

**Army Regulation 25–13**

**Information Management**

# **Army Telecommunications and Unified Capabilities**

**Headquarters  
Department of the Army  
Washington, DC  
11 May 2017**

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

AR 25–13

Army Telecommunications and Unified Capabilities

This major revision, dated 11 May 2017—

- o Incorporates responsibilities of U.S. Army Cyber Command as required by Headquarters, Department of the Army General Order No. 2017–01. This general order established U.S. Army Cyber Command as a direct reporting unit of the Chief Information Officer/G-6. U.S. Army Network Enterprise Technology Command, formerly a direct reporting unit of the Chief Information Officer/G–6, Headquarters, Department of the Army, is assigned to U.S. Army Cyber Command (throughout).
- o Provides guidance for the management of bandwidth utilization and the reduction and removal of nonessential (non-mission) data, voice, and video communications traffic in times of surge or crisis (para 3–5).
- o Incorporates guidance for the transition of services away from Integrated Services Digital Network equipment and transport; and provides policy concerning the reduction and elimination of investment in Integrated Services Digital Network supported technology (para 4–4).
- o Incorporates guidance and process for voice precedence (flash override, flash immediate, and priority) service requests and requirements submission (para 4–5a(5)).
- o Provides guidance for the management, reporting, and personnel accountability of video teleconferencing services (para 4–6).
- o Provides additional guidance on the procurement and use of next-generation Department of Defense wireless services and devices under wireless enterprise blanket purchase agreements in order to align with current policy; and deletes the secure mobile environment portable electronic device (para 4–8c(1)).
- o Replaces “Global Information Grid waiver” references with “Department of Defense Information Network waiver” and provides additional guidance consistent with current Department of Defense Information Network waiver policy, process, and procedure; and provides additional guidance on the multiple type of waivers (para 6–3 and throughout).
- o Incorporates guidance for the Unified Capabilities Approved Product List Removal List (para 7–3).
- o Incorporates guidance for unclassified and secret level voice services being provided by either Defense Information Systems Agency or Army; and corrects Command, Control, Communications, Computers and Information Management services to two service categories (para 7–4).
- o Incorporates guidance for installation of Assured Service Local Area Network services (para 7–7).
- o Identifies the web-based Army Information Technology Approval System as the replacement for the Goal 1 Waiver system (throughout).


**Information Management**  
**Army Telecommunications and Unified Capabilities**

---

By Order of the Secretary of the Army:

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

Official:

  
**GERALD B. O'KEEFE**  
*Administrative Assistant to the*  
*Secretary of the Army*

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

**Summary.** This regulation establishes policies and assigns responsibilities for the management of telecommunications and unified capabilities. It applies to information technology contained in business systems and national security systems (except as noted) developed for, or purchased by, the Department of the Army. It implements the provisions of Title 10, United States Code, Sections 2223 and 3014; Title 40 United States Code, Subtitle III, Clinger-Cohen Act; Title 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 described 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 nonjudicial 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, or above. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

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

**Supplementation.** Supplementation of this regulation and establishment of agen-

cy, command, and installation forms are prohibited without prior approval from the Chief Information Officer/G–6 (SAIS–PRU), 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–PRU), 107 Army Pentagon, Washington, DC 20310–0107.

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

**Distribution.** This regulation is available in electronic media only and is intended for command levels A, 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

---

\*This regulation supersedes AR 25–13, dated 25 March 2013.

## Contents—Continued

Explanation of abbreviations and terms • 1–3, *page 1*

Responsibilities • 1–4, *page 1*

### Chapter 2

#### Responsibilities, *page 1*

Assistant Secretary of the Army for Acquisition, Logistics and Technology • 2–1, *page 1*

Chief Information Officer/G–6 • 2–2, *page 1*

Chief, National Guard Bureau • 2–3, *page 2*

Chief, Army Reserve • 2–4, *page 3*

Chief, U.S. Army Corps of Engineers • 2–5, *page 3*

Commanders and activity heads of Army commands, Army service component commands, and direct reporting units • 2–6, *page 3*

### Chapter 3

#### Utilization of telecommunications and unified capabilities, *page 5*

Official uses of telecommunications and computing systems • 3–1, *page 5*

Unauthorized and prohibited uses of telecommunications and computing systems • 3–2, *page 6*

Communications monitoring and recording • 3–3, *page 6*

Leasing of Government-owned telecommunications assets • 3–4, *page 7*

Bandwidth utilization management (minimize) • 3–5, *page 7*

Information technology support for telework • 3–6, *page 8*

Military construction communication systems policy • 3–7, *page 8*

Architectures • 3–8, *page 8*

### Chapter 4

#### Telecommunications Systems and Services, *page 8*

Applicability • 4–1, *page 8*

Time-division multiplex equipment • 4–2, *page 8*

Asynchronous transport mode equipment • 4–3, *page 9*

Integrated services digital networking • 4–4, *page 9*

Telephone systems • 4–5, *page 9*

Video services • 4–6, *page 11*

Commercial television service • 4–7, *page 12*

Multifunction mobile devices • 4–8, *page 13*

Wireless priority service and wireline government emergency telecommunications service • 4–9, *page 15*

Non-tactical radio systems • 4–10, *page 15*

### Chapter 5

#### Satellite Communication Systems and Position Navigation and Timing, *page 16*

General • 5–1, *page 16*

Commercial satellite communication annual usage report • 5–2, *page 16*

Satellite communication requirements • 5–3, *page 16*

Use of wideband military satellite communications • 5–4, *page 17*

Satellite communication standardization • 5–5, *page 17*

Network command operations of military satellite communication systems • 5–6, *page 17*

Army component command to United States Strategic Command • 5–7, *page 17*

International Maritime Satellite and Iridium • 5–8, *page 17*

Position, navigation, and timing global positioning system, precise positioning service, and standard positioning services • 5–9, *page 18*

### Chapter 6

#### Long-Haul and Deployable Telecommunications, *page 18*

General • 6–1, *page 18*

Mission partner and defense contractor connections to the Defense Information Systems Network • 6–2, *page 19*

Department of Defense Information Network waivers • 6–3, *page 20*

Military telecommunications agreements • 6–4, *page 21*

## Contents—Continued

### Chapter 7

#### **Unified Capabilities**, *page 22*

Introduction • 7-1, *page 22*

General • 7-2, *page 23*

Unified capabilities approved product list • 7-3, *page 23*

Voice services • 7-4, *page 23*

Video telecommunication services • 7-5, *page 25*

Collaboration capabilities • 7-6, *page 25*

Installation information infrastructure • 7-7, *page 26*

### Appendixes

**A.** References, *page 27*

**B.** Telecommunications Services Authorized for Specific Activities, *page 31*

**C.** Internal Control Evaluation, *page 35*

### Glossary



## **Chapter 1 Introduction**

### **1–1. Purpose**

This regulation establishes Department of the Army (DA) policies and assigns responsibilities for the management of telecommunications and unified capabilities (UC). It implements the provisions of Title 10, United States Code (10 USC) Sections 2223 and 3014; 40 USC Subtitle III, Clinger-Cohen Act; 44 USC 35; 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**

See appendix A.

### **1–3. Explanation of abbreviations and terms**

See the glossary.

### **1–4. Responsibilities**

See chapter 2.

## **Chapter 2 Responsibilities**

### **2–1. Assistant Secretary of the Army for Acquisition, Logistics and Technology**

The ASA (AL&T) will —

*a.* Monitor and account for equipment from production to transfer onto appropriate command accounts (from production to in-service, or to in-storage/inventory). Commands will maintain and account for physical inventory of UC and telecommunications equipment.

*b.* Assist the Chief Information Officer (CIO)/G–6, using an engineering-based approach, to determine current and future bandwidth requirements for circuits that connect installations to the Department of Defense Information Network (DODIN).

### **2–2. Chief Information Officer/G–6**

The CIO/G–6 is the senior Army authority for telecommunications and UC. The CIO/G–6 will —

*a.* Serve as senior Army authority for Joint Staff-controlled mobile and transportable telecommunications assets.

*b.* Oversee the Army Spectrum Management program. This includes the coordination and use of radio frequency resources within the United States and its possessions and the registration and processing of spectrum-dependent systems through the Army Spectrum Certification Program.

*c.* Advise the planning, programming, budgeting, and executing of resources to support enterprise-level telecommunications and network services, such as the Defense Information Systems Network (DISN) Subscription Service.

*d.* Integrate policy, oversight, and guidance to achieve Army communications objectives in the Army information environment.

