunications and IT systems will be conducted in accordance with applicable directives (that is, AR 380–53 and AR 25–2 for Information System (IS) security monitoring; AR 190–53 for law enforcement purposes; AR 380–10 for electronic surveillance, and Department of Defense Instruction (DODI) 8560.01 for communications security (COMSEC)). Monitoring includes, but is not limited to, active attacks by authorized entities to test or verify the security of the system.

b. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information placed on or sent over DOD computer systems, may be monitored. Email, personal user files and directories, and any use of the Internet or records created by Internet use are subject to monitoring, inspection, and audit by command or agency management or its representatives at any time, with or without notice. Use of the DOD computer system indicates that the user consents to monitoring and understands that the command or agency has a right to inspect and audit all information, including email communications and records created by Internet use.

2-4. Leasing of Government-owned telecommunications assets

a. If requested, Government-owned, outside plant telephone facilities, inside plant telephone facilities, or antenna space may be leased to commercial telephone or radio companies in accordance with the provisions of this regulation, AR 700–131, and applicable installation memorandum of understanding. Outside plant facilities, inside plant facilities, and antennas are classified as IT equipment and accounted for as such. Outside plant facilities include installed or inplace telephone cable (copper and fiber optic), and their associated connecting terminals, telephone poles, manholes, and duct bank systems. Inside plant facilities include installed or in-place telephone frames, switches, electronic equipment, multiplexes, and fiber optic electronic equipment.

b. The leasing of plant facilities to vendors is permitted and encouraged.

(1) Leasing of telecommunications facility assets requires a formal lease agreement.

(2) The NEC is required to maintain a current inventory of cable plant facilities leased to vendors.

c. Leasing activities outside the continental United States (OCONUS) will follow this practice when negotiating new, revised, or existing services or facility leases; and when negotiating new or renegotiating existing status of forces, base rights, or other intergovernmental agreements, unless notified that the Secretary of State has determined such action inconsistent with foreign policy objectives of the United States.

d. Compensation paid by telephone companies for the lease of any Government-owned appropriated funds (APF) facilities (for example, cable pair, equipment, manholes, and antenna space) will be in the form of a credit toward the existing monthly bill, when possible (also referred to as "payment-in-kind"). If a credit to the existing monthly bill is

not possible, a check can be accepted. In accordance with 10 USC 2667, checks will be made payable to the U.S. Treasury under receipt account 97R5189, Lease of DOD Real Property for Army, to be redistributed to the leasing organization via Department of the Army. Terms of the reciprocal lease agreement will provide that the Government may, according to its needs, reacquire any leased asset.

(1) Nonappropriated fund revenue. The revenue from the lease of nonappropriated fund (NAF) telecommunications assets will be deposited into the NAF activity's fund.

(2) *Shared usage*. When leasing telecommunications services, the leasing activity will make every effort to lease in the name of the U.S. Government to permit the shared use of communications services, facilities, or installations among U.S. Government departments and agencies.

2–5. Information technology support for telework

The DOD telework policy can be found in DODI 1035.01.

2–6. Military construction communication systems policy

Military construction communication systems policy is located in AR 25-1.

Chapter 3 Telecommunications Systems and Services

3–1. Applicability and policy

a. Telecommunications provide the ability to gather and disseminate information through the transmission, emission, and reception of information of any nature by audio, visual, electro-optical, or electromagnetic systems. This section pertains to existing telecommunications systems and services, to include data networks, mobile devices, telephones (including cellular), pagers, radios, satellites, fax machines, video teleconferencing, commercial television services, and others that will remain in use until transitioned to an IP solution.

b. Telecommunications services authorized for specific installation activities are identified in appendix B of this publication.

3–2. Server moratorium

a. A moratorium exists on IT spending for all servers, including the construction, renovation, or leasing of a data center or server room, and on the procurement of the following IT equipment: servers, racks, storage area networks, matrix switches, optical storage systems, tape drives and storage devices, high-speed printers, and mainframe and mini computers. Therefore, specified IT equipment will not be procured and hosting facilities will not be constructed, renovated, or leased without a written waiver granted in advance by the CIO/G–6 consistent with the Army Data Center Consolidation Plan Execution Order. A link to the execution order is on the Army Data Center Consolidation Program page at Army Knowledge Online (AKO) (https://www.us.army.mil/suite/page/643748/).

b. Contracting officers will not award a contract or procurement action related to the listed purchases or actions without an approved waiver. These requirements will be included in AR 25–1 and will be subject to audit by the Army Audit Agency.

c. Any command that has an urgent requirement to construct or renovate an Army data center must submit a Webbased waiver request to the CIO/G-6, SAIS-PR at https://adminapps.hqda.pentagon.mil/. For these specific waivers, the subject line must state "FYXX IT Moratorium – Servers," "FYXX IT Moratorium – IT Equipment," or "FYXX IT Moratorium – Construction/Renovation," where the "XX" is the current fiscal year (FY). The request will include—

(1) A detailed justification.

- (2) An impact statement that describes the results of not receiving an approved waiver.
- (3) A bill of materials.

(4) The location where the equipment will be installed, or where the construction or renovation will take place.

(5) An approved requirements document.

(6) A general officer or senior executive service member endorsement.

d. For server-purchase waivers, the requirements document will include information about the utilization of the existing server (including peak and average memory utilization and storage utilization percentages).

3-3. Time-division multiplex equipment

a. Further investment in voice-switching (for example, time-division multiplex (TDM)) equipment will be terminated as soon as possible. Current TDM systems will begin reaching the end of their supportable life beginning in 2015.

b. Commands that have an urgent requirement to purchase (or have already purchased) TDM equipment will submit requirements through the current CIO/G-6 (SAIS-PR) process. For these specific waivers, the subject line must state

"Moratorium – IT Equipment," where the "XX" is the current FY. The request needs to include a detailed justification, impact statement describing results of not receiving a CIO/G–6 approval, vendor quote, and an approved requirements document (for example, capabilities request (CAPR), operational needs statement, or Joint urgent operational needs statement).

c. Commands that have requirements to purchase or replace existing Defense Red Switched Network (DRSN) switches will provide a detailed justification and impact statement to the CIO/G-6 (SAIS-PR) review authority (the Program Manager, Installation Information Infrastructure Modernization Program (PM I3MP)), to enable the PM to submit requirements via the chain of command to the CIO/G-6 for approval. The PM 13MP will coordinate and obtain funding for approved Army requirements, and forward requirements to the Joint DRSN Logistics and Acquisition Manager, Hill Air Force Base.

d. The moratorium and requirement to submit requests for waivers to purchase voice-switching equipment applies to all TDM voice-switching equipment that is not capable of providing VoIP or VoSIP services. The stated Army direction is to migrate as soon as practical to an almost-everything-over-Internet Protocol architecture, to include UC and collaboration, with an end state for end-to-end IP (see the Army CIO/G–6 Strategy for "End State" Army Network Architecture – Tactical, dated 6 April 2011).

e. Any command that has an urgent requirement to implement VoIP or VoSIP capability must follow the process included in paragraph 6-4 of this publication. The request will include—

- (1) A detailed justification.
- (2) An operational need statement.
- (3) Architecture details.
- (4) The supported organizations or entire installation.
- (5) An impact statement that describes the results of not receiving an approved waiver.
- (6) A bill of materials.

(7) The location where the equipment will be installed or where construction or renovation will take place.

(8) An approved requirements document and endorsement from a general officer or civilian equivalent.

3-4. Asynchronous transport mode equipment

a. Further investment in asynchronous transport mode (ATM) equipment will be terminated as soon as possible, and no longer installed within Army networks.

b. ACOMs that continue to require ATM support will be responsible for providing the funding for required levels of support. The Global Information Grid Waiver Board will consider all requirements for the continuance of ATM support beyond current sunset dates established in the Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII)) ATM Phase-Out Plan memorandum. New equipment can no longer be ordered from the one remaining vendor, and the current commitment for support expired 31 December 2012. While stopgap support may be available past the expiration date, it is likely that maintenance costs beyond December 2012 will rise markedly and potentially become prohibitively expensive. The goal is to eliminate ATM technology by 2015.

3-5. Telephone systems

a. Telephone system and network support. Telephone system and network support is provided through a combination of common-user and dedicated networks.

(1) Sensitive but unclassified voice network. The SBU voice network, formerly known as the Defense Switch Network (DSN), is the official DOD- switched voice network and is the preferred telecommunications means for all users. However, if SBU voice cannot be used in a timely manner, or if the person being called does not have SBU voice service, other long-distance services may be used. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02 provides the policies for all SBU voice, DRSN, and UC applications usage.

(2) *Networx*. The Networx contract will be used for non-mission command administrative voice services. The Networx contract is the General Services Administration contract providing additional telecommunications services outside DISA DISN contracts. It is the replacement for the Federal Telecommunications Service (FTS) 2001 contract. Networx contract services will be used for commercial access, unless other commercial voice services can be accessed without the expenditure of APF to increase the number or type of existing commercial circuits. NETCOM is the Army's responsible official for Networx service contracts. All requirements for Networx contract services will be submitted to NETCOM via applicable brigades and theater-level signal commands for service provisioning.

(3) Washington Interagency Telecommunications Services. Washington Interagency Telecommunications Services provide centralized administrative telecommunications service for DOD in the National Capital Region (NCR) in accordance with DODI 4640.07. This eliminates the necessity for each component to establish, operate, and maintain duplicative facilities. Tactical and special intelligence telecommunications are exempt from this directive.

(4) Annual inventory of unclassified voice switches.

(a) Commands will complete the annual inventory requirement by registering all new switches in the System Network Approval Process database. This includes switches that are able to make or receive SBU voice, DRSN, or

public switched telephone network (PSTN) calls and is technology independent (for example, waivered TDM, VoIP, VoSIP, and Local Session Controllers (LSC)).

(*b*) Commands will complete the annual inventory requirement by reviewing and updating the current information previously entered in the System Network Approval Process database (for example, any changes to the switch; points of contact; interim approval to operate (IATO) or approval to operate (ATO) information; location (if it is a deployable switch); DAA; and phone numbers).

(5) *Telephone services in military departments*. A DOD criterion classifies telephone service in military departments. Army telephones served by Government-owned or commercial telephone systems are classified as official (Classes A, C, and D); or as unofficial (Class B), in accordance with Defense Finance and Accounting Service-Indianapolis Regulation 37–1.

(6) Wired and wireless telephone and telephone-related service. (See DA Pam 25–1–1 for information on requests for wired and wireless telephone and telephone-related service.) The ordering process and procedures are available on AKO and Defense Knowledge Online (DKO).

(7) Long-distance calling.

(a) Sensitive but unclassified voice network. (See paragraph 3-5a(1).)

(b) Networx contract services. (See paragraph 3–5a(2).)

(c) Installation switch. Installation switches will be programmed to utilize SBU voice as the primary network where available; otherwise, the most economic route will be selected.

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

(e) Control and accounting. The NEC will ensure that callers at Army installations, without either a call detail reporting capability or an automatic identification system, will use a standardized control and accounting system with report capability to manage use of official telephone service.

(f) Local procedures. The installation commander will determine the local procedures for handling incoming official collect calls.

(8) Verification of bills and payment for telephone services.

(a) Verifying bills. Federal statutes require certification of long-distance telephone calls as official before paying for them. The office of the installation NEC has certification responsibility. The purpose of verification is to collect payment from those making unofficial calls. In accordance with U.S. Comptroller General Decision B–217996, (21 October 1985), NECs need not verify every call. Other procedures, such as statistical sampling or historical data, may be used to satisfy the statutory requirements, if they provide a high degree of reliability or certainty that certified calls are official. The NEC will establish local verification procedures for use, when necessary to certify bills or categories of bills as official (for example, repetitive one-time service bills for installation, removal, or relocation of instruments). (See DA Pam 25–1–1.)

(b) Networx contract service verification. The NEC will use judgment sampling to verify bills for Networx contract services. The General Services Administration, via the DISA Defense Information Technology Contracting Organization (DITCO), is the Government's contracting agency for Networx contract services.

(c) Billing and payment. On a monthly basis, the TCO or other designated official will review telephone billing and usage (to include phone cards). Federal agencies must pay interest or late charges if they do not make payments by due dates. The receiving unit (addressees) must "date-stamp" all telephone bills immediately upon receipt. The NEC will use the "date-stamp" to determine the payment due date when an invoice or contract does not show a due date. Charges for installation telephone services will be included in the assignment of charges for telephones services provided from Government-owned or commercially leased telephone systems.

(*d*) Pay in accordance with use and unofficial telephones. Pay in accordance with use, switched telephone service (coinless and coin box), and other unofficial telecommunications are morale, welfare, and recreation (MWR) functions. NAF contract procedures will be used, and contractor fee payments in accordance with these contracts will be paid to the nonappropriated fund instrumentalities (NAFI). These services will be managed by MWR in accordance with AR 215–1 and AR 215–4.

(9) Use of calling cards (includes prepaid and postpaid cards) and Government Emergency Telecommunication Service (GETS) cards.

(a) Approval. Installation commanders will approve the acquisition and use of telephone calling cards.

(b) Accountability. NECs (or designated Information Management Officers (IMOs)) will establish and maintain accountability procedures for telephone calling cards.