*e.* Review and provide subject matter expertise on information technology (IT), telecommunications, and UC unfunded requirements submitted by commands to CIO/G–6 for potential procurement funding.

*f.* Generate requirements for enterprise-wide telecommunications and UC services.

*g.* Provide the appropriate level representative to the following working groups, forums, and boards:

- (1) Participant and voting member of the Military Communications-Electronics Board.
- (2) Participant and voting member of the DOD Unified Capabilities Steering Group.
- (3) Participant and voting member in the Defense Information Assurance Security Accreditation Working Group (DSAWG), reference the DSAWG home page at <http://www.disa.mil/services/network-services/enterprise-connections/dsawg>.
- (4) Participant and voting member in the Defense Information Systems Agency (DISA) Customer Forum.
- (5) Participant and voting member of the DOD Interoperability Steering Group.

(6) Serve as the Army voting member of the Satellite Communications (SATCOM) Gateway Configuration Control Working Group.

(7) Participant in the DOD Unified Capabilities Industry Advisory Council.

*h.* Delegate to Commander, U.S. Army Cyber Command (USARCYBER) all infrastructure management activities, tactics, processes, procedures, and protocols for the management of infrastructure assets such as Army networks, UC, telecommunications, installation facilities, data storage, IT services continuity, and mid-range and mainframe computing. Commander, USARCYBER will —

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

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

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

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

(5) Submit approved requests for UC and telecommunications services to DISA for coordination and implementation.

(6) Coordinate with individual camps, posts, and stations that have a Network Enterprise Center (NEC) or NEC-like responsibility within their respective geographic locations as outlined in this regulation.

(7) In conjunction with the Signal Theater Commands, Signal Brigades, and NECs, review and revalidate all expired communications service authorizations (CSAs), regardless of the user.

(8) 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 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 DISA in representing U.S. interests within NATO communications forums.

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

*(g)* Identify and validate unique critical communications circuit requirements considered vital to the Army and submit them to the Joint Staff via CIO/G-6 (SAIS-AOI).

*(h)* In conjunction with the Signal Theater Commands, Signal Brigades, and NECs, review and revalidate all expired CSAs, regardless of the 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), Voice over Internet Protocol (VoIP), Voice over Secure Internet Protocol (VoSIP), and Joint Worldwide Intelligence Communication System (JWICS)). DISA reviews validated and expired CSAs, and the information is used to determine if the circuit is still required. If the circuit is no longer required, the NEC will work with DISA and the vendor to terminate/discontinue the circuit and ensure any billing has also stopped. Refer to AR 25-2 for applicable cybersecurity policy and governance.

*(i)* Require Network Enterprise Technology Command (NETCOM) to monitor and record/validate all telecommunications and UC equipment on the network to commands. NETCOM will maintain inventory numbers.

### **2-3. Chief, National Guard Bureau**

The CNGB is responsible for all National Guard matters between the DA and the States, and will—

*a.* Collaborate with the National Guard Bureau (NGB), CIO/G-6, USARCYBER and the Joint Force Headquarters-State (JFHQs-State) 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.

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

*c.* Appoint the Director, ARNG as the authorizing official for GuardNet.

*d.* Oversee organizations that operate and maintain GuardNet, a separate network providing Land Warrior Network (LandWarNet) services to states, territories, and the District of Columbia, which also connects the ARNG to the DISA DODIN. This includes, but is not limited to —



(1) Planning and programming UC resources to support NGB and JFHQs–State UC requirements, as required by the CNGB; CIO/G–6; CG, USARCYBER; Adjutants General of the States and Territories; and the CG of the District of Columbia.

(2) 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.

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

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

(5) Executing ARNG leases of communications and UC solutions and services to ensure that those services conform to NGB, CIO/G–6, and USARCYBER guidance in collaboration with the JFHQs–State, where applicable.

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

(7) Providing subject-matter expertise in negotiations and collaborations with the NGB, HQDA CIO/G–6, USARCYBER, and JFHQs–State concerning recognized requirements.

(8) Managing GuardNet-specific, system-to-system interfaces between the states and the DA in collaboration with the JFHQs–State where applicable.

(9) Identifying and validating unique, critical communications requirements considered vital to the NGB and ARNG in collaboration with the JFHQs–State (where applicable), and submitting these requirements to CIO/G–6, USARCYBER.

(10) Collaborating with the JFHQs–State Directorates of Information Management, which have NEC-like responsibilities within their respective states as outlined in this regulation.

#### **2–4. Chief, Army Reserve**

The CAR will —

*a.* Serve as the designated lead agent for the Army Reserve Network II (ARNet II), to include—

(1) Planning, programming, budgeting, and executing resources to support ARNet II capabilities, as required by CIO/G–6 and Commanding General (CG), USARCYBER.

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

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

(4) Formulating, managing, supporting, and approving written agreements, where applicable.

*b.* Designate a single NEC responsible for support of all facilities and infrastructure.

#### **2–5. Chief, U.S. Army Corps of Engineers**

The USACE will —

*a.* Assign roles and responsibilities to the USACE CIO as the designated lead agent for the CorpsNet, to include—

(1) Planning, programming, budgeting, and executing resources to Support CorpsNet capabilities, as required by CIO/G–6 and CG, USARCYBER.

(2) Directing all infrastructure management activities, policies, procedures, and protocols for management of the CorpsNet.

(3) Exercising technical and configuration management authority for CorpsNet, USACE specialized systems, and functional processing centers.

(4) Formulating, managing, supporting, and approving written agreements, where applicable.

*b.* Designate two primary NECs responsible for supporting all USACE facilities and infrastructure.

*c.* Serve as the authorizing official (formerly known as designated approval authority) for all USACE systems.

#### **2–6. Commanders and activity heads of Army commands, Army service component commands, and direct reporting units**

The responsibilities listed in this section do not apply to organizations that do not use or are exempted from using traditional Army funds to purchase IT equipment based on compliance with special or higher-level regulations or policies. Commanders and activity heads of ACOMs, ASCCs, and DRUs will —

*a.* Establish procedures to ensure —

(1) All data, video, and voice-switching hardware and software being considered for acquisition are on the UC Approved Product List (APL) found at <https://aplits.disa.mil/processaplist.do>; or available from the Computer Hardware, Enterprise Software and Solutions (CHESS) catalog before procuring these items. The CHESS catalog can be found at <https://chess.army.mil>.

(2) Contracting officers, resource managers, and acquisition officials ensure compliance with the use of enterprise service agreements/enterprise license agreements (ESA/ELA), in accordance with AR 25-1. Trusted Agents must be appointed prior to procurement and download of software using ESA/ELA through the CHESS portal.

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

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

(5) Information managers (or designated telephone control officers (TCOs)) review and validate bills when received from the service provider, which are certified by users for toll-free service, multifunction mobile devices, pager service, cellular phone service, calling card usage, long-distance commercial calls, and commercial lines.

(6) Review and revalidation of DOD physical inventory includes an analysis of leased and Government-owned, long-haul telecommunications circuits, services, and equipment.

(7) The coordination and use of radio frequencies for spectrum-dependent systems is in accordance with AR 5-12.

(8) Coordination of spectrum supportability risk assessments (SSRA) of non-program of record procured emitters in accordance with AR 5-12, when required.

(9) Organizational telecommunications and UC inventory are updated annually and verified accurately.

(10) Procurement of telecommunications/UC/IT equipment is conducted in accordance with policies established in Army Federal Acquisition Regulations (AFARS) Part 5139, AFARS Appendix EE (for Government Credit Card Purchases), AR 710-2, and AR 735-5.

(11) Organizations establish formal accountability of newly acquired telecommunications/UC/IT equipment in an Accountable Property System of Record, in accordance with AR 710-2 and AR 735-5.

*b.* Review long-haul, common-user transmission requirements and forward all requirements not needing CIO/G-6, combatant command, Joint Staff, or Office of the Secretary of Defense (OSD) approval to USARCYBER 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.

*c.* Review and submit, as delegated by the supported combatant commander, requirements for service with the information prescribed in DISA Circular (DISAC) 310-130-1.

*d.* Program, budget, fund, and provide support for assigned portions of the DISN through the planning, programming, budgeting, and execution process, to include approved contractor and foreign government systems.

*e.* Provide and/or coordinate 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.

*f.* In coordination with the services Theater Signal Command, ensure that information security, communications security (COMSEC), emissions security (formerly known as TEMPEST), physical security measures, and installation requirements conform to Army and DISN security policy.

*g.* In coordination with the services Theater Signal Command, ensure that approved systems use DISN services to meet mission requirements, and ensure compliance with Army and DISN policies and procedures, in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02.

*h.* In coordination with the services Theater Signal Command, 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 combatant commander will be forwarded to the Joint Staff for resolution.

*i.* In coordination with the services Theater Signal Command, 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.

*j.* In coordination with the services Theater Signal Command, provide requisite site support for DISN equipment located on their respective posts, installations, or the equivalent. DISA will specify site support requirements in appropriate procedural documentation and coordinated with the Services and defense agencies. Required support 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.

k. In coordination with the services Theater Signal Command, complete required annual inventory of unclassified voice switches.

(1) Commands will complete the annual inventory requirement by registering all current and new switches in the System Network Approval Process (SNAP) database (See DISA's Network Services Enterprise Connection Division DISN Connection Process Guide at [http://www.disa.mil/network-services/enterprise-connections/~media/files/disa/services/disn-connect/references/disn\\_cpg.pdf](http://www.disa.mil/network-services/enterprise-connections/~media/files/disa/services/disn-connect/references/disn_cpg.pdf)). This includes switches that are able to make or receive sensitive but unclassified (SBU) voice, multilevel secure voice, or public switched telephone network (PSTN) calls and is technology independent (for example, waived Time-Division Multiplex (TDM), VoIP, VoSIP, Local Session Controllers and Failover Session Controllers).

(2) Commands will complete the annual inventory requirement by reviewing and updating the current information previously entered in the SNAP 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); authorizing official; and phone numbers).

## **Chapter 3**

### **Utilization of telecommunications and unified capabilities**

#### **3-1. Official uses of telecommunications and computing systems**

a. The use of DOD and other government telephone systems, 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 ensure all users understand authorized and unauthorized uses of government telecommunications and UC services, and will provide an acceptable use policy to be signed by users. Local policies and procedures will be issued, as necessary, to avoid disruptions to telecommunications systems. DODD 5500.07 and DOD 5500.07-R Joint Ethics Regulation, Aug 2013, serve 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 systems 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 para 3-3 for additional information on communications monitoring).

c. Use of non-DOD or non-DODIN commercial transport as an alternative to DOD, DODIN, or DISN-provided transport requires a DODIN Waiver (see para 6-3).

d. Army-funded IT and information management 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 FAR.

e. Official business calls, email, instant messages, chat, 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).

f. 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 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 communications when commercial service is unavailable, or so limited that it is considered unavailable. 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 para 4-9 for guidance on acquiring and using cellular telephones and other portable devices).

g. 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 DA Pam 25-1-1).

h. 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, domestic partner, or minor children; scheduling doctor, auto, or home repair appointments; brief Internet searches; and emailing directions to visiting relatives). Non-mission email should be limited and government email addresses should not be used or given out for personal purposes. Several examples include sales promotions, social media correspondence, travel promotions, and consumer surveys.

- i. The Joint Travel Regulations (<https://www.defensetravel.dod.mil/site/travelreg.cfm>) provide guidance for telephone calls while at a temporary duty location.
- j. Submit requests for leased commercial phone service via memorandum to the installation NEC (see DA Pam 25-1-1).

### **3-2. Unauthorized and prohibited uses of telecommunications and computing systems**

a. 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 DOD-owned IT. Introducing or using software, firmware, or hardware on DOD owned/issued IT that has not been approved by the Army CIO/G-6-appointed authorizing official is prohibited.

c. Prohibitions on the use of Army communications systems include—

(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 websites, pornographic images, or computer-generated or otherwise pornographic images; chain email messages; unofficial advertising, soliciting, or selling via email; and other uses that are incompatible with public service.

(2) Use of inappropriate signature blocks when sending electronic messages (emails). Army policies for records management apply to emails. Emails generated by Army personnel in their official capacity from Army communication devices (including but not limited to computers and hand held devices) will not contain slogans, quotes, or other personalized information as part of the individual sender's signature block. Signature blocks within emails will contain only the necessary business information, such as: the name of the organization (office, activity, or unit represented); official mailing address or unit information; name of individual; telephone numbers (Defense Switched Network, commercial telephone, cell phone number, or facsimile numbers); office email addresses or government websites (unit web or social media page); government disclaimer (Privacy Act Statement, Attorney Client Notice); unit historical motto (<http://www.tioh.hqda.pentagon.mil>); or any other information approved by HQDA. Requests for exceptions will be submitted to the first O6 or equivalent in the chain of command (with possible delegation to the next O5 in the chain of command, or his/her equivalent).

(3) 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.

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

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

(6) 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 in AR 25-1.

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

### **3-3. Communications monitoring and recording**

a. Army policy permits communications monitoring and 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—

- (1) AR 380-53 and AR 25-2 for information system security monitoring.
- (2) AR 190-53 for law enforcement purposes.
- (3) AR 380-10 for electronic surveillance.
- (4) DODI 8560.01.

b. Monitoring includes, but is not limited to, active attacks by authorized entities to test or verify the security of the system.

c. 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, instant

messages, chat, IP voice, 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.

### **3–4. Leasing of Government-owned telecommunications assets**

*a.* If requested, Government-owned, outside plant (OSP) telephone facilities, inside plant telephone facilities, and/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 memorandums of understanding. OSP facilities, inside plant facilities, and antennas are classified as IT equipment and are accounted for in accordance with AR 710–2 and AR 735–5. OSP facilities include installed or in-place telecommunications cable (copper and fiber optic), and their associated connecting terminals, telephone poles, maintenance holes, and duct bank systems. Inside plant facilities include, but are not limited to, 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.

(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 organizations outside the continental United States (OCONUS), will comply with this paragraph when negotiating new, revised, or existing services or facility leases; and when 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 telecommunications companies for the lease of any Government-owned appropriated funds (APF) facilities (for example, cable pair, equipment, maintenance holes, 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 DA. Terms of the reciprocal lease agreement will provide that the Government may, according to its needs, reacquire any leased asset.

(1) Nonappropriated fund (NAF) revenue. The revenue from the lease of 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.

### **3–5. Bandwidth utilization management (minimize)**

*a.* The Army will utilize all means available (user or technical) to reduce (that is, minimize) and/or remove nonessential data, voice, and video communications traffic during times of surge or crisis, as required, to ensure communications availability to meet Army requirements. Operational bandwidth requirements take precedence over non-official or non-work related access and usage.

*b.* The authorizing official, in consultation with the Installation Commander, is empowered to minimize web-based Internet access effectively and efficiently in the event of a crisis at one or more installations under his or her responsibility.

*c.* Minimization will be controlled by three levels:

(1) Minimize Level 1: This level is the normal day-to-day operating level of the NIPRNet. All published policies controlling access and use are enforced. Additional unauthorized sites may be blocked, based on DA and ARCYBER directives when issued.

(2) Minimize Level 2: Implement this level to maximize the bandwidth available for mission operations by decreasing personal use of communications systems and equipment. Implement when used bandwidth exceeds 75 percent and/or there is a loss of 20 percent or more of bandwidth capability. Minimize Level 2 will remain in effect for the period specified by the authorizing official, or until normal bandwidth availability is restored.

(3) Minimize Level 3: Implement this level in response to a serious information attack, and all communication to non-military sites must be halted; or in an extreme emergency situation where operations security is the highest priority. This level eliminates personal use of the Internet and maximizes available network bandwidth for official operations. Minimize Level 3 remains in effect for the period specified by the authorizing official.

*d.* Exceptions. Exceptions to the minimize policy will be applied to positions which may require unimpeded access to the Internet due to mission requirements, such as, but not limited to, public affairs officers (PAOs), intelligence specialists, staff judge advocates, inspectors general, auditors, and criminal investigation specialists. Other exceptions may be authorized by the appropriate authorizing official. Organizations requiring exceptions to web access blocking will maintain records to document access requirements for each position.

*e.* Emergencies. To be able to respond to emergencies, any organizational or IS's content and/or proxy exception can be temporarily revoked without notice or with minimal notice in situations when immediate response is required to resolve or protect the network from a security-related issue. This may happen when there is suspicion that the specific content filter exception has created a security hole that is being exploited by an attacker or is otherwise facilitating an intrusion. In such a case, the revoked content and/or proxy exception will be replaced by a deny access policy until the problem has been investigated and its source precisely identified. The specified content and/or proxy exception will be reinstated or suspended depending on the outcome of the investigation.

### **3-6. Information technology support for telework**

The DOD telework policy is located in DODI 1035.01 ([www.dtic.mil/whs/directives/corres/pdf/103501p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/103501p.pdf)).