(c) Certification. Telephone calling cardholders must sign a local certification that acknowledges receipt of the telephone calling card and warns against loss, fraud, and unofficial use.

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

(10) Telephone and information system directory. Each NEC is responsible for maintaining a telephone and IS

directory that provides local organizations' telephone numbers. TCOs will provide their local NEC with their organizations' telephone directories.

(a) Publishing directories. Each Army installation will publish an organizational telephone and IS directory at least annually (see DA Pam 25–1–1). The names of individuals will be included only by exception as determined by the local public affairs official (PAO). If a telephone exchange serves several installations, refer to the IT Policy page at http://ciog6.army.mil/ for additional information. Electronic versions of the directory will be placed on that community's page on AKO, DKO, or Army Knowledge Online SIPRNET (AKO–S), as appropriate, but not on the Internet. Every effort will be made to publish e-directories and avoid printing and distribution costs.

(b) Releasing telephone or information system directories to the public. All installation directories will be unclassified. Installation telephone or IS directories (organizational only) may be released to contractors through the Government procuring or administrative contracting officer. Under no circumstances will directories containing names, home addresses, and telephone numbers be released to the public or placed on any Web site without access controls and prior approval of the organization's PAO. Approval from the organization's PAO and security official are required prior to posting personal information on AKO, DKO, or other private Web sites. If personal information is posted on AKO or DKO, the information will be further restricted to those individuals who have "need-to-know" status.

(c) The Army Knowledge Online and Defense Knowledge Online community pages. The AKO and DKO community pages will be utilized for publishing directories containing individuals' names and office information. AKO and DKO white pages are the primary tool for individual locator information.

b. Official existing telecommunications and unified capabilities services in personal quarters of key personnel. Official voice (telephone), data (SIPRNET or NIPRNET), and video service are authorized for key personnel whose positions require immediate response or have a direct bearing on the timely execution of critical actions. Key personnel will be designated based on functional position and mission impact. Official service installed in the quarters of key personnel will meet, at a minimum, the following conditions and arrangements:

(1) Access to local exchange. Official service will not have direct-dial access to the local commercial telephone system.

(2) Access to Sensitive but Unclassified Voice Network. Direct-dial access to SBU voice and Defense Telephone System is permitted. Official service in personal quarters will be class-marked for SBU voice and local on-post service only. All other services will be provided through the on-post switchboard operator (that is, Networx contract and commercial telephone exchange service will be routed through the local installation switchboard operator) or a local command operations center.

(3) *Restrictions*. Service will be restricted to the conduct of official Government business for mission command or tactical purposes.

(4) Separation of official and personal use services. Personnel selected for official communications service in their on-post quarters must provide, at their own expense, any of these services for the conduct of personal, unofficial business. This separate service will be from the local commercial exchange or the Government-furnished exchange, if authorized for local use.

(5) *Volunteers*. Installation commanders have the authority to install telephone lines and other necessary telecommunication equipment, and pay for the installation charges for the equipment when a spouse or volunteer with "official volunteer status" (pursuant to 10 USC 1588(f)), works out of the home (see DA Pam 25–1–1).

(6) *Multiline instrument*. The use of multiline instruments or electronic key systems to terminate official and unofficial lines in approved on-post quarters is authorized. Government-owned voice, data, and video systems will be used when it provides the lowest cost to the Government. In calculating lowest cost, consider the costs of reworking cable, removing and replacing instruments or key systems, purchasing instruments or key systems, and so on, for current and future occupants.

(7) *Classified*. Access to classified networks will be reviewed in accordance with AR 25–2 and approved on a caseby-case basis. Access controls and procedures will be documented in writing.

c. Secure wired and wireless communications equipment. See DA Pam 25–1–1 for information on secure wired and wireless communications equipment.

d. Automated service attendant. NECs will establish and provide installation operator services either on a local installation basis or on a centralized or regional basis. The types of services provided will be determined by each NEC.

3-6. Video services

a. Video teleconferencing. This policy applies to all Army video teleconferencing activities and capabilities (including videophones, desktop, and personal computer (PC)-based devices). A video teleconference (VTC) facility designated as a baseline service will be managed by the installation NEC. The NEC is responsible for establishing commonuser VTC procedures and guidelines for the respective garrisons. The NEC or other designee will approve all VTC systems. All items will meet the DOD Video Conferencing Profile (Federal Telecommunications Recommendation 1080B–2002 standards), be IP capable, and IPv6 compliant while moving away from integrated services digital network (ISDN) capabilities. Army activities will use contract vehicles managed centrally by the CHESS as the primary source when acquiring VTC equipment and services in accordance with AR 25–1. Funding for equipment and personnel to operate, maintain, and install common-user VTC facilities, is in accordance with the Army baseline service agreement (see DA Pam 25–1–1 for implementing procedures). The NEC or other designee will approve all VTC systems, to include those VTC systems used for mission purposes.

b. Video teleconferencing for intelligence. All intelligence activities requiring sensitive compartmented information (SCI)-secure VTC capability will use the JWICS or an equivalent SCI-secure VTC medium, and will be managed by the Army intelligence organization where the JWICS is installed.

c. Fixed-facility video teleconferencing. VTC fixed (permanent) facilities, which cost over the "other procurement, Army" threshold, will be validated by the requesting NEC, approved by the chain of command, and prioritized by the respective commander. For guidance on "other procurement, Army" thresholds, see AR 25–1.

d. Defense Information System Network video services.

(1) DISA provides the DISN Video Services (DVS) global contract as the vehicle to enable a DVS network or system to interoperate multiple conferences with fixed systems, roll-about VTC equipment, and portable VTC terminals. Installations that require common-user conference facilities will utilize the DVS global program for its connectivity or interoperability features.

(2) The DISN VTC manager (that is, NEC) will contact DISA about the return of any unused minutes for any VTC session that has been cancelled or the time has been adjusted, rescheduled or ended earlier than scheduled.

e. Budget submission for video teleconference. NECs will plan for expense and investment VTC systems to meet their current and projected needs. Requirements for investment equipment will be developed and forwarded annually, along with the requirement identified above by each NEC. This submission is the basis for establishing annual funding increments for system replacement. NECs will plan for expense and investment VTC equipment through installation resource management channels as part of their annual operating budget, and for inclusion in the Installation Management Command (IMCOM) and the appropriate signal command program objective memorandum (POM) submissions.

3-7. Commercial television service

Commercial television services (such as satellite, cable, and broadband services) provide television programs through a distribution system to standard television or radio receivers of subscribers who pay for such service.

a. Non-appropriated fund instrumentalities authority. Facilities that provide commercial television service are commercially owned and operated. The installation commander is the franchising authority. When appropriate, the installation commander may designate a NAFI to be the franchising authority. Overall staff management of commercial television service is the responsibility of the Assistant Chief of Staff for Installation Management/Family and Morale Welfare and Recreation Command at the Army level, and will be executed at the local level at the discretion of the installation commander.

b. Franchise. Commercial television service is primarily intended for the use and enjoyment of personnel occupying quarters (such as barracks rooms, temporary lodging facilities, and Family housing) on military installations and in this regard, will be considered the equivalent in purpose to MWR activities. DOD installations are commercial television service franchising authorities for the purpose of the applicable commercial television service laws. As a result, installations may issue a franchise that grants a commercial television service company access to the installation and designated rights-of-way to permit the commercial television service company to serve its subscribers. Individual subscribers contract directly with the commercial television service company for unofficial service. These subscribers are responsible for paying subscription fees and no APF are involved. Provisions of the FAR are applicable only when a DOD component subscribes to commercial television service for official DOD business and APF are utilized for payment of subscriber fees.

c. Use of appropriated funds. The provisions of the FAR are applicable to obtaining services when an Army activity subscribes for official DOD business and APF are utilized for payment of subscribers' fees.

d. Network enterprise center validation. NEC validation is required before any official services can be obtained. *e. Official transient lodging activities.* Provisions of AR 215–4 are applicable to obtaining services when an official transient lodging activity provides these services and NAF are used.

f. Non-exclusive franchises. Army policy is to provide for non-exclusive franchises only. A franchising authority may not grant an exclusive franchise, and may not unreasonably refuse to award additional franchises. The award of a franchise is not procurement by the Army and is not governed by the FAR. The franchise agreement must not obligate the Army to procure commercial television services for official purposes. If services are to be procured using APF, the services will be procured by contract in accordance with the FAR and its supplements.

g. Use of appropriated funds. APF available for morale and welfare purposes may be spent for user and connection fees for services to APF activities that serve the community as a whole in accordance with AR 215–1. Examples of these activities are hospital patient lounges and barracks day rooms (see appendix B for more information).

h. Subscription. No Army member will be coerced to subscribe to a franchisee's services.

i. Programming. Installations will not use Government funds or personnel to produce free programming solely for the benefit of a commercial television service company.

j. Installation channels. The Army will require that the commercial television service franchisee reserve oninstallation channel(s) for use by the installation. This channel(s) will be provided at no cost to the Government. The channel(s) reserved for Government use need not be activated at the same time as the rest of the commercial television service system. The channel(s) may be activated at any subsequent time at the option of the Government. When the channel(s) is activated, the following restrictions apply—

(1) Official programming. The Army must avoid both the fact and the appearance of underwriting a commercial television service system.

(2) Advertising. Program materials for use on command information stations will not contain commercial advertising or announcements.

(3) Non-Army use. During the periods of Government use, the reserved command channels may not be broadcast off-installation to non-Army subscribers.

(4) On-installation programming support. The installation PAO will support installation programming by providing advice, assistance, and command information materials and topics.

(5) Operational control. The PAO will have operational control of the reserved command channels.

(6) Official programming. Official programming is generated from installation visual information activities. The provisions of AR 360–1 address requests to use closed-circuit television (CCTV), commercial television service, or other systems for internal public affairs purposes.

k. Nonappropriated fund activities. The expenditure of APF to expand Government-owned commercial television services to provide entertainment television service to NAF activities or individuals is not authorized unless such expenditures are justified under provisions of AR 215–1.

3–8. Multifunction mobile devices

Portable electronic devices (PEDs) include mobile, cellular, and wireless telephones; personal digital assistants (PDAs); secure mobile environment portable electronic devices (SME PED); smart phones; tablets; and other devices as they are approved and placed on the UC APL or available through CHESS (see Department of Defense Directive (DODD) 8100.02).

a. Requirements. Army procured, provided, and maintained devices are to be used for official business and authorized use only, and may be approved for hand-held portable use. Authorized personal use of cellular phones is subject to the same restrictions and prohibitions that apply to other communications systems.

b. Local policies. Commanders will develop procedures for all subordinate organizations to implement policy on acquiring and using PEDs. Justification of the need will be included in requesting documentation. All devices will be managed as accountable items (see AR 740–26). Vendor service plans will be reviewed quarterly to identify and switch to plans that cover the organization's needs at the lowest overall cost.

c. Procurement.

(1) The NETCOM G-3 is the exclusive point of contact for procuring all wireless services and devices, including cellular telephones, pagers, wireless data devices, and related airtime service. When procuring wireless services and devices, all Army users are required to utilize the ordering procedures established by NETCOM and procure the services from established blanket purchase agreements (BPAs).

(2) Only PEDs that are listed on the UC APL are authorized on DOD networks.

d. User authentication. Organizations must require passwords where supported for user login and other user authentication, when not superseded by the use of an enforced and approved Public Key Infrastructure (PKI)-enabled hardware token (for example, common access card (CAC)). Portable devices may also receive approval to utilize biometrics as an authentication method.

e. Lost portable electronic devices. Users will immediately report stolen or missing PEDs to the NEC office so that service can be canceled or suspended to prevent illegal use or charges.

f. Sensitive transmissions. All wireless communications devices that are used to transmit sensitive information must be encrypted when connected to the installation network in accordance with AR 25–2.

g. Secure cell systems. Tactical units in a deployed environment will use only the Army's encrypted secure cell systems.

h. Beepers, pagers, and personal digital assistants. When beeper or pager functions are part of the features of a cellular telephone or personal digital assistant, the item will be managed the same as a cellular telephone. All Army organizations will use NETCOM BPAs established to provide economies of scale. The scope of beeper or pager service will be authorized based upon geographic service areas.

i. Usage. The following are unauthorized practices:

(1) Automatically forwarding residence telephone calls to Government PED telephone numbers. The only exception is for approved telework purposes. The forwarding of telephones is authorized with a commander's approval.

(2) Automatically forwarding personal cellular telephone calls to office phone numbers.

j. User training and agreements. Users will complete mandatory training and sign a user agreement prior to issuance of portable devices. The user agreement will include a description of the wireless service plan. The user will avoid using features or capabilities outside the plan.

k. Secure mobile environment portable electronic device.

(1) Army organizations are authorized to procure the SME PED and peripheral equipment. Peripheral equipment includes those items designed for use with the SME PED to facilitate data input, output, storage, and transfer or support functions (such as power, security, or upgrades). The SME PED and peripherals will be procured via the Army Information Systems Security Program (see AR 25–2 for more information).

(2) The purchase of SME PED products directly from the vendor(s) is prohibited.

(3) Army organizations are not authorized to procure software servers unless a Goal 1 waiver is granted (see paragraph 3-2). Implementation of SME PEDs will be aligned to enterprise email as enterprise email continues implementation.