### **3-7. Military construction communication systems policy**

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

### **3-8. Architectures**

Approved DOD and Army architecture documents will be used to establish architectural procedures, implementation plans, and requirements. Army architectures must be cybersecurity compliant, interoperable, defensible, and aligned with CIO/G-6 Strategic Goals and Guidance. Army architecture documents will align with the following documents: Unified Capabilities Requirements (UCR) 2013; DOD UC Framework; DOD UC Master Plan; LandWarNet 2020 and Beyond Enterprise Architecture; Army, Air Force and DISA Unified Capabilities Implementation Plan; Technical Criteria for the Installation Information Infrastructure Architecture; and applicable Security Technical Implementation Guides (STIGs).

## **Chapter 4**

### **Telecommunications Systems and Services**

#### **4-1. Applicability**

*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 chapter pertains to existing telecommunications systems and services, to include data networks, mobile devices, telephones (including cellular), pagers, radios, satellites, facsimile machines, video conferencing, commercial television services, and other systems and services that may 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.

#### **4-2. Time-division multiplex equipment**

*a.* Further investment in legacy voice-switching (for example, TDM) equipment is terminated. A majority of Army TDM equipment is beyond useful life.

*b.* Commands will reduce or eliminate TDM circuits. Requirements for local call capability will transition to an IP solution (for example, VoIP, DISA Voice Internet Service Provider (ISP) service, VoSIP, DISA Enterprise Classified VoIP).

*c.* Commands that have an urgent requirement to purchase (or have already purchased) TDM equipment will submit requirements through the CIO/G-6 (SAIS-PRI) Army Information Technology Approval System (ITAS) process.

*d.* Commands that have requirements to purchase or replace existing Multilevel Secure Voice (previously known as Defense Red Switched Network (DRSN)) switches will provide a detailed justification and impact statement to the CIO/G-6 review authority (program manager (PM), Installation Information Infrastructure Communications and Capabilities (PM I3C2)), to enable the command PM to submit requirements via his or her chain of command to CIO/G-6 (SAIS-AOI) for approval. The PM I3C2 will coordinate and obtain funding for approved Army requirements, and forward requirements to the Joint DRSN Logistics and Acquisition Manager, Hill Air Force Base.

*e.* The moratorium on investment in legacy voice-switching equipment and the requirement to submit requests for waivers to purchase voice-switching equipment applies to all TDM voice-switching equipment that is not capable of providing unclassified and/or secret IP voice services. The Army will migrate as soon as practical to an almost-everything-over-Internet Protocol architecture, to include UC and collaboration, with an end state of end-to-end IP.

*f.* Any command that has an urgent requirement to implement unclassified or secret voice capability must follow the process included in paragraph 7–4 of this publication. The request will include the following—

- (1) A detailed justification.
- (2) An operational need statement.
- (3) Architecture details.
- (4) The supported organizations or identification of 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.

#### **4–3. Asynchronous transport mode equipment**

*a.* Further investment in asynchronous transport mode (ATM) equipment or ATM interfaces on customer or provided edge equipment will be terminated and no longer installed within Army networks per Network Services (NS) Customer Notice 2014–02 and Assistant Secretary of Defense Networks and Information Integration (ASD NII) ATM Phase-Out Plan Memorandum.

*b.* All Army organizations that continue to require ATM support are responsible for providing the funding for required levels of support. The DODIN 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) ATM Phase-Out Plan memorandum. New equipment can no longer be ordered, and the commitment for support expired 31 December 2012. While stopgap support may be available, costs to continue support of ATM will rise markedly and become prohibitively expensive.

#### **4–4. Integrated services digital networking**

*a.* All Army organizations will cease investment in (nonemergency) integrated services digital network (ISDN) supported technology, equipment, and transport. All Army organizations will transition from ISDN to a compatible IP-supported technology or service including, but not limited to, video, facsimile, voice, and other network capabilities.

*b.* CIO/G–6 will provide an exception to cease investment in ISDN for organizations without IP and without funding available for transition to IP. Commands seeking approval to procure ISDN-supported technology and equipment will submit a request to CIO/G–6 (SAIS-PRI) through the web-based Army ITAS at <https://www.eprobe.army.mil/enterprise-portal/web/itas/home>.

#### **4–5. 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) SBU voice network. The SBU voice network (formerly known as the DSN), is the official DOD switched voice network and is the preferred method of telecommunications for all users. However, if SBU voice cannot be used without adversely impacting mission or business outcomes, or if the person being called does not have SBU voice service, other long-distance services may be used. CJCSI 6211.02 provides the policies for official and authorized use of the DISN.

(2) For non-mission command administrative voice services and additional telecommunications services outside DISA DISN contracts, contact USARCYBER.

(3) Washington Interagency Telecommunications Services. Washington Interagency Telecommunications Services provides centralized administrative telecommunications service for DOD in the National Capital Region, 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 DODI 4640.07.

(4) 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.

(5) DISN Voice Precedence.

(a) DISN voice precedence encompasses unclassified and classified systems.

(b) All DISN service requests for voice precedence (flash override, flash, immediate, and priority) requirements must be forwarded through the requestor's chain of command to CIO/G-6 (SAIS-AOI). Upon approval, CIO/G-6 will forward to the appropriate approval authority, in accordance with CJCSI 6211.02.

(c) After final approval, the command will ensure that telecommunications requests have the precedence level annotated in their submission within the DISA ordering system. USARCYBER is responsible for ensuring this information is in the telecommunications request. Any alterations or discontinued precedence voice capabilities will be reported to USARCYBER and CIO/G-6 (SAIS-AOI).

(d) ARCYBER will maintain a tracking mechanism for these requests.

(6) Wired and wireless telephone and telephone-related service.

(a) The use of cordless telephones to communicate sensitive information is prohibited unless the device can be properly encrypted. Specific encryption requirements are found in the Army Wireless Security Standards Best Business Practice, Version 4.0, 26 June 2013 ([https://www.milsuite.mil/wiki/portal:army\\_information\\_assurance/best\\_business\\_practices](https://www.milsuite.mil/wiki/portal:army_information_assurance/best_business_practices)).

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

(7) Long-distance calling.

(a) SBU voice network. (See para 4-5a(1).)

(b) Installation switch. Installation switches will be programmed to utilize SBU voice as the primary network where available. Otherwise, the most economic option will be selected.

(c) 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.

(d) Control and accounting. The NEC will ensure that callers at Army installations, without 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.

(e) 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) Verification of 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, (<http://www.gao.gov/assets/470/467699.pdf>) NECs need not verify every call. Other procedures, such as statistical sampling or historical data, satisfies 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) 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.

(c) 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. Commanders will approve the acquisition and use of telephone calling cards.

(b) Accountability. Commanders will establish and maintain accountability procedures for telephone calling cards. TCOs will assist the Commander in accountability as directed.

(c) Certification. Telephone call 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 call cards will immediately relinquish their card to the NEC or designated Information Management Officer (IMO) and are subject to disciplinary action.



(10) Telephone and IS 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 PAO. Electronic versions of the directory will be placed on that community's page on AKO, SharePoint, or AKO SIPR-Net, as appropriate, but not on the Internet. Every effort will be made to publish e-directories in order to avoid printing and distribution costs.

(b) Releasing telephone or IS 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 website without access controls and prior approval of the organization's PAO. Approval from the organization's PAO and security official is required prior to posting personal information on AKO or other private websites. If personal information is posted on AKO the information will be further restricted to those individuals who have "need-to-know" status.

(c) The AKO community pages. The AKO community pages will be utilized for publishing directories containing individuals' names and office information. The Defense Enterprise Email Global Address List is the primary tool for individual locator information.

b. Official existing telecommunications and UC 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 SBU 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 (contact USARCYBER for 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, domestic partner, 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 they provide 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 case-by-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 NEC-provided local installation basis or on a Regional Call Center-provided basis, or an USARCYBER provided enterprise basis.

#### **4-6. Video services**

The responsibilities listed in this section do not apply to organizations that do not use or are exempted from using traditional Army funds to purchase IT equipment based on compliance with special or higher-level regulations or policies.

*a.* Video teleconferencing. This policy applies to all Army video teleconferencing activities and solutions (including videophones, desktop, and personal computer-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 common-user VTC procedures and guidelines for the respective garrisons. The NEC or other designee approves all VTC systems. Army activities will use contract vehicles managed centrally by PM CHESSE 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 approves all VTC systems, to include those VTC systems used for mission purposes.

*b.* All VTC systems will be reported annually to USARCYBER.