(4) For Army organizations that obtain a waiver or re-purpose existing servers, deployment will be limited to locations approved by the NETCOM Assistant Chief of Staff, G–3. This will ensure synchronization with Army enterprise network efforts within the LandWarNet (for example, enterprise email). Non-Army organizations that obtain SME PEDs through the Army are exempt from the server moratorium, but are encouraged to consolidate where possible.

(5) Army organizations that procure and implement SME PEDs must follow all IA and security policies in accordance with DODD 8500.01E, DODI 8510.01, and DODI 8500.2 and all applicable STIGs.

(6) Users will complete mandatory training and sign a user agreement prior to the issuance of a SME PED. A sample copy of a SME PED user agreement can be found in the DISA SME PED STIG at http://iase.disa.mil/stigs/ net_perimeter/wireless/smartphone.html, in accordance with the ASD (NII) SME PED Implementation Guidance.

(7) The SME PED will be registered to a single, specific user and is intended only for personnel who have a bona fide requirement to process classified information outside of their normal workplace, or who otherwise require the capability to process classified information in a mobile environment.

(8) Each command will be responsible for preparing its own training plan and materials. User training will focus on, but not be limited to, the secure operation of the device, COMSEC operational procedures, security incident reporting, classified message incident (CMI) or data spill, device handling procedures, and information handling procedures.

(a) Training will be provided to each individual user and must be completed prior to issuance of a SME PED.

(b) Terminal administrators (TAs) will be trained and responsible for SME PED configuration, user and security training, control and use requirements, and administration of SME PEDs. Training will include the following:

1. Procedures for provisioning SME PEDs.

2. Preparation and maintenance of the user agreement.

3. Completion of required user training.

4. Requirement that all Army SME PEDs be configured to operate with the user's DOD-approved CAC PKI certificates.

5. Procedures for reporting security incidents; procedures for safeguarding passwords.

6. Procedures for re-provisioning DOD-approved CAC PKI certificates on SME PEDs when user certificates expire.

7. Proper use of the SCI facility mode.

3-9. Wireless priority service and wireline Government Emergency Telecommunications Service

Wireless priority service (WPS) and the Government Emergency Telecommunications Service (GETS) provide an endto-end nationwide wireless and wireline priority communications capability to key national security and emergency preparedness personnel during natural or man-made disasters or emergencies that cause congestion or network outages in the PSTN. WPS and GETS complement each other and ensure a high probability of call completions in both the wireless and wireline portions of the PSTN. WPS is a service added to the wireless phone after the phone has been issued to the user. Requests for WPS service must be submitted to the NEC or the local GETS and WPS program manager. The NEC or the GETS and WPS program manager will submit the request for WPS service to the National Communications System (now a part of the Department of Homeland Security), which will assign the authorization to the wireless number.

3-10. Non-tactical radio systems

a. Non-tactical land mobile radio systems.

(1) Usage. Non-tactical land mobile radio (LMR) systems provide wireless communications to support force protection, public safety, homeland security, and installation management missions of installations, posts, camps, and stations (see also DA Pam 25–1–1). Army non-tactical LMR systems also provide the means for installations to communicate and work cooperatively with nearby Federal, Defense, State, and local activities supporting homeland security and public safety missions.

(2) *The Network Enterprise Center as operator*. The installation NEC is the single provider and operator of all LMR capabilities, as approved by the CIO/G–6 at Army installations. LMR systems that are not operated by the NEC are prohibited, unless an exception is approved by the respective garrison-owning command.

(3) *Memoranda of understanding*. Memoranda of understanding that describe operational roles and responsibilities for all LMR services shared between the installation and outside agencies or other installations are required. A separate

memorandum of understanding will be developed and approved by the respective garrison and each outside agency or installation.

(4) *Resourcing*. The CIO/G–6 will notify NETCOM of the requirements for compliance with domestic and international laws, as well as DOD and Army policies regulating LMR usage. Installation NECs will identify all requirements for achieving compliance with their respective signal brigade. The signal brigades will identify regional priorities for LMR investments to the appropriate theater-level signal command based upon the level of risk to the installation of non-compliance with these laws and policies. Theater-level signal commands may submit these prioritized requirements to CIO/G–6 through the Army LMR Program (see also DA Pam 25–1–1 for information on LMR acquisition).

(5) *Capability standards*. All procured non-tactical installation LMR systems will comply with the National Telecommunications and Information Association (NTIA) narrowband mandate, Association of Public Safety Communications Officials International Project 25 (APCO P25) standards, and will support Type 3 encryption devices via the Advanced Encryption Standard.

(6) *Frequency assignments*. Installations will coordinate individual migrations of frequency assignments through the supporting area frequency coordinator, with the Army Spectrum Management Office (ASMO). The ASMO will coordinate these frequency assignments with DOD components and other Federal departments and agencies under current National Telecommunications and Information Association policy and procedures to minimize mutual interference and retain system integrity.

(7) *Waivers*. Submit requests for waivers for spectrum policies to the ASMO. Requestors will contact the ASMO for additional technical guidance.

b. Radio system support services.

(1) Installation requirements. Requirements for entry into existing networks will be identified to the installation NEC. Installation radio system support comprises non-tactical, user-operated, radio-networks, systems, facilities, equipment, and information services required to support host and tenant activities at the installation level.

(2) Usage. Installation radio system support services include fixed, trunked, conventional, mobile, and portable radio systems. Installation radio system support services are authorized only when existing ISs, including installation LMR, cannot satisfy mission-essential requirements. Requirements for installation radio support system services will be justified based upon operational necessities and an economic analysis. Commercial off-the-shelf (COTS) equipment available on Army-negotiated contracts will be utilized, unless otherwise justified. Availability of radio frequency assignment will be verified before procurement action is started. All installation information radio operations will be established and maintained in accordance with the security requirements of AR 25–2.

(3) *Military Affiliate Radio System*. The Military Affiliate Radio System (MARS) provides DOD-sponsored emergency communications on a local, national, or international basis as an adjunct to normal communications. The Army MARS program is addressed in AR 25–6. Commanders and agency heads will support and encourage MARS and amateur radio activities and avoid, within the limitations imposed by military agencies, any action that would tend to jeopardize the independent prerogatives of individual amateur radio operators.

Chapter 4 Satellite Communication Systems and Position Navigation and Timing

4-1. General

a. Satellite communications (SATCOM) include military satellite communications (MILSATCOM) and commercial satellite communications (COMSATCOM). MILSATCOM includes those systems (space, control, and terminal segments) owned and operated by DOD.

b. MILSATCOM also includes DOD gateways and service unique gateways. COMSATCOM encompasses DODleased bandwidth, DOD-owned or DOD-leased commercial band terminals and gateways landing DOD missions, and COMSATCOM used by DOD but provided by commercial entities using commercial terminals. The term SATCOM also includes allied, international partners, and other U.S. Government SATCOM used or provided by DOD. SATCOM systems are an integral part of the DOD network connectivity structure, which includes the architectures and systems of the combatant commands, and Defense and other Government agencies.

c. Army SATCOM terminal systems include military developed and acquired terminal systems (including Armyowned COTS terminals such as Inmarsat terminals and Iridium handsets). SATCOM systems are considered a DOD constrained resource. Access to SATCOM systems is based on Joint Staff validated and prioritized requirements and approved priorities. The United States Strategic Command (USSTRATCOM) and the Joint Staff manage access (see also CJCSI 6250.01D and DA Pam 25–1–1).

4-2. Commercial satellite communication annual usage report

a. To facilitate a strategic approach to COMSATCOM acquisition, DOD needs to understand how it purchases and uses COMSATCOM services and hardware. CJCSI 6250.01D requires USSTRATCOM, in coordination with the DISA, to prepare an annual commercial satellite communications analysis or report during the first quarter of each FY

for the previous FY, in order to validate cost and utilization information on the procurement of all COMSATCOM services. Headquarters, Department of the Army (HQDA), CIO/G–6 (SAIS–AON) is the organization that consolidates all Army input to the annual report. Upon receipt of the Joint Action Control Office tasking, NETCOM and 7th Signal Command will consolidate and report all commercial SATCOM usage contracted through NETCOM and submit the report to HQDA, CIO/G–6. All other Army organizations will report directly to the SAIS–AON action officer. The annual Joint Action Control Office tasking will include a detailed set of instructions for completing the report.

b. Individuals directly responsible for procuring the contracted SATCOM services will provide the required information in the format requested by the Joint Action Control Office tasking and submit it to HQDA, CIO/G-6 (SAIS-AON-S) to meet the assigned suspense date. The data-collection template requires cost and usage data for both fixed satellite services (FSSs) and mobile satellite services (MSSs), including equipment costs. FSSs are defined as solutions in the commercial C-band, Ku-band, Ka-band, or X-band typically achieved through the direct lease of bandwidth. This includes end-to-end connectivity solutions where commercial SATCOM provides a piece of the end-to-end link and managed solutions. MSSs are defined as predefined portable and hand-held solutions usually provided in the L-band, and billed in accordance with usage bases. Expenditure is defined as cost associated with the COMSATCOM services rendered with the FY.

4–3. Satellite communication requirements

a. Policy and procedures. CJCSI 6250.01D establishes top-level operational policy and procedures, and provides guidance for the planning, management, employment, and use of SATCOM (both military and commercial) systems. More detailed implementation guidance is found in the USSTRATCOM 714-series of strategic instructions. The space segments of all SATCOM systems are controlled as Joint assets to meet Joint Staff-approved requirements. Organizations and units must submit a satellite database (SDB) requirement to document their SATCOM requirements through the respective combatant command, Service, or agency to the Joint Staff Joint SATCOM Panel for validation and approval. The process is outlined in CJCSI 6250.01D. Submitting an SDB entry does not guarantee access to SATCOM systems, but allows organizations and units to request access via the Satellite Access Request and Gateway Access Request process. Satellite access is predicated on having a Joint Staff-approved SDB requirement and sufficient priority to assure access.

b. Satellite communication systems expert. The Army is assigned SATCOM systems expert responsibility for the payload and network control systems of the Defense Satellite Communications System, wideband global SATCOM (WGS), and the Mobile User Objective System.

c. Service requests. All Army components requiring COMSATCOM service from the DISA will submit a telecommunications request through DISA Direct Order Entry (DDOE). If the service cannot be provided by DISA, an Office of the Secretary of Defense (OSD) net centric waiver is required for an Army customer to request NETCOM to procure their COMSATCOM directly from a vendor. An SDB submission is still required with a submission of a telecommunications request for COMSATCOM.

4-4. Use of wideband military satellite communications

The Army will procure and field only single- and multiband-capable wideband satellite systems with at least one of these bands being a wideband MILSATCOM frequency band (that is, X-band or Ka-band).

a. Upgrading. All fielded wideband satellite terminal systems, including their network control, will be required to upgrade and be capable of operating over MILSATCOM as soon as fiscally possible when WGS achieves worldwide coverage. This will ensure the Army can take advantage of the WGS capability and reduce commercial transponder leasing costs.

b. Exceptions. Exceptions to the use of wideband frequency bands will be considered on a case-by-case basis. Justifications for exceptions to policy will be included in the operation needs statement and DD Form 1494 (Application for Equipment Frequency Allocation) submissions (see DA Pam 25–1–1 for procedures).

4–5. Satellite communication standardization

Organizations requiring SATCOM must comply with CJCSI 6250.01D and USSTRATCOM 714-series of strategic instructions, which standardize and consolidate Joint operations, management and control policies, processes, and procedures.

4-6. Network Command operations of military satellite communication systems

NETCOM operates and maintains designated strategic MILSATCOM terminals, the satellite Earth terminals for the Direct Communications Link, selected DOD Teleport sites, and Fixed Regional Hub Nodes.

4-7. Army component command to United States Strategic Command

As the Army component command to USSTRATCOM, the U.S. Army Space and Missile Defense Command/Army Strategic Command is the SATCOM systems expert for wideband MILSATCOM and the Mobile User Objective

System. The U.S. Army Space and Missile Defense Command/Army Strategic Command performs payload control on DOD wideband MILSATCOM satellites.

4-8. International Maritime Satellite and Iridium

a. Inmarsat and Iridium systems. The Inmarsat and Iridium systems are the only DOD-authorized commercial mobile SATCOM systems. Primary mission-command communications will be conducted via DISA, Joint or Combatant Commander, or Army networks and devices; with the Inmarsat and Iridium systems filling voids where primary military communications providers are not available and the transmission of such information is unclassified or appropriately protected to the level of the data sensitivity. Inmarsat must be used with an secure telephone equipment (STE) or other National Security Agency (NSA)-approved device. Iridium systems, with the exception of those used to communicate with continental United States (CONUS) first responders, must be used with the NSA-approved secure sleeve. Iridium secure sleeves are considered COMSEC equipment and must be procured through BPA with the Communications Security Logistics Activity (CSLA) (see AR 525–27, AR 25–2, and DA Pam 25–1–1 for more information).

b. Procurement of Inmarsat and Iridium equipment. ACOMs are responsible for funding Inmarsat terminal and Iridium handset acquisitions and airtime. Organizations and units will submit their requirements for approval to Deputy Chief of Staff (DCS)/G–3/5/7 (DAMO–RQ). Organizations and units will submit a telecommunications request through NETCOM to use the Army's Blanket Purchase Agreement (BPA) for Inmarsat services, including Inmarsat terminal systems, Broadband Global Area Network subscriber identity module card acquisition, and airtime activation. The procuring organization or unit is responsible for arranging the commissioning of Army Inmarsat terminals into satellite access operation by arrangement through NETCOM.

c. Operation of Inmarsat equipment. ACOMs and ASCCs will ensure field operators configure Inmarsat units to the correct Inmarsat land-Earth station. ACOMs, ASCCs, and direct-reporting units may use Inmarsat terminals during deployments and exercises. Upon the establishment of communications by the supporting signal units, Inmarsat terminals will become a backup means for communications.

d. Equipment readiness. ACOMs and ASCCs are responsible for testing Inmarsat terminals to ensure devices are in proper working order. Diagnostic tests will be performed in accordance with the operator's manual.

4–9. Position navigation and timing global positioning system, precise positioning service, and standard positioning services

The global positioning system (GPS) was designed as a worldwide, continuous, all-weather satellite navigation service that provides highly accurate positioning, velocity, and timing data to military users. The primary purpose of GPS is to enhance the effectiveness of U.S. and allied military forces.

a. Precise position navigation and timing capabilities enable and support a breadth of Army and Joint force (JF) critical missions and infrastructure in conducting all facets and scales of operations, including—

(1) Movement and maneuver (precise land, air, and sea navigation, and mine clearing).

(2) Fires (weapons delivery, precise fire support, self location, and target location).

(3) Intelligence (intelligence, surveillance, reconnaissance, operational environment awareness-force location and movement awareness, and target location (specifically time-sensitive targeting)).

(4) Sustainment (logistics).

(5) Command and control (timing and frequency synchronization for networks and blue force situational awareness).

b. The development and procurement of all precise positioning service (PPS), GPS user equipment, and PPS security devices, including those for special applications, will be coordinated with the GPS Directorate (PM organization under the United States Air Force Space and Missile Center). Army PPS users will employ PPS user equipment in accordance with CJCSI 6130.01D to support combat and sustainment operations. The Army Acquisition Executive (AAE) submits waiver requests to OSD for use of the standard positioning service (SPS). These SPS systems cannot be used for critical military operations, such as weapon delivery coordination, target location, and fire support.

c. Except for congressional exemptions (range instrumentation, advanced technology, mapping, special operations, and classified applications), the GPS Directorate will develop and procure all DOD GPS common-user equipment. Submit waiver requests for special applications to OSD through the AAE.

Chapter 5 Long-haul and Deployable Telecommunications

5-1. General

This section provides Army policies on the use of long-haul communications, wide-area networks, and deployable communications (see DA Pam 25–1–1 for additional information).

a. Defense Information System Network. The Defense Information System Network (DISN) is DOD's integrated worldwide enterprise-level network for exchanging secure and non-secure data, voice, and video information.

b. Requirements.

(1) All Army long-haul customers will use DISN service and transport to satisfy Army long-haul and wide-area network transfer communications requirements to the maximum extent possible. Requirements will be processed in accordance with DISA Circulars (DISAC) 310–55–9 and 310–130–1, and the supporting Army activity's procedures. The policies above state that all long-haul telecommunications services will be planned, designed, implemented, managed, and acquired by DISA.

(2) All Army requests to DISA for acquiring basic long-haul services will be submitted to Army Telecommunications Division (ATD), NETCOM for technical review, financial approval, assurance of Army compliance with governing policies and regulations, and for completion of the order through the DDOE system. DISA is designated as the only entity authorized to order telecommunication services from the Networx contract for the Army.

(3) If DISA is unable to fulfill Army requirements, a GIG waiver must be acquired (see paragraph 5-2).

(4) Army organizations will continually assess the impact of mission and operational concepts on their long-haul communications requirements. NECs will validate operational requirements before requesting connection approval from NETCOM to ensure DISN is the best solution for the requirements by considering the bandwidth, security, connectivity, and other technical issues.

(5) The amount of bandwidth requested will be reasonable and justifiable according to existing operational needs and realistic projected growth for 1 to 3 years. Bandwidth utilization statistics will show a 3-month sustained peak utilization during normal business hours of at least 65 percent before a bandwidth upgrade is requested, unless there are other known circumstances (such as unit re-stationing and system fielding) that will cause the existing, available bandwidth to be exceeded. NECs will validate bandwidth requests in accordance with above.

(6) Bandwidth will be managed in the most effective and efficient manner in accordance with the tools and resources available. The first priority of bandwidth usage is to accomplish Army missions.

(7) Regarding the identification and planning for future bandwidth requirements, NETCOM will validate requests for bandwidth changes received from customers once an engineering analysis has been completed. Requests will be based on current utilization and known future bandwidth requirements needed to support future enterprise initiatives and systems.

(8) NECs will ensure data, video, and voice switching hardware and software are on the UC APL found at https:// aplits.disa.mil/ before procuring these items. All software placed on the network is required to have a certificate of networthiness (see AR 25–2).

c. Sensitive but unclassified voice network. SBU voice is the DOD-preferred means of providing non-secure circuit switched voice communications in accordance with CJCSI 6211.02. SBU voice may be used to transmit unclassified facsimile traffic. SBU voice is part of the DISN.

d. Defense Red Switched Network services. The DRSN is a secure, mission-command system that supports secure voice and conferencing requirements; and is a separate, secure switched network that is part of the DISN.

(1) Overall requirements. The combatant commanders and DOD agencies coordinate the overall Joint requirements for DRSN services in accordance with CJCSI 6211.02. Army commanders are responsible for their designated portions of the DRSN. This may include, but is not limited to, providing operation and maintenance (O&M) funds for the DRSN logistics support, sustainment, training, DRSN-related equipment, and special interface trunks required by the combatant command or supported command for which they are responsible.

(2) Unique requirements. Unique requirements will be forwarded through the Army Signal Commands to HQDA, CIO/G-6, SAIS-AOI, for coordination and validation. Guidance for submitting DRSN requests can be found in the CJCSI 6211.02.

(3) *Certification*. Servicing ACOMs will certify whether funds are available as part of the DRSN approval request. The funding review and forecast for certification will be coordinated through the chain of command to the CIO/G–6 prior to approval.

e. Defense Message System.

(1) Usage. The Defense Message System (DMS) has been designated as the DOD record messaging system. The DMS may be implemented in all environments. Organizational messaging is defined as correspondence that is used to conduct the official business of the Army. As an organizational message system, DMS may be used to commit resources, direct action, clarify official positions, or issue official guidance. DMS migration will be accomplished through centralized fielding by the Army DMS PM (see DA Pam 25–1–1).

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

(3) *Privacy communications*. For information on the Privacy Communication System messaging, refer to Allied Communication Publication (ACP) 127(G) located at http://jcs.dtic.mil/j6/cceb/acps/; and the DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements available to CAC holders through the DMS asset distribution system at https://dkwwwefgv001.roscc1.disa.mil/.

f. Joint Chiefs of Staff-controlled mobile or transportable communications assets. Joint Chiefs of Staff (JCS)

maintains control of mobile or transportable communications equipment, and ensures the equipment is kept in readiness for worldwide emergency and contingency communications for the operational and support needs of the JCS. All ACOMs with requirements for JCS-controlled assets will submit requests in accordance with CJCSI 3110.10.

5-2. Non-Department of Defense connections to the Defense Information System Network

a. Approval authority. The Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD (NII)/DOD CIO) will approve all non-DOD connections to the DISN. Army sponsors must validate and endorse non-DOD requests for connection to the DISN.

b. Non-DOD connection requests. All non-DOD connection requests will be submitted via DISA to the HQDA, CIO/G-6 (SAIS-AOI) for coordination and validation (see DODI 8100.04 and CJCSI 6211.02).

c. Termination of connection. Command sponsors are responsible for the oversight of the connection to include termination of the connection. Termination can be due to contract expiration, new vendor providing services, or approval expiration date. Upon termination or expiration of a current non-DOD approval, the sponsor will notify the HQDA, CIO/G–6 (SAIS–AOI) when connections are terminated.

d. Renewal of connection. If a non-DOD connection is within its expiration date and the sponsor's requirement is still valid, the sponsor is responsible to renew the connection request. A renewal letter will be submitted to the DISA.

(1) If there is no change to mission, sponsor, contract, or location, the sponsor fills out the revalidation template located at http://www.disa.mil/Services/Network-Services/DISN-Connection-Process//media/Files/DISA/Services/DIS-N-Connect/Library/reval_nondod_request_pdf.pdf. This will be sent to DISA for revalidation with a copy to the HQDA, CIO/G-6 (SAIS-AOI).

(2) If the sponsor has any of these changes (mission, sponsor, contract, or location), a new validation template will be used and clearly state what the change is at the top of the document. A full revalidation is needed due to a change in sponsor. The template and revalidation information can be found in the DISN Connection Process Guide located at http://www.disa.mil/Services/Network-Services//media/Files/DISA/Services/DISN-Connect/Library/dis-n_cap_04272011.pdf.

5–3. Global information grid waivers

a. Policy. DODI 8100.04 and CJCSI 6211.02 serve as the basis for Army policy in which the GIG waiver board will approve waivers for any DOD use of non-DISA Services (for example, DISN). Army entities requiring communications services outside of DISA will submit a GIG waiver. This includes, but is not limited to, compliance with DOD networks, computing infrastructure, Internet connectivity, satellite, and domain management, as well as the oversight of the migration of legacy networks into DISN to satisfy Program Budget Decision (PBD) 723C, 10 December 2004.

b. Information Assurance. An interim authority to operate (IATO) or authority to operate (ATO) must be completed in conjunction with submitting the waiver request. An ATO or IATO is required prior to going before the Defense Security and Information Assurance Working Group (DSAWG) and the GIG Waiver Panel. Army personnel will work in the Certification and Accreditation Tracking Database located at https://armydiacaptdb.arl.army.mil to acquire an ATO or IATO via the DOD Information Assurance Certification and Accreditation Process. Contact iacora@us.army. mil with questions.

c. Computer network in defense service provider.

(1) A computer network defense service provider (CNDSP) is not required for an organization that will only be passing public information or data over the commercial Internet Service Provider (ISP) connection. An organization does not have to fill in this space in the SNAP database or in the presentation software; it only has to indicate this is not applicable. However, the following two items are required to be identified in the presentation:

(a) Active monitoring (for example, indicate how often the connection is monitored on a daily, weekly, or bimonthly basis, or some other time period).

(b) If there is a discrepancy, threat, or hacking event, identify the person within the organization who will receive a report of the event.

(2) A CNDSP must be identified, and an agreement must be in place, for an organization that is passing DOD information or data over the commercial ISP connection to verify the CNDSP is providing this service.

d. Internet service providers. The only authorized access from Army computers, systems, and networks to the Internet is through a DISN-controlled and DISN-monitored connection. Exceptional situations may exist where Army organizations connected to the NIPRNET may also require direct connection to the Internet (for example, through a commercially provided ISP). For exceptions, the organization must submit a waiver request for validation by the NEC through the chain of command to HQDA, CIO/G–6 (SAIS–AOI).

(1) Commercial Internet service. Army organizations may acquire commercial Internet service (for providing email service, Web access, and OCONUS liaison missions), after approval of a GIG waiver, for users who do not have or cannot obtain access through an Army, DOD, or other Government gateway. However, these organizations will not have any connectivity to any Government-owned networks, such as NIPRNET, SIPRNET, and JWICS. NEC validation is required before any official access services can be obtained for a commercially provided ISP. NECs will ensure the proposed network architecture complies with security requirements and makes efficient use of available bandwidth.

(2) Unofficial service. Internet connections for educational (off-duty or non-duty related) or unofficial MWR activities are permitted, but no computer, system, or network used for these purposes can be connected to the NIPRNET. Units in the field may obtain commercial ISP service for these purposes (for example, for communicating with Family support groups in the sustaining base) using unit funds established and managed in accordance with AR 215–1 (see AR 215–4, which governs IT supplies and services acquired with NAFs). These Internet connections will be coordinated through the NEC with the NETCOM support office prior to connection.

(3) Cost for unofficial service. The cost to procure Internet access via an ISP is a communications cost under the appropriate IT budget line(s). Army funds will not be used to provide Internet access to Army housing or quarters unless sufficient justification exists, on a case-by-case basis (for example, key command personnel with a genuine need for service at any and all hours, and so on). Unofficial, free, or pay-for-use Internet access is to be managed by MWR in accordance with ARs 215–1 and 215–4.

e. Global information grid waivers. A GIG waiver is not required for the following exceptions:

(1) When a commercial ISP will be used solely for a MWR mission and is paid for by MWR (See DODI 1015.10).

(2) If a customer is temporarily using a commercial ISP in direct support of a training exercise. A permanent connection for one or more exercises that occur annually does not qualify as an exception.

(3) Nothing in this regulation precludes occupants in Army housing and quarters from obtaining commercial ISP services for their own personal use, provided the cost is borne by the occupant(s).