*c.* All items will meet the DOD Video Conferencing Profile (Federal Telecommunications Recommendation 1080B–2002 standards) and be IPv6 compliant. VTC systems will use IP technology instead of ISDN VTC technology.

*d.* VTC system owners, administrators, and managers are accountable to ensure personnel with elevated privileges or access (for example, administrative or operational rights and permissions, configuration, registration, IP addressing, and so on) comply with the following—

(1) Acceptable computing environment certifications, to include—

(*a*) Online DISA Global Video Services (GVS) Facilitator and User VTC certification courses/modules, which can be found at <https://disa.deps.mil/ext/cop/ns-extranet/externalconnect/sitepages/home.aspx>.

(*b*) Army-specific training appropriate for hardware and software in use at the location.

(*c*) Vendor-specific training appropriate for hardware and software in use at the location.

(2) Implement and enforce the use of all applicable Standard Operating Procedures; Checklists; Configurations; and Tactics, Techniques, and Procedures for VTC infrastructure, conference rooms, and personnel.

(3) Ensure VTC systems are – or will be – connected via IP network. Connected systems are required to meet DOD, DISA, and Army requirements for operating on the IP network. Systems must be validated by the local NEC, authorized designee, or Network Operations Center prior to connecting.

(4) Ensure all VTC equipment and services are sustained and appropriately supported with secure configurations and security patches in order to connect or remain connected to the DODIN and LandWarNet.

*e.* Use of multi-point control units (MCU) will be reduced to the minimum amount possible. The reduction in use of unnecessary MCU connections is important to maintaining optimum performance for VTC services. Commanders, agency, and organization chiefs must ensure that end-points and MCUs connect directly to the host end-point or MCU without cascading or daisy-chaining.

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

*g.* Fixed-facility video teleconferencing. VTC fixed (permanent) facilities, which cost over the “other procurement, Army” dollar threshold, will be validated by the requesting NEC, approved by the chain of command, and prioritized by the respective commander.

*h.* Budget submission for VTC. NECs will plan for the expense of, and investment in, VTC systems to meet their current and projected needs. Requirements for investment in equipment will be developed and forwarded annually, along with the requirement identified by each NEC, consistent with established budget review schedule and AR 1–1. NECs will plan for expense of and investment in VTC equipment through installation resource management channels as part of their annual operating budget, and for inclusion in the Installation Management Command program objective memorandum (POM) submission and the appropriate signal command POM submission.

*i.* DISN video services.

(1) The DISA DISN GVS network is an enterprise-grade service that provides VTC capabilities to the DOD and Mission Partners with a need to collaborate via high-quality VTC over an SBU IP data network. Installations that require common-user conference facilities will connect via the Army LandWarNet to the GVS global program to use the DISA connectivity and interoperability features.

(2) DISN VTC system owners, administrators, and managers will track usage and periodically review with DISA to resolve discrepancies.

#### **4–7. Commercial television service**

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

*a.* NAFI 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 Command at the Army level, and is 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, is considered equivalent 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 APF.*

(1) 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.

(2) 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).

*d. NEC validation.* NEC validation is required before any official services are 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. Subscription.* No Army member or organization will be coerced to subscribe to a franchisee's services.

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

*i. Installation channels.* The Army requires that the commercial television service franchisee reserve on-installation channel(s) for use by the installation. The 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/are activated, the following restrictions apply—

(1) Official programming. The Army must avoid 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, commercial television service, or other systems for internal public affairs purposes.

*j. NAF 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.

#### **4-8. Multifunction mobile devices**

The responsibilities listed in this section do not apply to organizations that do not use or are exempted from using traditional Army funds to purchase IT equipment based on compliance with special or higher-level regulations or policies. Portable electronic devices (PEDs) include mobile, cellular, and wireless telephones; personal digital assistants (PDAs); smart phones; tablets; and other devices that are approved and placed on the UC APL or available through CHESS (see DODD 8100.02).

*a.* Requirements. Army procured, provided, and maintained devices are to be used for official business and authorized use only. 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) USARCYBER 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 USARCYBER and procure the services from established blanket purchase agreements (BPAs). Services on existing contracts must transition to the enterprise BPAs upon expiration of the contract or at the end of the current option period, whichever occurs first.

*(a)* All agencies are required to assess current wireless device inventories and usage, and to establish controls to ensure that they are not paying for unused or underutilized devices. In addition, agencies must validate their wireless bills monthly, bringing any discrepancies or errors to the attention of their contracting office and USARCYBER for adjudication with the wireless carrier.

*(b)* All active devices not under BPA suspension or a flat-rate service plan that are not used (voice, data, or text) for a period of 60 days must be discontinued immediately. Devices with no usage that are part of a continuity of operations package or an emergency deployment package must be identified and moved to a flat-rate service that converts to a full-use capability when activated for contingency response.

*(c)* All Army agencies are required to utilize the ordering procedures established in the ordering guide located at <https://www.us.army.mil/suite/page/606723>.

*(d)* Agencies will coordinate directly with and submit all procurement actions for wireless services to USARCYBER via the Wireless Expense Management Portal (see <https://portal.army.mil/apps/wem/>).

*(e)* Waiver. Commands may request a waiver to this policy in order to meet compelling, mission-essential operational requirements or when the capability can be provided through a more cost effective means. Requests for waivers must be consolidated by the initiating command, receive concurrence of the first General Officer Commander or civilian equivalent, and be approved by the ACOM, ASCC or DRU commander. CIO/G–6 retains oversight of the waiver process. The waiver process should not exceed 30 days after the initiating organization properly submits a completed waiver request. Requests for exceptions to this policy must be submitted via the ITAS approval process located at: <https://www.eprobe.army.mil/enterprise-portal/web/itas/home>.

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

*(a)* 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.

*(b)* Lost PEDs. 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.

*d.* 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.

*e.* Secure cell systems. Tactical units in a deployed environment will use only the Army’s encrypted secure cell systems.

*f.* Beepers, pagers, and PDAs. When beeper or pager functions are part of the features of a cellular telephone or PDA, the item will be managed the same as a cellular telephone. All Army organizations will use USARCYBER BPAs established to provide economies of scale. The scope of beeper or pager service will be authorized based upon geographic service areas.

*g.* 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.

*h.* 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.

#### **4–9. Wireless priority service and wireline government emergency telecommunications service**

Wireless priority service (WPS) and GETS provide an end-to-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.

#### **4–10. 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 (also see 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) NEC as operator. The installation NEC is the single provider and operator of all LMR capabilities, as approved by CIO/G–6 (SAIS–AOI) 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) Memorandums of understanding. Memorandums 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 cooperating outside agency or installation.

(4) Resourcing. CIO/G–6 (SAIS–AOI) will notify USARCYBER of the requirements for LMR 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 noncompliance with these laws and policies. Theater-level signal commands may submit these prioritized requirements to CIO/G–6 (SAIS–AOI) through the Army LMR Program (also see 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 narrowband mandate, Association of Public Safety Communications Officials International Project 25 standards, and will support Type 3 encryption devices via the Advanced Encryption Standard.

(6) Frequency assignment coordination and spectrum supportability.

*(a)* Coordinate and process frequency requirements in accordance with AR 5–12.

*(b)* If required, process SSRA in accordance with AR 5–12.

(7) Waivers. Submit requests for waivers in accordance with AR 5–12.

##### *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) Frequency Range. Enterprise-LMR hardware fielded to installation first responders will be capable of supporting digital and analog communications across the U.S. National Table of Frequency Allocation for Very High Frequency, Ultra High Frequency, 700 megahertz (MHz) and 800 MHz public safety frequency bands and/or equivalent/applicable host national allocations as follows:

*(a)* DOD LMR 138–144 MHz; 148–150.8 MHz; and 380–399.875 MHz.

*(b)* Non-Federal LMR 150.8–162 MHz and 450–512 MHz.

- (c) Federal Government LMR 162–174 MHz and 406.1–420 MHz.
- (d) State and Local Public Safety 700/800 (764–870 MHz).
- (e) Host Nation Approved Spectrum Allocation.
- (4) Military Auxiliary Radio System. The Military Auxiliary Radio System provides, as addressed in AR 25–6, contingency radio communications support to U.S. Government operations through the utilization of organized volunteer radio operators and operating facilities under the appropriate authorities, as directed and coordinated with the DOD.

## **Chapter 5**

### **Satellite Communication Systems and Position Navigation and Timing**

#### **5–1. General**

- a. SATCOM includes military satellite communications (MILSATCOM) and commercial satellite communications (COMSATCOM). 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.
- b. MILSATCOM includes those systems (space, control, and terminal segments) owned and operated by DOD. MILSATCOM also includes DOD gateways and service unique gateways.
- c. COMSATCOM encompasses DOD-leased 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.
- d. Army SATCOM terminal systems include military developed and acquired terminal systems (including Army-owned COTS terminals such as International Maritime Satellite (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 6250.01E and DA Pam 25–1–1).

#### **5–2. Commercial satellite communication annual usage report**

- a. To facilitate a strategic approach to COMSATCOM acquisition, DOD must understand how it purchases and uses COMSATCOM services and hardware. CJCSI 6250.01E requires USSTRATCOM, in coordination with DISA, to prepare an annual COMSATCOM analysis or report during the first quarter of each fiscal year (FY) for the previous FY, in order to validate cost and utilization information on the procurement of all COMSATCOM services. CIO/G–6 (SAIS–AON) consolidates all Army input to the annual report. Upon receipt of the Joint Action Control Office (JACO) tasking, USARCYBER will consolidate and report all commercial SATCOM usage contracted through USARCYBER and submit the report to CIO/G–6 (SAIS–AON). All other Army organizations will report directly to CIO/G–6 (SAIS–AON) action officer. The annual JACO tasking will include a detailed set of instructions for completing the report.
- b. Individuals responsible for procuring the contracted SATCOM services will provide the required information in the format requested by the JACO tasking and submit it to CIO/G–6 (SAIS–AON) to meet the assigned suspense date. The data-collection template requires cost and usage data for 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 within the FY.

#### **5–3. Satellite communication requirements**

- a. General. CJCSI 6250.01E 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 6250.01E. 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.* SATCOM systems expert. Army is assigned SATCOM system expert responsibility for the Defense Satellite Communications System, Wideband Global SATCOM (WGS), the Global Broadcast Service, and the Mobile User Objective System. Army is also the consolidated SATCOM systems expert for consolidated military Super High Frequency systems.

*c.* Service requests. Order services by contacting your SATCOM Support Center (SSC) or by contacting COMSATCOM Center directly if you are not supported by a SSC. All Army components requiring COMSATCOM service from DISA will submit a telecommunications request through DISA's online web-order system. If the service cannot be provided by DISA, an OSD DODIN waiver is required for an Army customer to request USARCYBER to procure their COMSATCOM directly from a vendor. An SDB submission is still required with a submission of a telecommunications request for COMSATCOM.

#### **5-4. 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.* Upgrades. All fielded wideband satellite terminal systems, to include 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).

#### **5-5. Satellite communication standardization**

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

#### **5-6. Network command operations of military satellite communication systems**

USARCYBER operates and maintains SATCOM Earth Terminal Stations and technical control facilities for the Direct Communications Link, selected Standard Tactical Entry Point, DOD Teleport and Enterprise Gateways, and Warfighter Information Network-Tactical Regional Hub Nodes.

#### **5-7. Army component command to United States Strategic Command**

As the ASCC 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.

#### **5-8. 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. The Inmarsat and Iridium systems fill 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 secure telephone equipment 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 the same process as the Iridium handset/equipment (see AR 525-27, AR 25-2, and DA Pam 25-1-1 for more information).

*b.* Procurement of Inmarsat and Iridium equipment. ACOMs, ASCCs, and DRUs are responsible for funding Inmarsat terminals and satellite airtime use, and for funding Iridium handsets, subscriber identity module cards, and registration fees. Under the DOD's FY 14-18 contract with Iridium, the Army pays a fixed cost for Iridium airtime use from a centralized funding element, and the end-users do not pay an airtime usage fee. Organizations and units will submit their requirements for approval to Deputy Chief of Staff, G-3/5/7 (DAMO-RQ). Organizations and units will submit their requirements for approval to Deputy Chief of Staff, G-3/5/7 (DAMO-RQ) per AR 71-9. The procuring organization or unit is responsible for arranging the commissioning of Army Inmarsat terminals into satellite access operation by arrangement through USARCYBER. USARCYBER will maintain records of all Army Inmarsat and Iridium usage.

c. Operation of Inmarsat equipment. ACOMs, ASCCs, and DRUs will ensure field operators configure Inmarsat units to the correct Inmarsat land-Earth station. ACOMs, ASCCs, and DRUs 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, ASCCs, and DRUs 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.

### **5–9. Position, navigation, and timing global positioning system, precise positioning service, and standard positioning services**

The global positioning system (GPS) is 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 number of Army and Joint force critical missions and infrastructure in conducting all facets and scales of operations, including the following—

- (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 (AF SMC)). Army PPS users will employ PPS user equipment in accordance with CJCSI 6130.01 to support combat and sustainment operations. CJCSI 6130.01 exempts specified non-combat applications (range instrumentation, advanced technology, mapping, special operations, and classified applications) from the requirement to employ PPS user equipment. Standard positioning service (SPS) systems may be used in these applications. Do not use SPS for critical military operations, such as weapon delivery coordination, target location, and fire support. Waiver requests to use SPS user equipment for any applications not exempted by CJCSI will be submitted to OSD through the Army acquisition executive (AAE).

c. Army program/project and product managers will coordinate the procurement of PPS user equipment with Program Manager, Positioning Navigation and Timing who will ensure procurements comply with all applicable OSD and AAE guidance and AF SMC technical standards for interoperability.

## **Chapter 6 Long-Haul and Deployable Telecommunications**

### **6–1. 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 Systems 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 DISACs 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 into the DISA Direct Storefront or DISA Direct Order Entry. USARCYBER will conduct a technical review, financial approval, assurance of Army compliance with governing policies and regulations, and coordination of the follow-on steps within the DISA online web-order system.

(3) If a DOD solution or DISA is unable to fulfill Army requirements, a DODIN waiver must be acquired (see para 6–3).

(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



USARCYBER 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 75 percent before a bandwidth upgrade is requested, unless there are other known circumstances (such as unit restationing and system fielding) that will cause the existing, available bandwidth to be exceeded. NECs will validate bandwidth requests in accordance with this paragraph.

(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. Additional information is available in paragraph 3–5.

(7) Regarding the identification and planning for future bandwidth requirements, USARCYBER will validate requests for bandwidth changes received from customers once an engineering analysis has been completed. Current utilization and known future bandwidth requirements needed to support future enterprise initiatives and systems will be the basis of these requests.

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

*c.* SBU voice network. SBU voice is the DOD-preferred means of providing non-secure circuit switched and IP 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.* Multilevel secure voice services. The multilevel secure voice service is a secure, mission-command system that supports secure voice and conferencing requirements. It 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 secure voice services in accordance with CJCSI 6211.02. Army commanders are responsible for their designated portions of the secure voice service. This may include, but is not limited to, providing operation and maintenance funds for the secure voice logistics support, sustainment, training, secure voice-related equipment, and special interface trunks required by the combatant command or supported command for which they are responsible.

(2) Unique requirements. Forward unique requirements through the Army Signal Commands to CIO/G–6 (SAIS–AOI), for coordination and validation. Guidance for submitting DISN information services requests can be found in CJCSI 6211.02D ([http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/6211\\_02a.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf)).

(3) Certification. Servicing ACOMs, ASCCs, and DRUs will certify whether funds are available as part of the multilevel secure voice approval request. The funding review and forecast for certification will be coordinated through the chain of command to CIO/G–6 (SAIS–AOI) prior to approval.

*e.* Organizational Messaging Service.

(1) Usage. The organizational messaging service (OMS) provides official organizational messaging to the DOD, federal departments and agencies, and certain allied governments. OMS may be used to commit resources, direct action, clarify official positions, and issue official guidance.

(2) Message size. Attachments to OMS 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 ACP 127(G) located at <http://www.dtic.mil>; and the Defense Message System General Service Message Security Classifications, Categories, and Marking Phrase Requirements available to CAC holders through the OMS asset distribution system at <https://dkwwwefgv001.roscc1.disa.mil/>.

*f.* Joint Chiefs of Staff (JCS)-controlled mobile or transportable communications assets. JCS maintains control of mobile or transportable communications equipment, and ensures the equipment is ready for worldwide emergency and contingency communications for the operational and support needs of the JCS. All Army organizations with requirements for JCS-controlled assets will submit requests in accordance with CJCSI 3110.1.

## **6–2. Mission partner and defense contractor connections to the Defense Information Systems Network**

*a.* Approval authority. The DOD CIO will approve all mission partner and defense contractor circuit connections to the DISN. Army sponsors must validate and endorse mission partner and defense contractor requests for connection to the DISN.