5-4. Military telecommunications agreements

a. International agreements. Army activities will adhere to U.S.-ratified international standardization agreements (including NATO standardization agreements and American, British, Canadian and Australian Quadripartite standardization agreements) when designing or procuring UC equipment. Exceptions may be requested through CIO/G–6 (SAIS–AOC) when unique Army specifications are a major impediment to the adoption of an otherwise cost-effective allied system. Army CIO/G–6 is the voting representative to the SATCOM Interoperability Standards Committee in support of NATO.

b. North Atlantic Treaty Organization communications. Army activities will carry out assigned responsibilities contained in formally consummated memoranda of understanding or similar documents between the U.S. Government, NATO, and NATO nations, including formal U.S. commitments made in support of NATO and NATO-member communications plans, programs, and policy.

c. North Atlantic Treaty Organization facilities. Whenever the Army requires communications facilities, the available communications facilities of NATO or member nations will be used to the maximum extent feasible, provided reliable communications for use can be assured, and that such use is cost effective.

d. Unilateral communications. When NATO and NATO-member communications are nonexistent, inadequate, or not cost effective for use, the U.S. will provide unilateral communications. These are wholly owned, operated, and maintained by the U.S. Government or U.S. commercial enterprises, or a combination thereof, and will be used by the U.S. to provide minimum essential unilateral control of U.S. forces and to complement NATO and NATO-member nation communications.

e. Interoperability. Interoperability will be achieved on a planned, step-by-step basis and efforts toward consolidated, collocated, interconnected, and interoperable systems will result in mutually supportive U.S., NATO, and NATO-member systems that satisfy NATO, other NATO members, and U.S. requirements.

f. Compatibility and interoperability of tactical mission command, communications, and intelligence systems.

(1) *Tactical mission command, communications, and intelligence systems.* The Army will develop, acquire, and deploy tactical mission command, communications, and intelligence systems that meet the operational needs of U.S. tactical forces and are interoperable with allied tactical and non-tactical mission command, communications, and intelligence systems, including systems used to support civil authorities.

(2) *Requirements*. The coordination and validation of requirements, to include required Joint coordination, will be accomplished in accordance with AR 70-1 and AR 71-9.

(3) *Interfaces*. For interfaces between tactical and non-tactical mission command, communications, and intelligence systems that support Joint or combined operations, the J–2, Joint Staff assists in making defense intelligence communication acquisition requirements, supports military forces, and helps achieve Joint and multinational interoperability. Intelligence warfighting requirements are examined for solutions and to ensure compliance with DODDs and Joint directives.

(4) *Joint approval*. The Joint Staff is the approval authority for Joint or combined communications systems prior to the initiation of system development. Established Joint interface standards and operational procedures are standard practices for tactical Army mission command, communications, and intelligence systems. Requirements for new Army-funded Joint or combined tactical mission command, communications, and intelligence systems will be validated by the CIO/G–6 prior to forwarding to the Joint Staff.

(5) North Atlantic Treaty Organization agreements. The basis for U.S. and Allied compatibility and interoperability of tactical mission command, communications, and intelligence systems will be those agreements between the U.S., NATO countries, or alliances as specified in requirements documents and Allied standardization agreements.

(6) Interoperability testing. Interoperability testing and evaluation (T&E) of tactical mission command, communications, and intelligence systems will be performed during the acquisition process. T&E will be conducted throughout the acquisition process via established system benchmarking or demonstrations to reduce acquisition risks and to estimate operational effectiveness and suitability of the system. Critical capabilities, test objectives, and evaluation criteria related to mission requirements will be established at the beginning of the acquisition process. Functional proponents and material developers (MATDEVs) will use performance measurements to ascertain performance and results-based management of mission command, communications, and intelligence systems (see AR 25–1 and AR 73–1 for policy on interoperability testing).

Chapter 6 Unified Capabilities

6-1. Introduction

The Army's objective is to transition to UC and add new capabilities and features to meet existing and emerging Army requirements. At the same time, this new technology must provide the same assured service and high-quality communications that users expect (including continuity of service during power failures). Also, the addition of voice and video over IP to data networks adds new IA vulnerabilities. These vulnerabilities will be mitigated using appropriate IA techniques.

6-2. Policy

a. In accordance with DODI 8100.04, DOD components will integrate current network technologies with future network technologies to provide UC (for example, any single or combination of information media such as voice, video, or data, whether converged or non-converged) on DOD networks. Products that provide or support UC acquired or operated by DOD components will be certified for interoperability and IA. ACOMs will comply with functional requirements, performance objectives, and technical specifications for DOD networks that support UC, as specified in ASD (NII)/DOD CIO publication DOD Unified Capabilities Requirements (UCR) 2008 (UCR2008) or latest version.

b. For exclusions to UC requirements, see DODI 8100.04.

c. The NEC is designated as the installation information manager on Army installations. There will be only one NEC at an installation and a single NEC at U.S. Army Reserve Command. The installation NEC will be the single authority for providing common-use IT services (for example, Command, Control, Communications, Computers and Information Management (C4IM Services List). The NEC will be the initial focal point for tenant organizations and activities to obtain support for unique IT services that are not provided in the C4IM Services List. The garrison NEC is the only organization on the installation authorized and responsible for providing common-use baseline services on a non-reimbursable basis to all installation tenants as prescribed by the C4IM Services List. IT support services consist of the following four categories: baseline, enhanced, mission-funded, and mission-unique. Upon identifying a requirement that needs higher-level approval, the NEC will forward any requirement to the local Theater-level signal command, which in turn forwards the requirement to NETCOM and to the CIO/G–6 for higher-level approval. The current authorization C4IM Service List and LandWarNet Catalog is located at https://www.itmetrics.hua.army.mil/.

d. In accordance with DODI 8100.04, DOD Components will submit requests for UC transport (regardless of technology implemented) to the Director, DISA for consideration and approval.

6-3. Unified capabilities approved product list

ACOMs will purchase data, video, and voice-switching hardware and software from the UC APL found at https:// aplits.disa.mil/processAPList.do. If no listed product meets the organization's needs, the organization may sponsor a product for testing that does meet their needs. In accordance with AR 25–2, COMSEC cryptographic or encryption devices and equipment must be procured through BPA with the Communications Security Logistics Activity (CSLA).

6-4. Voice services

a. Voiceover Internet Protocol.

(1) *End-to-end Voiceover Internet Protocol*. End-to-end VoIP is the DOD preferred means of providing unclassified voice communications. The latest UCR will be used as policy guidance for implementing VoIP capabilities. Voice will be migrated from a circuit-switched, TDM infrastructure to an IP packet-switched infrastructure.

(2) Network Enterprise Technology Command. NETCOM will serve as the single authority assigned to operate, manage, and defend the Army's infrastructure at the enterprise level for VoIP infrastructure.

(3) Program Manager, Installation Information Infrastructure Modernization Program. The PM I3MP will procure and field VoIP capability as a part of the network infrastructure modernization cycle.

(4) Non-end-to-end Voiceover Internet Protocol. Commands requesting new requirements to implement VoIP that does not support end-to-end capability, and is not being provided by I3MP, will be reviewed on a case-by-case basis. The request will be processed through the appropriate NEC, signal command, then through NETCOM, and then

forwarded to CIO/G–6 (SAIS–AOI) for approval. Organizations not located on an installation with a NEC will forward their requirement to the appropriate signal command, then to NETCOM. The package submitted to CIO/G–6 (SAIS–AOI) will include a cost or operational benefit analysis of the proposed implementation, which will reflect benefits in either monetary terms or enhanced capability.

(5) *Backup power*. Whenever the primary source of power is disrupted, backup power will maintain continuous operation of voice services for users who can initiate precedence calls. For health, safety, and security reasons, all other users must be provided with communications capabilities when the primary power fails, but these communications do not have to be VoIP. The VoIP system design will ensure reliability requirements meet those stated within the most recent approved UCR and the appropriate VoIP STIGs.

(6) Analog and digital time-division multiplex telephone service. A plain old telephone service (analog phone) connected to a legacy circuit switch may be installed in Army buildings as a backup to the VoIP service, if that building has backwards compatibility. A plain old telephone service phone may also be connected to a media gateway and PSTN. This is to provide emergency voice service if VoIP phones do not function.

(a) Service requests. NECs will submit voice service requests to NETCOM G–3 with a courtesy copy provided to the respective brigade office. NETCOM will obtain voice service requests, such as local central office trunks, direct-indial numbers, commercial business lines, and Foreign Exchange (FX) trunks or lines, via consolidated local service contracts that are competed among interested service providers. NETCOM will satisfy requirements for base communications (BASECOM) local-leased telephone services through BASECOM consolidated contracts. Those interested in acquiring local-leased telephone and telephone-related services will send an email to the point of contact (POC) at usarmy.huachuca.netcom.mbx.g-34–atd-basecom@mail.mil. If the existing consolidated contract cannot be used to satisfy the requirement, NETCOM will competitively award a new contract to satisfy the requirement. NETCOM will determine whether an existing consolidated contract will be modified, or if a new contract is required to fulfill service requirements (see DA Pam 25–1–1 for more information).

(b) Work orders. NECs will submit a DD Form 1367 (Commercial Communication Work Order) against an existing consolidated contract when acquiring voice services for the installation. NEC ordering officers, appointed by the NETCOM contracting officer, are authorized to place orders up to the dollar limit defined in their appointment orders. NECs will submit all orders that exceed the NEC ordering officer's threshold to the NETCOM contracting officer. If an Army user is in a location where there is no NEC support, the user will coordinate procurement directly with the NETCOM. A lack of NEC support does not negate the requirement to procure service through NETCOM.

(c) Base communication funding. The supporting NEC will be the focal point for all common-use BASECOM on the installation or the supported area. BASECOM falls into one of four categories of services that are listed on the C4IM Services List, and are funded on a reimbursable or non-reimbursable basis depending on whether the services requested are baseline services or above baseline services. The four categories of services are listed below (see AR 25–1 for more information)—

1. Baseline services. Baseline services are specifically designated as "baseline" in the C4IM Services List. Installation NECs will provide baseline IT services to Army activities on a non-reimbursable basis.

2. Enhanced services. Enhanced services are "baseline" services with enhanced performance measures that exceed one or more of the standards listed in the C4IM Services List. Army activities desiring enhanced IT services will request and obtain these services from the installation NEC on a reimbursable basis. Army activities will enter into support agreements for enhanced services through the NEC to the respective signal brigade.

3. *Mission-funded services*. Mission-funded services are specifically designated as "mission funded" in the C4IM Services List. Army and non-Army activities desiring mission-funded services will request and obtain these services from the installation NEC on a reimbursable basis, unless the NEC determines that NEC operations cannot reasonably provide the required service. Customers will enter into support agreements for mission-funded services through the NEC to the respective signal brigade.

4. *Mission-unique services*. Mission-unique services do not appear on the C4IM Services list since the list only includes the most commonplace IT services. Resourcing and provisioning for these services are the responsibility of the tenant activity. If the unique mission service (for example, lab and test range) interfaces in any way with the installation IT infrastructure, activities will submit acquisition plans to the installation NEC for review and comment. After receiving NEC comments, Army activities may acquire mission unique IT services by—

a. Providing mission services with internal organization resources.

b. Obtaining contract support for mission services.

c. Reimbursing NEC for mission services. Customers will enter into support agreements for mission-funded services through the NEC to the respective signal brigade.

(7) NECs will submit a request to NETCOM requesting a telecommunications service priority (TSP) for the restoration priority of leased 911 and E911 circuits. This will give priority to 911 circuits if an outage occurs. Submit request to usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil.

b. Voiceover Secure Internet Protocol.

(1) End-to-end VoSIP is the DOD preferred means of providing classified (secret only) voice communications. The latest UCR will be used as policy guidance for implementation of VoSIP capabilities. The UCR requires that VoSIP

migrate to multi-vendor equipment using the Assured Services Session Initiation Protocol (AS–SIP). The UCR further requires that this AS–SIP equipment be interoperability-tested and IA-accredited by the Joint Interoperability Test Command (JITC), then placed on the UC APL at https://aplits.disa.mil/. For AS–SIP equipment, only VoSIP equipment listed on the UC APL is authorized for use.

(2) ACOMs will use DISA as their primary VoSIP service provider.

(a) DISA will provide an Enterprise VoSIP solution for all new VoSIP requirements, which will alleviate the requirement for the Army to implement call processors.

(b) Any VoSIP requirement that cannot be fulfilled by DISA will be reviewed on a case-by-case basis for CIO/G-6 (SAIS-AOI) approval. All requests will be forwarded with appropriate recommendations via the chain of command. The request will include—

1. A detailed justification.

2. An operational need statement.

- 3. Architecture.
- 4. The supported organizations or the entire installation.
- 5. An impact statement that describes the results of not receiving an approved waiver.
- 6. A bill of materials.
- 7. The location where the equipment will be installed or where construction or renovation will take place.

8. An approved requirements document and a General Officer or Senior Executive Service member endorsement. (c) The NEC will be the initial focal point for organizations and activities to obtain Enterprise VoSIP services. The

NEC will follow the most current version of the C4IM Services List in reference to the date of request. The C4IM Services List and customer-facing LandWarNet Catalog are located at https://www.itmetrics.hua.army.mil.

(3) NETCOM will serve as the single authority assigned to operate, manage, and defend the Army's existing infrastructure at the command level for VoSIP infrastructure.

(4) VoSIP must follow DISA's SIPRNET connection approval process. All VoSIP systems must follow all current processes and policies in the DOD Information Assurance Certification and Accreditation Process. DISA is responsible for the VoSIP IP addressing scheme and numbering plans.

6-5. Video services

See paragraph 3-6 for more information on video services.

6–6. Element management system

a. The Army Cyber Command will operate and maintain an element management system to protect the IP voice and video network. The IP voice network must be monitored to ensure security as it currently does not route through the Army's top-level architecture (TLA) stacks. NETCOM is responsible for the function requirements documents that contain designs for regional top-level architecture and standard TLAs. Army TLA stacks will be compliant with current DISA network and enclave STIGs.

b. The PM I3MP will implement the element management system.

6–7. Collaboration capabilities

a. Unified collaboration capabilities. These capabilities integrate standards-based communication and collaboration services, including, but not limited to, presence, instant messaging, chat, voice, video, Web conferencing, and unified communication and collaboration applications or clients. These standards-based UC services will be integrated with available enterprise applications, both strategic and tactical.

b. Use of encryption. Collaboration that requires data integrity, message authenticity, or non-repudiation of DODsensitive information (other than personally identifiable information sent by information-privileged individuals, volunteers, or Reservists) will be signed using DOD-approved certificates. The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates. A DOD PKI encryption certificate will be used to sign and encrypt sensitive information for transmission.

c. Bandwidth usage. NECs are required to develop local procedures on efficient and effective bandwidth usage, and encourage processes to manage bandwidth demand.

d. Use of official Government unified capabilities services. Only Government-provided services are authorized for use as primary UC. All UC services provided by a commercial service provider are prohibited for Army business communications.

e. Collaborative tool administration. Local procedures will provide for the implementation of sound 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) Accounts are assigned only to individuals authorized to use Army-operated IT systems.
- (3) Passwords are protected and stored to the same level of protection as the most sensitive data in the system.

(4) Inactive accounts are terminated after a specified period of time (for example, 30 days) if no longer needed.

(5) Addresses are correctly formatted and registered with central directories as required for efficient operations, and that the Global Address List reflects SBU voice numbers as well as commercial numbers.

f. Instant messaging and chat records. Army records management policies apply to IM and chat traffic. Designated records managers (RMs), records coordinators (RCs), and records custodians will monitor the application of records management procedures to IM and chat records. Backup storage is not considered records archiving (see AR 25–400–2 and AR 25–1 for more information on preserving communications as records).

g. Backup and storage. Systems administrators will ensure that IM and chat servers are backed up for a period of no less than 90 days in an offsite secure storage facility. Backups will be conducted on a daily, weekly, and monthly basis in accordance with local procedures.

6-8. Installation information infrastructure

a. During construction of a facility, local area networks (LANs) will be installed to meet the requirements of end users, as specified by the UCR. The LAN may be a high-availability Assured Service Local Area Network (ASLAN), a medium-availability ASLAN, or a non-ASLAN. Note that the UCR provides specific requirements for non-ASLANs.

b. Existing metallic cabling will be used as long as it is capable of providing the required service(s). New cable runs, optical fiber or combined fiber, and twisted pair cable must be installed for within and building premises. This includes cable from the main distribution frame, through intermediate distribution frames, and to the communications distribution room. Army military construction that provides only copper to the outlet will provide additional raceway space to accommodate future fiber-optic cable installation, for both premise wiring and the outside cable plant. Fiber-optic cable will be installed to the outlet during construction, if the user or proponent has a current valid requirement for fiber-optic connectivity.

Appendix A References

Section I Required Publications

AR 25–1

Army Information Technology (Cited in paras 2-6, 3-2b, 3-6a, 3-10b(2), 5-4f(6), 6-3, 6-4c, 6-7f, C-5.)

AR 25–2

Information Assurance (Cited in paras 1-4, 2-2b, 2-3, 3-5b(7), 3-8k(1), 3-8f, 5-1a(1)(h), C-19.)

AR 215–1

Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities (Cited in paras 3-5a(8)(d), 3-7k, 3-7g, 5-3d(2), 5-3d(3), B-4.)

AR 215-4

Nonappropriated Fund Contracting (Cited in paras 3-5a(8)(d), 3-7e, 5-3d(2).)

CJCSI 6250.01D

Satellite Communications (Available from https://ca.dtic.mil/cjcs_directives/cdata/limited/6250_01.pdf.) (Cited in paras 4–2a, 4–3a, 4–5.)

DA Pam 25-1-1

Information Technology Support and Services (Cited in paras 2–1i, 2–1f, 3–5b(5), 3–5b(7), 3–5a(6), 3–5a(8)(a), 3–5a(10)(a), 3–6a, 3–10a, 3–10a(4), 4–1c, 4–4c, 4–8a, 5–1d, 5–1, 6–4a.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read a related publication to understand this publication. Army publications are available on the Army Publishing Directorate (APD) Web site at http://www.apd.army.mil. Department of Defense publications are available at http://www.dtic.mil/whs/directives. The United States Code is available at http://www.gpo/gov/fdsys. The CJCSI are available at http://www.dtic.mil.

AR 25-400-2

The Army Records Information Management System (ARIMS)

AR 25–6

Military Affiliate Radio System (MARS) and Amateur Radio Program

AR 25–30

The Army Publishing Program

AR 70–1 Army Acquisition Policy

AR 71–9 Warfighting Capabilities Determination

AR 73–1 Test and Evaluation Policy

AR 190–53 Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 360–1 The Army Public Affairs Program

AR 380–10

Foreign Disclosure and Contacts with Foreign Representatives

AR 380–53 Communications Security Monitoring

AR 525–27 Army Emergency Management Program

AR 700–131 Loan, Lease, and Donation of Army Materiel

AR 740–26 Physical Inventory Control

ACP 123 Common Messaging Strategy and Procedures (Available from http://jcs.dtic.mil/j6/cceb/acps/.)

ACP 127 Communications Instructions – Tape Relay Procedures (Available from http://jcs.dtic.mil/j6/cceb/acps/.)

CJCSI 3110.10 Communication Systems Supplement to the Joint Strategic Capabilities Plan

CJCSI 6130.01D

2007 CJCS Master Positioning, Navigation, and Timing Plan (MPNTP)

CJCSI 6211.02

Defense Information System Network (DISN) Responsibilities

DFAS-IN 37-1 Regulation

Finance and Accounting Policy Implementation (Available at http://www.asafm.army.mil.)

DISAC 310-55-9

Base Level Support for the Defense Information System Network (DISN) (Available at http://www.disa.mil/About/Policy-Publication-Information.)

DISAC 310-130-1

Submission of Telecommunications Service Requests (Available at http://www.disa.mil/About/Policy-Publication-Information.)

DODD 5105.19 Defense Information Systems Agency (DISA)

DODD 5105.77 National Guard Bureau (NGB)

DODD 5105.83 National Guard Joint Force Headquarters - State (NG JFHQs-State)

DODD 8000.01 Management of the Department of Defense Information Enterprise

DODD 8100.02

Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG)

DODD 8500.01E Information Assurance (IA)

DODD 8521.01E Department of Defense Biometrics DODD O-8530.1 Computer Network Defense (CND)

DOD 5500.07–R Joint Ethics Regulation

DODI 1015.10 Military Morale, Welfare, Recreation (MWR) Programs

DODI 1015.12 Lodging Program Resource Management

DODI 1035.01 Telework Policy

DODI 4640.07 Telecommunications Services in the National Capital Region (NCR)

DODI 8100.04 DOD Unified Capabilities (UC)

DODI 8500.2 Information Assurance (IA) Implementation

DODI 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)

DODI 8560.01 Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing

JP 1-02

Department of Defense Dictionary of Military and Associated Terms (Available at http://www.dtic.mil/doctrine/ new_pubs/jp1_02.pdf.)

Army CIO/G-6 Strategy for End State; Army Network Architecture (Available at http://ciog6.army.mil.)

Secretary of the Army Memorandum

Subj: Information Technology Management Reforms, 9 September 2011 (Available at http://www.apd.army.mil.)

Assistant Secretary of Defense Networks and Information Integration (ASD (NII)) Memorandum Subj: Secure Mobile Environment (SME) Personal Electronic Device (PED) Implementation Guidance (Available at http://ciog6.army.mil.)

Assistant Secretary of Defense Networks and Information Integration (ASD (NII)) Memorandum Subj: Asynchronous Transport Mode (ATM) Phase-Out Plan (Available at http://ciog6.army.mil.)

Association of Public Safety Communication Officials International Project (APCO P25) (Available at http://apcointl.org/spectrum-management/resources/interoperability/p25.html.)

Federal Telecommunications Recommendations Standard (FTR) 1080B–2002 (Available at http://www.ncs.gov/library/fed_rec/FTR%201080B–2002%208–15.pdf.)

Technical Criteria for the Installation Information Infrastructure Architecture (I3A) (Available at https://www.us.army.mil/suite/folder/5745483.)

Unified Capabilities Requirements 2008 (UCR 2008) Change 3 (Available at http://www.disa.mil/Services/Network-Services/UCCO.)

U.S. Comptroller General Decision B-217996

(Available at http://www.gao.gov/.)

10 USC 1588(f)

Authority to Accept Certain Voluntary Services

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 3014 Office of the Secretary of the Army

40 USC Subtitle III Information Technology Management

44 USC 35 Coordination of Federal Information Policy

44 USC 36 Management and Promotion of Electronic Government Services

47 USC 226 Telephone Operator Service

Section III Prescribed Forms This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated below, DA forms are available on the Army Publishing Directorate (APD) Web site at www.apd.army.mil. DD forms are available on the Office of the Secretary of Defense (OSD) Web site at www.dtic. mil/whs/directives/infomgt/forms/index.htm.

DA Form 11–2 Internal Control Evaluation Certification

DA Form 2028 Recommended Changes to Publications and Blank Forms

DD Form 1367 Commercial Communication Work Order

DD Form 1494 Application for Equipment Frequency Allocation

Appendix B Telecommunications Services Authorized for Specific Activities

B-1. U.S. Army National Guard

Installation voice and data services may be provided to off-post ARNG units, activities, and detachments on a reimbursable basis with funding from the ARNG. On-post voice and data services to ARNG units, activities, and detachments will be provided as common-use IT services with funding provided in accordance with the current Army reimbursement policy for common-use IT services. For more information see the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA (FM&C)) Web site at http://www.asafm.army.mil/.

B-2. U.S. Army Reserve

Installation voice and data services may be provided to on-post and off-post U.S. Army Reserve units and activities on a reimbursable basis with funding from the U.S. Army Reserve. When such services are provided, funding will be in accordance with the current Army reimbursement policy for common-use IT services in accordance with the C4IM Services List (for more information, see the ASA (FM&C) Web site at http://www.asafm.army.mil/).

B–3. Reserve Officer Training Corps

Local voice and data services for senior and junior Reserve Officer Training Corps detachments are normally provided by the supported educational institution. Services beyond those provided by the educational institution may be provided by the supporting NEC on a reimbursable basis. The requesting detachments are responsible for ensuring that funds are available through their chain of command. All available services, including Networx contract and equivalent service, will be considered prior to approving commercial service.

B-4. Army Morale, Welfare, and Recreation programs and non-appropriated activities

AR 215–1 defines the Army policy for providing telecommunications services to Army MWR operations. Official electronic communications services, including Class A–2 telephone service, network services, VTC, NIPRNET, and Internet are authorized when used for executive control and essential command supervision and mission command and management functions. Access to other data services may be provided if the capacity exists, and it does not inhibit Army mission-command functions. If the existing telecommunications and network systems do not have the capacity to allow MWR traffic, Theater-level signal commands and NECs will include it in future system upgrades.

a. All MWR directly operated activities will be provided Class A-2 telephone service and data-transfer services (such as administrative, sales, and service) within the confines of this paragraph.

b. MWR commercially contracted concessions will use commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

B-5. Defense Commissary Agency

Official common-user telephone and data services are authorized for use by commissary store activities, when essential to commissary management. Management functions include statistical data gathering and reporting, personnel management, official telecommunications with other Army installations and Government agencies, and procuring contractual services.

a. Class A–3 and C telephone services are provided to CONUS commissary officers, their assistants, and administrative control sections.

b. Class A–4 telephone service is authorized for use by cashiers for the purpose of official telecommunications with the local banking facilities for check collection.

c. Class A-4 telephone service is installed in locations where only cashier personnel have access to the service.

d. Class C telephone service is authorized for managers of meat departments, produce departments, grocery departments, warehouses, and associated commissary annexes. This service is provided on a reimbursable basis, and only in the office of the department, warehouse, and annex managers.

e. At installations where the commissary officer is not authorized to contract for voice and data service, the NEC may provide support for the requirement. In such cases, a host and tenant agreement is executed. Depending on the source of reimbursement, this agreement may be between the NEC and the commissary officer or the area commissary field director.

f. Official common-user communications services are authorized on a nonreimbursable basis for use by commissary stores overseas, including Alaska, Puerto Rico, and Hawaii.

g. If the existing telecommunications and network systems do not have the capacity or would otherwise be adversely impacted by Defense Commissary Agency (DeCA) traffic, ACOMs and NECs will plan to accommodate such traffic in future system upgrades, or otherwise provide right-of-way access and support for the separate acquisition of commercial voice and data telecommunications services for DeCA facilities.