*b.* Mission partner and defense contractor connection requests. All mission partner and defense contractor connection requests will be submitted via DISA to, CIO/G–6 (SAIS–AOI) for coordination and validation (see DODI 8100.04 and CJCSI 6211.02).

c. A Computer Network Defense Service Provider (CNDSP) must be identified, and an agreement must be in place to verify the CNDSP documented is providing this service.

d. All DISN solutions must be ordered through the DISA online web-order system.

e. 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 mission partner and defense contractor approval, the sponsor will notify CIO/G-6 (SAIS-AOI) when connections are terminated.

f. Renewal of connection. If a mission partner and defense contractor 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 DISA.

(1) If there is no change to mission, sponsor, contract, or location, the sponsor fills out the revalidation template located at <https://snap.dod.mil/gcap/home.do>. This will be sent to DISA for revalidation with a copy to CIO/G-6 (SAIS-AOI).

(2) If the sponsor has changes to mission, sponsor, contract, or location, a new validation template will be used and will clearly state what the change is at the top of the document. A full revalidation is needed in case of a change in sponsor. See the template and revalidation information in the DISN Connection Process Guide at [http://www.disa.mil/network-services/~media/files/disa/services/disn-connect/references/disn\\_cpg.pdf](http://www.disa.mil/network-services/~media/files/disa/services/disn-connect/references/disn_cpg.pdf).

### **6-3. Department of Defense Information Network waivers**

a. General. DODI 8100.04 and CJCSI 6211.02 serve as the basis for Army policy in which the DOD CIO utilizes the DODIN Waiver Panel (DWP) as a governance tool to ensure DISA Enterprise Services are evaluated first to fulfill an IT requirement before considering a non-DOD commercial resource. Army entities requiring communications services not provided by DISA will submit a DODIN waiver. A waiver will only be approved if it can be shown that a DOD IS or DISA cannot provide the service.

b. Cybersecurity.

(1) Army personnel will work in the Certification and Accreditation Tracking Database located at <https://emass-army.csd.disa.mil> to acquire an ATO or IATO via the DOD's Risk Management Framework (RMF) for IT (see DODI 8510.01). Contact [iacora@us.army.mil](mailto:iacora@us.army.mil) with questions. Packages submitted without appropriate cybersecurity documentation will be held at, CIO/G-6 until provided.

(2) Connection types.

(a) Waiver requests for systems in development need at least an interim authority to test (IATT) signed by an authorizing official.

(b) For systems at a conceptual stage (no equipment to test), the DSAWG will reduce the IATT requirement to a "commander's mission approval letter" and a topology diagram. This will be accomplished at the discretion of the DSAWG, based on the requirement and proper analysis of the risk to the DISN.

(c) Waiver requests for operational systems require an ATO signed by an authorizing official. The system must have an ATO prior to operating on the Internet, DISN, or other DOD network. These systems are brought into full compliance once a DODIN waiver is approved. Waivers will not be processed further if the accreditation/authorization is not current or does not have an expiration date. If the request is in a conceptual stage, a signed "commander's mission approval letter" is acceptable.

c. Computer Network Defense Service Provider.

(1) A CNDSP is not required for an organization that will only be passing public information or data over the commercial Internet service provider (C-ISP) connection. An organization does not have to report this 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 request:

(a) Active monitoring (for example, indicate how often the connection is monitored on a daily, weekly, or bi-monthly 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 C-ISP connection to verify the CNDSP is providing this service.

d. Types of DODIN Waivers. The types of waiver requests are for C-ISP, networks, satellite services, cross component computing issues, continuation of ATM beyond sunset dates, and Cloud Computing.

(1) C-ISP.

(a) Authorized access. The only authorized access from Army computers, systems, and networks to the Internet is through a DODIN-controlled and DODIN-monitored connection. Exceptional situations may exist where Army organi-

zations 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, CIO/G-6 (SAIS-AOI).

(b) Commercial Internet service. Army organizations may acquire commercial Internet service (for providing email service, web access, and OCONUS liaison missions), after approval of a DODIN 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 C-ISP. NECs will ensure the proposed network architecture complies with security requirements and makes efficient use of available bandwidth

(c) 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 C-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 (also see AR 215-4, which governs IT supplies and services acquired with NAFs). These Internet connections will be coordinated through the NEC with the USARCYBER support office prior to connection.

(d) 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 all hours, and so on). Unofficial, free, or pay-for-use Internet access will be managed by MWR in accordance with ARs 215-1 and 215-4.

(e) Any C-ISP found to be operating without an approved DODIN Waiver or not in compliance with an IATO or ATO must be immediately terminated or brought into compliance within 45 days.

(2) Networks. Unless explicitly permitted by DOD policy, all telecommunications and IT networks and circuits that extend beyond the confines of the installation will be procured and/or contracted for by DISA. For urgent or critical operational mission requirements, a waiver must be approved by the DWP and signed by the DOD CIO. Refer to the DISN Connection Process Guide for additional procedures ([http://www.disa.mil/network-services/~media/files/disa/services/dsn-connect/references/dsn\\_cpg.pdf](http://www.disa.mil/network-services/~media/files/disa/services/dsn-connect/references/dsn_cpg.pdf)). If an alternative connection path, that is, C-ISP is required for NIPRNet access (that is, enclave/standalone), or network connection, a waiver must be approved by the DWP and signed by DOD CIO.

(3) Satellite services. All SATCOM services will be procured via DISA. Commands should review the DISA service catalog for options. If DISA is unable to fulfill the requirement, commands may go through the DODIN waiver process for an exception. (See chapter 5 for additional information).

(4) ATM. If there is a requirement for continued use of ATM in the Army network, a DODIN Waiver is required.

(5) Cloud Computing. Outsourcing DOD IT support to commercial cloud providers brings potential risks to the Army that must be managed at the enterprise level. The DODIN Waiver Panel, informed by the DSAWG, is established to grant approval for DODIN Internet connections and deviation from existing cybersecurity standards. For the Department, use of third party, off-premises cloud services requires a waiver from the DWP in order to preserve the security of DOD data and mission assurance in the face of persistent cyber threats from capable adversaries.

*e.* Exceptions to DODIN waivers. A DODIN waiver is not required for the following exceptions:

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

(2) C-ISPs installed in the facilities/quarters of wounded warriors for their Internet access. Component authorizing official approval is still required.

(3) Field training exercises and/or urgent need/contingency operations C-ISPs operating less than 90 days—

(a) Do not require a waiver, but must be reported to the DOD CIO DWP for situational awareness and enumeration.

(b) Must have proper cybersecurity, a valid mission need, and authorizing official and Service representative officer approval.

(c) Require a waiver if operating more than 90 days.

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

#### **6-4. 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, CIO/G-6 is the voting representative to the SATCOM Interoperability Standards Committee in support of NATO.

*b.* NATO communications. Army activities will carry out assigned responsibilities contained in signed memorandums 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.* NATO facilities. Whenever the Army requires communications facilities, the available communications facilities of NATO or member nations will be used to the maximum extent possible, provided reliable communications for use are assured, and that such use is cost effective.

*d.* Unilateral communications. When NATO and NATO-member communications facilities 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 DOD 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 CIO/G-6 prior to forwarding to the Joint Staff.

(5) NATO 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 materiel 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 7**

### **Unified Capabilities**

#### **7-1. 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, these new technologies 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 cybersecurity vulnerabilities. These vulnerabilities will be mitigated using appropriate cybersecurity techniques.

## **7-2. General**

*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 medium 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 cybersecurity. All Army organizations will comply with functional requirements, performance objectives, and technical specifications for DOD networks that support UC, as specified in DOD CIO publication DOD UCR 2013 (or the latest version) and the UC Framework.

*b.* For exemptions 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 per 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 is the starting point for tenant organizations and activities to obtain support for unique IT services that are not provided in the C4IM Services List. The installation NEC is the only organization on the installation authorized and responsible for providing common-use baseline services on a nonreimbursable basis to all installation tenants as prescribed by the C4IM Services List. IT support services are categorized as baseline or mission-funded. Upon identifying a requirement that requires higher-level approval, the NEC will forward the requirement to the local Theater-level signal command, which in turn forwards the requirement to USARCYBER and to CIO/G-6 (SAIS-AOI) for higher-level approval. The current authorization C4IM services list and LandWarNet Catalog are 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 DISA for consideration and approval.