B-6. Army and Air Force Exchange Service

Headquarters, Army and Air Force Exchange Service (AAFES) exchange regions, area exchanges, exchange managers, main store managers, and military clothing sales store operations will be authorized Class A–2 official telephone service in CONUS and OCONUS on a nonreimbursable basis for official business (that is, command management functions). Access to commercial circuits for the conduct of AAFES business will be on a reimbursable basis at Government rates whenever possible. Access to data services, networks, or cable plants will be provided by the installation to accomplish command management functions that require data transfer. These services are on an asneeded basis, provided the capacity exists and it does not inhibit Army mission-command functions. All AAFES directly operated activities are authorized Class C telephone service and data-transfer services (for example, administrative, sales, and service within the confines of this paragraph). AAFES commercially contracted concessions will use

commercial telephone service. Class B service and access to installation data services may be provided if commercial service is not available.

B–7. Contractors

a. Contractors providing resale services related to NAFI operations will use commercial telephone service when available. Class B service may be provided if commercial service is not available. Contractors normally will be provided only proximity access to intra-post Class C service necessary for coordinating local support, and for fire and safety reasons. Contractors normally will not be provided access to data services and networks for the conduct of official business, unless stipulated as a provision of their contract.

b. Contractors providing APF type of support may receive official telephone service. The contracting officer determines whether such service is advantageous to the Government and whether it is mission essential. Authorized service must be specified in the contract as Government-furnished.

c. When official telephone service is authorized, Class A and Class C service may be provided, as determined by the NEC, contracting officer, or contracting officer's representative for specific contracts. NECs will charge the contractor public tariff rates for supplemental services. These services include facilities such as key equipment, special switchboards, private lines, and FX lines for the exclusive use of the contractor. In the absence of tariff rates, or excessive rates, the installation commander determines equitable charges based on the actual cost of providing the services.

d. When the Army furnishes long-distance service from Class B–2 telephones to contractors on a reimbursable basis, the contractor will pay all actual charges and all taxes. Army activities do not provide official Government telephone calling cards to contractors. The procedures for authorizing, controlling, and recording long-distance service also apply to official collect telephone calls that contractor personnel place or receive.

e. The agency funding the contract reimburses the host installation for telephone charges that the contractor incurs. CJCSI 6211.02 provides guidance concerning SBU voice use by U.S. civilian contractor personnel.

B-8. Field operating agencies and direct-reporting units

The following telephone services may be provided to field operating agencies and direct-reporting units located on an Army installation or stationed nearby with agreement:

a. Class A-1 service when performing a military function, to include medical.

b. Class A-2 service when performing a civil works function.

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

d. Access to data services and networks is provided when the capacity exists and does not inhibit Army missioncommand functions already on the network.

B-9. Department of Defense Dependent Schools

Provide Class A-2 and Class C telephone service to Government-operated school facilities for military Family members on an Army installation. Access to other voice and data services is dependent upon local agreements.

B–10. American Red Cross

Provide official voice and data service without reimbursement if American Red Cross personnel supplement MWR functions. The American Red Cross must use separate, unofficial voice and data service to conduct unofficial business.

B-11. Army lodging and temporary duty facilities

The Comptroller General has ruled, "Where sufficient official need exists for a telephone not in private quarters, appropriated funds may be used, regardless of the incidental personal benefit to the occupant." (See DODI 1015.12 for more information.) Therefore, the following guidelines are provided for official telephone service in Army transient facilities. Theater-level signal commands and NECs will—

a. Set controls to ensure that the Army does not pay for unofficial or personal toll calls with appropriated funds, establish controls through system hardware and software configurations if possible, and set up direct toll billing procedures for transient residents.

b. Authorize direct access from transient billets to SBU and the local calling area, when necessary. Appropriated funds must not be used to pay message unit charges accrued for unofficial or personal individual calls to the local area.

c. Implement the requirements detailed in the Telephone Operator Consumer Service Improvement Act (47 USC 226).

B-12. Official telephone service for hospitalized active duty military personnel

A hospital room is the duty location for hospitalized personnel. If capacity exists in the installation telephone infrastructure, Class C telephone service must be provided. The installation NEC has authority to approve a higher class of service or special features.

B-13. Private telephone service for hospital patients

Upon request, the hospital administrator will coordinate infrastructure with the installation NEC for the local telephone company to provide private unofficial telephone service to hospital patients. A contractual agreement for commercial service is solely between the patient and the commercial company providing the service. Local telephone companies will reimburse the installation NEC for any infrastructure used to support private unofficial telephone service to patients. When the Government provides Class B service, the patient must pay the recurring cost plus the cost of individual toll calls.

B–14. Nonprofit organizations

The commander, or appropriate DA civilian supervisor heading an organization within an Army component, may authorize support to certain nonprofit organizations in a manner consistent with the provisions of DOD 5500.07–R. Nonprofit organizations do not pay service charges for Class A or C telephone service on an Army installation when performing a function related to or furthering a Federal Government objective, or one that is in the interest of public health and welfare. Nonprofit organizations will reimburse the installation for all long-distance telephone services. SBU voice access will not be authorized. Access to data services and networks may be furnished, provided the capacity exists and it does not reduce the effectiveness of security or the operational functions of the network. The extent of services will be based upon local agreements.

B-15. Government employee labor unions

Class B-2 rates for telephone services apply to Government employee labor unions. Only reimbursable long-distance telephone services may be provided. Labor unions are not authorized to have SBU voice access. However, access to these and other voice and data services is dependent upon local collective-bargaining agreements.

B–16. Public schools

Public schools normally use commercial voice and data service on Army installations. If commercial service is unavailable, the school reimburses the Government for the cost of Class B services. Access to data services and networks may be furnished, provided the capacity exists and it does not reduce the effectiveness of security or the operational functions of the network. The extent of services will be based upon local agreements.

B-17. Civilian post offices on military installations

Reimbursable voice and data service will be provided to on-base civilian post offices, branches, or stations when requested. The extent of services is dependent upon local agreements.

B–18. Soldiers in the barracks

All private telephone service for Soldiers in barracks will be through the AAFES contract. Other organizations are not authorized to establish telephone service for Soldiers in barracks. Access to other voice and data services is dependent upon local agreements.

B-19. Army Community Service volunteers and Army Family support groups

Army Community Service volunteers and Army Family support groups are authorized to place calls or access email using official Government communications networks (for example, SBU voice and Networx contract) through local operations centers or installation telephone operators, as long as such communications support the APF command support functions (see AR 25–2 for requirements on access to computer systems). Access to data services and networks may be furnished, provided the capacity exists and does not reduce the effectiveness of security or the operational functions of the network. The extent of services will be based upon local agreements.

Appendix C Internal Control Evaluation Checklist

C-1. Function

The functions covered by this checklist are the administration of Army IM and IT organizations. They include key controls for telecommunications and UC.

C-2. Purpose

The purpose of this checklist is to help HQDA, ACOMs, and installations evaluate key internal controls outlined below; it is not intended to cover all controls.

C-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 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

C-4. Test questions

a. Have information system plans, programs, and requirements been coordinated with the appropriate IM/IT managers? (All)

b. Is a process in place to acquire IT and ensure that all required licensing and registration are accomplished? (NEC)

c. Is the NEC the single organization responsible for the oversight and management of installation IT? (NEC)

d. Are periodic reviews of current IT being conducted to ensure they are still required and meet user needs? (HQDA, ACOM)

e. Are quarterly reviews of current IT within the Army Portfolio Management Solution-Army Information Technology Repository being conducted and verified by the users, and are they still required and meet user needs? (HQDA, ACOM)

f. Are evaluations being conducted of existing systems for obsolescence? (HQDA, ACOM)

g. Has a business care analysis (BCA) been performed prior to implementing the thin client concept? (NEC)

h. Is an accurate inventory being maintained and validated annually for IT equipment? (NEC, IMO)

i. Are continuation of operations (COOPs) and procedures documented, distributed, and tested at least annually? (ACOM, NEC)

j. Has guidance been provided to ensure that all software is checked for viruses before being loaded? (NEC)

k. Are existing capabilities and assets considered prior to upgrading, improving, or implementing local area networks (LANs)? (Theater-level signal command, NEC)

l. Are uneconomical IT service contracts identified and terminated? (All)

m. Has the NEC coordinated the acquisition of licenses with the CHESS office prior to entering into an agreement with a COTS vendor? (NEC)

n. Are spare capacity and the functional expansion of IT being considered or used when new requirements are identified? (All)

o. Has the NEC reported its server consolidation status for all of its Army tenants to the Army CIO/G-6? (NEC)

p. Are measures being taken to ensure that hard drives are disposed of properly? (NEC)

q. Are criteria established to justify and approve the acquisition of multifunction mobile devices, cellular phones, and pagers? (Theater-level signal command, NEC)

r. Has guidance been provided to review and revalidate multifunction mobile devices, cellular phones, and pagers every two years? (Theater-level signal command, NEC)

s. Do procedures require the establishment of a reutilization program to identify and turn in multifunction mobile devices, cellular phones, and pagers that are no longer required or seldom used? (Theater-level signal command, NEC)

t. Is there a requirement for multifunction mobile devices, cellular phones, and pagers to be recorded in the property book? (Theater-level signal command, NEC)

u. Has the NEC implemented accountable billing procedures? (NEC)

v. Have maintenance and support strategies been devised to minimize overall systems life-cycle costs at an acceptable level of risk? (program executive officer (PEO), PM, ACOM)

w. Have program managers, project managers, and IT MATDEVs coordinated their system architectures and fielding plans with the gaining commands, DRUs, Theater-level signal commands, and installation NECs prior to fielding systems? (PEO, PM)

x. 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, IMO)

y. Are private-sector service providers made aware that written assurance of compliance with software copyright laws may be required? (Theater-level signal command, NEC, IMO)

C-5. Supersession

This checklist replaces the checklist for the administration of Army telecommunications and UC previously published in AR 25–1.

C-6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to CIO/G-6 (SAIS-PR) at cio-g6. policy.inbox@mail.mil or to 107 Army Pentagon, Washington, DC 20310-0107.

Glossary

Section I Abbreviations

AAE Army acquisition executive

AAFES Army and Air Force Exchange Service

ACOM Army command

ACP Allied Communication Publication

ACSIM Assistant Chief of Staff for Installation Management

AEA Army Enterprise Architecture

AKO Army Knowledge Online

AKO–S Army Knowledge Online SIPRNET

APF appropriated funds

AR Army Regulation

ARNG Army National Guard

ASA (ALT) Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASA (FM&C) Assistant Secretary of the Army (Financial Management and Comptroller)

ASCC Army service component command

ASD (NII) Assistant Secretary of Defense (Networks and Information Integration)

ATD Army Telecommunications Division

BASECOM base communications

BCA business care analysis

BPA blanket purchase agreement

C4IM

command, control, communications, computers and information management

CAC common access card

CAR Chief, Army Reserve

CCA Clinger-Cohen Act

CCTV closed circuit television

CG commanding general

CHESS Computer Hardware, Enterprise Software Solutions

CIO Chief Information Officer

CJCSI Chairman, Joint Chiefs of Staff instruction

CNDSP computer network defense service provider

COMSEC communications security

CONUS continental United States

COOP continuation of operations

COTS commercial off-the-shelf

CSA communications service authorization

CSLA Communications Security Logistics Activity

DA Department of the Army

DAA designated approval authority

DA Pam Department of the Army Pamphlet

DCS Deputy Chief of Staff **DeCA** Defense Commissary Agency

DISA Defense Information Systems Agency

DISAC Defense Information Systems Agency Circular

DISN Defense Information Systems Network

DKO Defense Knowledge Online

DMS Defense Message System

DOD Department of Defense

DODD Department of Defense directive

DODI Department of Defense instruction

DRU direct reporting unit

DSN defense switched network

EA enterprise architecture

EID enterprise identifier

EO Executive Order

FAR Federal Acquisition Regulation

FM frequency modulation

FX foreign exchange

FY fiscal year

GETS Government Emergency Telecommunication Service

GIG Global Information Grid GPS Global Positioning System

HMW health, morale, and welfare

HQ headquarters

HQDA Headquarters, Department of the Army

HTML hypertext markup language

I3MP
Installation Information Infrastructure Modernization Program

IA information assurance

IATO interim approval to operate

IM information management

IMO information management officer

Inmarsat International Maritime Satellite

IP Internet protocol

IS Information System

ISDN integrated services digital network

ISP Internet service provider

IT information technology

JCS Joint Chiefs of Staff

JFHQs-State Joint Forces Headquarters-State

JITC Joint Interoperability Test Command

JWICS Joint Worldwide Intelligence Communication System **kHz** kilohertz

LAN local area network

MARS Military Affiliate Radio System

MATDEVS material developers

MHz megahertz

MILSATCOM Military Satellite Communications

MWR morale, welfare, and recreation

NAF nonappropriated fund

NAFI nonappropriated fund instrumentalities

NATO North Atlantic Treaty Organization

NCR National Capital Region

NEC Network Enterprise Center

NETCOM Network Enterprise Technology Command

NetOps network operations

NGB National Guard Bureau

NIPRNET non-secure Internet protocol router network

NSA National Security Agency

O&M operation and maintenance

OCONUS outside the continental United States

OSD Office of the Secretary of Defense **P.L.** Public Law

Pam pamphlet

PBD program budget decision

PC personal computer

PDA personal digital assistant

PEO program executive officer

PKI Public Key Infrastructure

PM program manager

POC point of contact

POM program objective memorandum

PPS precise positioning service

PSTN Public Switched Telephone Network

RC records coordinator

RM records manager

SATCOM satellite communications

SBU sensitive but unclassified

SCI sensitive compartmented information

SDB satellite database

SIPRNET secure Internet protocol router network

STE secure telephone equipment

T&E testing and evaluation

TCO telephone control officer

TSP telecommunications service priority

URL uniform resource locator

USC United States Code

USSTRATCOM United States Strategic Command

VTC video teleconference

WGS wideband global satellite

XML eXtensible markup language

Section II Terms

Activity

An Army organization. Within the context of the Army Enterprise Architecture (AEA), a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes to support the accomplishment of tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element.

Architecture

See enterprise architecture and Army enterprise architecture.

Army business enterprise architecture

The framework of business processes and organizations that support the Army's Soldiers.

Army 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 ISs and national security systems that implement horizontal IT insertions, cutting across functional stovepipes and Service boundaries. The AEA supports the LandWarNet and is the combined total of all of the Army's operational, technical, and system architectures.

Army enterprise infrastructure

The systems and networks that comprise the LandWarNet.

Army knowledge management

The Armywide strategy is to transform the Army into a network-centric and knowledge-based force to improve information dominance by our Soldiers 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 with Joint, coalition, and international partners as mission needs dictate.

Army Reserve Network II

ARNet II is a separate network providing LandWarNet services that connect the USAR to the DISA GIG.

Army Web site

A collection of hypertext markup language (HTML) pages, graphics, images, video, audio, databases, or other media assets at a Uniform Resource Locator (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, PDAs or interactive television; and whose content is controlled, authorized, or sponsored by an Army organization or representative.

Broadcast

The transmission of radio, television, and data signals through the air waves or fiber-optic cable.

C4IM Services List

The source document that defines the Army enterprise baseline and mission IT services provided or supported by the directorate of information management. This list of service definitions is the foundation for the development and publishing of the LandWarNet Services Catalog. The C4IM services listed as "baseline" are core or common-user services that are the responsibility of the Army to centrally fund. Services listed as "mission" are the responsibility of ACOMs or 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 so forth) and are grounded by the business processes that enable mission execution in a more efficient and effective manner.

Cable television system

A facility consisting of a set of closed-transmission paths and associated signal generation, reception, and control equipment designated to provide cable service that includes both audio and video programming provided to multiple subscribers.

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.

Class A (official) telephone service

Telephone service authorized for the transaction of official business of the Government on DOD or military installations; requires access to commercial telephone company central office and toll trunks for the proper conduct of official business.

Class B (unofficial) telephone service

Telephone service installed on or in the immediate vicinity of a DOD/military installation served through a military Private Branch Exchange or Central Exchange system through which the conduct of personal or unofficial business is authorized. This telephone service has access to commercial telephone company central office and toll trunks.

Class C (official-restricted) telephone service

Telephone service authorized for the transaction of official business of the Government on a DOD/military installation and without access to Telephone Company central office or toll trunks.

Class D (official-special) telephone service

Telephone service installed on military installations for official business of the Government and restricted to special classes of service, such as fire alarm, guard alarm, and crash alarm.

Closed circuit television

Point-to-point signal transmission by cable or directional radiation where the audience is limited by physical control or nonstandard transmission.

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 cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Communications systems

A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

Compatibility

The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

Compliance

A system that meets, or is implementing an approved plan to meet, all applicable 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 manufacture, assembly, maintenance, or rebuild.

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.

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.

Defense Telephone System

A centrally managed system that provides telephone service to all DOD activities in the area, in accordance with its charter.

Doctrine

Fundamental principles by which 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.

Electronic mail

An information dissemination and retrieval service accessed through distributed user workstations normally provided through office automation initiative.

Enterprise

The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise architecture

A strategic information asset base, which defines the mission, the 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 baseline architecture, target architecture, and a sequencing plan (44 USC 3601).

Enterprise identifier

A 64-bit information identification tag (key) that remains unique across an enterprise. Each enterprise identifier (EID) is composed of a 32-bit EID seed followed by a 32-bit sequence determined by the EID server.

Enterprise information environment

The common, integrated computing and communications environment of the GIG. The enterprise information environment (EIE) is composed of GIG assets that operate as, or that assure, LANs, campus area networks, tactical networks, operational area networks, metropolitan area networks and wide area networks. The EIE is also composed of GIG organizational, regional, or global computing capabilities. The EIE includes all software associated with the operation of EIE assets, the development environments, and user productivity tools used in the GIG. The EIE includes a common set of enterprise services called Core Enterprise Services, which provide awareness and delivery of information on the GIG.

eXtensible Markup Language

A tagging language used to describe and annotate data so that data can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. XML also uses semantically rich labels to describe elements and attributes to enable meaningful comprehension.

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.

Federated architecture

An approach for EA development that is composed of a set of a coherent but distinct entity or architectures. The architectures of separate members of the federation. The members of the federation participate to produce interoperable, 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.

GuardNet

GuardNet is the IT infrastructure of the National Guard, securely supporting the NGB Joint team with nationwide ISs and mission-command networks that span 11 time zones and 54 States, Territories, and the District of Columbia at approximately 3,000 separate locations. GuardNet provides ARNG access to the Army's LandWarNet and Joint access to Air Force network services in these States.

Global Information Grid

The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to Soldiers, policy makers, and support personnel.

Hardware

The generic term that deals with physical items distinguished from a capability or function (for example, 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, hardware is the physical equipment or devices forming computer and peripheral components. (Also see software.)

Information

The meaning that humans assign to data by means of the known conventions used in their representations (see JP 1-02). Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights.

Information management

Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information management office or officer

The office or individual responsible to the respective commander, director, or chief 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 manage the organization's IT and IM processes and resources that enable the organization's business and mission processes.

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 the 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. This 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 system

The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of the Army Portfolio Management Solution-Army Information Technology Repository, the terms "application" and "information system" are used synonymously; and are defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The application of IT to solve a business or operational (tactical) problem creates an IS.

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 lead agency. For purposes of the preceding sentence, equipment is used by a lead agency if the equipment is used directly or is used by a contractor under a contract with the lead agency that 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 acquired by a Federal contractor incidental to a Federal contract (See 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.

Infrastructure

The shared computers, ancillary equipment, software, firmware and similar procedures, services, people, business processes, facilities (to include 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 other supported activities outside the perimeter of the military installation, which also depend on the installation for support.

Internet

An electronic communications network that connects computer networks and organizational computer facilities around the world.

Internet service provider

An organization that provides other organizations or individuals with access to, or presence on, the Internet. Most ISPs also provide extra services including help with the design, creation, and administration of Internet sites; and training and administration of Intranets.

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.

IPv4-interoperable

An IPv6-capable system or product capable of receiving, transmitting, and processing Internet Protocol version 4 (IPv4) packets.

IPv6-capable

A system or product meeting the minimal set of DOD Information Technology Standards and Profile Registry mandated requirements (appropriate to the product class) necessary to be interoperable with other IPv6-capable products in DOD deployments.

IPv6-enabled

IPv6-capable systems or products with the IPv6 functionality turned on, implying that IPv6 packets can be properly processed by that system or product or component.

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.

Intra-Army interoperability certification

Confirmation 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.

Intranet

A computer network that functions like the Internet, using Web browser software to access and process the information that employees need, and located on computers within the organization or enterprise. A firewall is usually used to block access from outside the Intranet. Intranets are private Web sites.

Land Warrior Network

Combination of infrastructure and services across the Army. It provides for processing, storing, and transporting information over a seamless network.

Land mobile radio systems

Antennas, consoles, switches, repeaters, hand-held radios, vehicular-mounted radios, and associated components of non-tactical radio frequency systems that operate in the bands 138–150.8 megahertz (MHz), 162–174 MHz, 380–399.9 MHz, and 406.1–420 MHz.

Life cycle

The total phases through which an item progresses from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

Machine readable

Data and information storage media requiring the use of one or more IS component(s) for translation into a medium understandable and usable to humans.

Master or community antenna television system

A facility consisting of a television reception service that receives broadcast radio frequency television signal and frequency modulation (FM) radio programs and distributes them via signal generation, reception, and control equipment.

Message (telecommunications)

Recorded information expressed in plain or encrypted language and prepared in a format specified for intended transmission by a telecommunications system.

Mission command

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 employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Mission command system

System of facilities, equipment (including hardware, firmware, and software), communications, procedures, and personnel available to commanders at all echelons and in all environments that are essential to plan, direct, and control operations conducted by assigned resources.

Mission-critical information system

A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act, the loss of which would cause the stoppage of Soldier operations or direct mission support of Soldier operations.

Mission-essential information system

A system that meets the definitions of "information system" and "national security system" in the Clinger-Cohen Act,

which the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The definition of "organizational mission" is one of the organizational missions of the Army; not just a single command or DA functional proponent.)

Narrowband operation

Equipment in the frequency bands 138–150.8 MHz, 162–174 MHz, 380–399.9 MHz, and 406.1–420 MHz operating in 12.5 kilohertz (kHz) or less of necessary bandwidth as defined by the National Telecommunications and Information Administration.

National security system

Any telecommunications or IS operated by the U.S. Government, and the function, operation, or use of which involves: 1) intelligence activities; 2) cryptologic activities related to national security; 3) mission command of military forces; 4) equipment that is an integral part of a weapon or weapons system; or 5) activities critical to the direct fulfillment of military or intelligence missions (ref. 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 on 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.

Nonappropriated fund(s)

Cash and other assets received from sources other than monies appropriated by the Congress of the United States. (NAFs must be resources of an approved NAFI.) NAFs are U.S. Government funds, but they are separate and apart from funds that are recorded in the books of the Treasury of the United States. They are used for the collective benefit of the authorized patrons who generate them.

Nonappropriated fund instrumentalities

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.

Organizational messaging

Correspondence that is 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.

Planning, programming, budgeting, and execution process

The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Process

A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place; with a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process owners

HQDA functional proponents, ACOMs, and others who have responsibility for any mission-related or administrative work process.

Procurement or 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.

Publicly accessible Web site (or public Web site) on the World Wide Web

Army Web site with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a Web site through a browser.

Satellite communications

DOD use of military-owned and 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. 01D).

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.

Sensitive compartmented information

SCI consists of information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. SCI encompasses communications intelligence and Special Activities Office information and materials.

Software

A set of computer programs, procedures, and associated documentation concerned with the operation of a dataprocessing system (for example, compiler, library routines, manuals, and circuit diagrams); and usually contrasted with hardware.

Support agreement

An agreement to provide recurring common-use IT services to another DOD or non-DOD Federal activity.

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 and defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (that is, the application of IT).

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.

Thin client

The use of client-server architecture networks that depend primarily on the central server for processing activities, and 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.

Ubiquitously

Having or seeming to have the ability to be everywhere at once; omnipresent.

Unified capabilities

The integration of voice, video, or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the Soldier and business communities.

UC transport

The secure and highly available enterprise network infrastructure used to provide voice, video, or data services through a combination of DOD and commercial terrestrial, wireless, and satellite communications capabilities.

Uniform resource locator

The Web address a person uses to direct a browser program to a particular Internet resource (for example, a file, a Web page, and an application). All Web addresses have a URL.

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 table of distribution and allowances command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, or otherwise applying doctrine, organization, training, materiel, leadership and education, personnel, and facilities products in 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, two-way voice, or one-way video; and includes full-motion video, compressed video, and sometimes freeze (still) frame video.

Web portals

Web sites that serve as starting points to other destinations or activities on the Web. Initially thought of as a "home base" type of Web page, portals attempt to provide all of a user's Internet needs in one location. Portals commonly provide services such as email, collaboration centers, online chat forums, searching, content, and newsfeeds.

Web site

A location on the Internet; specifically, it refers to the point of presence location in which it resides. All Web sites are referenced using a special addressing scheme called a URL. A Web site can mean a single HTML file or hundreds of files placed on the Internet by an enterprise.

World Wide 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 called the "Web").

Section III Special Abbreviations and Terms

APL approved product list

ARNet II Army Reserve Network II

AS–SIP Assured Services Session Initiation Protocol

ASLAN Assured Service Local Area Network

ASMO Army Spectrum Management Office

ATM asynchronous transport mode

ATO approval to operate

CMI classified message incident

COMSATCOM

commercial satellite communications

DDOE

Defense Information Systems Agency Direct Order Entry

DITCO

Defense Information Technology Contracting Organization

DRSN

Defense Red Switch Network

DSAWG

Defense Security and Information Assurance Working Group

DVS

Defense Information Systems Network Video Services

EIE

enterprise information environment

FSS fixed satellite service

FTS Federal Telecommunications Service

GuardNet Army National Guard Network

IMCOM Installation Management Command

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

JF Joint force

LandWarNet land warrior network

LMR land mobile radio

LSC local session controllers

MSS mobile satellite service

NTIA National Telecommunications and Information Association

PAO public affairs official PED portable electronic device

SME secure mobile environment

SPS standard positioning service

STIG Security Technical Implementation Guide

TA terminal administrator

TDM time-division multiplex

TLA top-level architecture

UC unified capabilities

UCR unified capabilities requirements

USGv6 U.S. Government version 6

VEUE Virtual End User Environment

VoIP Voiceover Internet Protocol

VoSIP Voiceover Secure Internet Protocol

WPS Wireless Priority Service

UNCLASSIFIED

PIN 103366-000