## **7-3. Unified capabilities approved product list**

*a.* All Army organizations will purchase data, video, and voice-switching hardware and software listed on 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 its needs. In accordance with AR 25-2, COMSEC cryptographic or encryption devices and equipment must be procured through a BPA with the Communications Security Logistics Agency.

*b.* UC APL Removal List. Army organizations will not procure any items on the UC APL removal list, which can be found at <http://www.disa.mil/services/network-services/ucco/apl-removal-list>. However, products procured and installed prior to being placed on the UC APL removal list may be eligible for continued operation in DOD networks provided applicable security requirements are met (for example cybersecurity and vulnerability assessments, STIGs, and so on). Expansion to the capacity (number of users) of a product on the UC APL removal list in an existing accredited enclave is not considered a new installation.

## **7-4. Voice services**

*a.* Voice over Internet Protocol (VoIP). VoIP is the DOD-preferred means of providing SBU voice communications. The next version of the UCR will include guidance for implementing VoIP capabilities. Voice will be migrated from a circuit-switched, TDM infrastructure to an IP packet-switched infrastructure.

*b.* DISA-provided voice service.

(1) All Army organizations will use DISA as their primary SBU IP voice service provider. DISA will provide an Enterprise SBU IP voice (currently referred to as EVoIP) solution for all new Army unclassified IP voice (currently identified as VoIP under the C4IM services catalog) requirements, thus releasing the Army from implementing unnecessary call processors.

(2) Any SBU IP voice requirement that cannot be fulfilled by DISA will be reviewed on a case-by-case basis using the ITAS waiver review process. All requests will be forwarded with appropriate recommendations via the chain of command. Requests will include—

*(a)* A detailed justification.

*(b)* An operational need statement.

*(c)* Architecture.

*(d)* The supported organizations or the entire installation.

*(e)* An impact statement that describes the results of not receiving an approved waiver.

*(f)* A bill of materials.

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

*(h)* An approved requirements document and a General Officer or Senior Executive Service member endorsement.

(3) DISA voice ISP-public switched telephone network (PSTN) service.

(a) All Army organizations that have a Session Controller will use the DISA ISP–PSTN service to provide full-featured commercial phone service (local, long distance, international, emergency, inbound, and outbound calling) through a standard NIPRNet connection.

(b) NECs will submit the telecommunications service request to DISA.

(c) Commands that use DISA ISP–PSTN service are responsible for paying per-minute billing and bandwidth management to accommodate this additional service on their local area network (LAN) and NIPRNet infrastructure.

(4) Exceptions to ISP–PSTN use.

(a) Commands will not use or will discontinue use of the DISA ISP–PSTN service if their original commercial phone services were at a reduced cost justified in current and previous billing, invoice, and accounting management processes, referenced in para 4–5a(8)(a).

(b) Commands that do not have a session controller connected to the NIPRNet soft switch core.

(5) Army-provided voice service.

(a) USARCYBER will serve as the single authority assigned to operate, manage, and defend the Army’s infrastructure at the enterprise level for VoIP infrastructure.

(b) PM I3C2. The PM I3C2 will procure and field VoIP capability as a part of the network infrastructure modernization cycle.

(c) 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 recently approved UCR and the appropriate VoIP STIGs.

(d) Analog and digital TDM telephone service. Digital and analog phones 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 digital or analog phone may also be connected to a media gateway and PSTN. This is to provide emergency voice service if VoIP phones do not function.

(e) Service requests. NECs will submit voice service requests to USARCYBER via the signal brigade and theater command for Army-provided voice services. USARCYBER will obtain voice service requests, such as local central office trunks, direct-in-dial numbers, commercial business lines, and foreign exchange (FX) trunks or lines, via consolidated local service contracts that are competed among interested service providers. USARCYBER 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 at [usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil](mailto:usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil). If the existing consolidated contract cannot be used to satisfy the requirement, USARCYBER will competitively award a new contract to satisfy the requirement. USARCYBER Army 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).

(f) 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 USARCYBER 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 USARCYBER contracting officer. If an Army user is in a location where there is no NEC support, the user will coordinate procurement via their regional signal command to USARCYBER. A lack of NEC support does not negate the requirement to procure service through USARCYBER.

(g) BASECOM funding. The supporting NEC is the focal point for all common-use BASECOM on the installation or the supported area. BASECOM falls into one of two categories of services that are listed on the C4IM Services List, and are funded on a reimbursable or nonreimbursable basis depending on whether the services requested are baseline services or above-baseline services. The two 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 available at <https://www.itmetrics.hua.army.mil>. Installation NECs will provide baseline IT services to Army activities on a nonreimbursable basis.

2. 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.

(h) NECs will submit a request to USARCYBER, with a courtesy copy to the appropriate Signal Brigade and Theater Command, requesting a telecommunications service priority for the restoration priority of leased emergency voice

circuits and phone numbers (for example, 911, E911, 999, and 112). This will give priority to emergency voice circuits and phone numbers if an outage occurs. Submit requests to [usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil](mailto:usarmy.huachuca.netcom.mbx.g-34-atd-basecom@mail.mil).

*c. Secret IP Voice.*

(1) Secret IP voice is the Army-preferred means of providing secret-only voice communications. The latest UCR will provide guidance for implementation of secret IP voice capabilities. The UCR requires that classified IP voice migrate to multivendor equipment using the Assured Services Session Initiation Protocol (AS-SIP). The UCR further requires that this AS-SIP equipment be interoperability-tested and cybersecurity-accredited by the Joint Interoperability Test Command, then placed on the UC APL at <https://aplits.disa.mil>. For AS-SIP equipment, only classified voice equipment listed on the UC APL is authorized for use.

(2) All Army organizations will use DISA as their primary secret IP voice service provider and follow the most current DISN Connection Process Guide.

(3) DISA will provide an Enterprise classified IP voice solution for all new Army secret IP voice requirements, which will alleviate the requirement for the Army to implement call processors.

(4) Any new secret IP voice requirement that cannot be fulfilled by DISA will be reviewed on a case-by-case basis by USARCYBER and CIO/G-6. All requests will be forwarded to CIO/G-6 (SAIS-AOI) and copy furnished to USARCYBER with appropriate recommendations via the chain of command. The request will include—

*(a) A detailed justification.*

*(b) An operational need statement.*

*(c) Architecture.*

*(d) Supported organizations (or the entire installation).*

*(e) An impact statement that describes the results of not receiving an approved request.*

*(f) A bill of materials.*

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

*(h) An approved requirements document with General Officer or Senior Executive Service member endorsement.*

(5) The NEC is the starting point for organizations and activities to obtain Enterprise secret IP voice services.

(6) All Army organizations that have procured, own, and operate an Army VoSIP enclave will transition to a DISA solution when the system is required to be modernized, technologically refreshed, or at end of life. Exceptions will be reviewed on a case-by-case basis for CIO/G-6 (SAIS-AOI) approval. All requests will be forwarded to CIO/G-6 (SAIS-AOI) and copy furnished to USARCYBER with appropriate recommendations via the chain of command. The request will include—

*(a) A detailed justification to retain an Army owned and operated system.*

*(b) An operational need statement.*

*(c) Architecture.*

*(d) Supported organizations (or the entire installation).*

*(e) An impact statement that describes the results of not receiving an approved request.*

*(f) A costing model that includes the delta between current Army expenditures vice transitioning to DISA. Current expenditures include all resources supporting the life cycle of the VoSIP system including, but not limited to, modernization/technology refresh and personnel costs.*

*(g) The location where the equipment renovation will take place or new location if being moved.*

*(h) An approved requirements document with General Officer or Senior Executive Service member endorsement.*

(7) USARCYBER will serve as the single authority assigned to operate, manage, and defend the Army's existing infrastructure at the command level for Army provided secret IP voice (currently identified as VoSIP under the C4IM services catalog) infrastructure. The C4IM Services List and customer-facing LandWarNet Catalog are located at <https://www.itmetrics.hua.army.mil>.

(8) VoSIP must follow DISA's SIPRNET connection approval process. All VoSIP systems must follow all current processes and policies in the DOD RMF. DISA is responsible for the VoSIP addressing scheme and numbering plans.

## **7-5. Video telecommunication services**

VTC systems will use IP technology instead of ISDN VTC technology. See para 4-7 for more information on video services.

## **7-6. Collaboration capabilities**

*a. Unified collaboration services.* These services integrate standards-based communication and collaboration, including, but not limited to, voice, video, instant messaging, chat, presence, and screen sharing features. DOD- Enterprise-provided UC services are preferred. Local UC services will be integrated with available enterprise applications, both strategic and tactical in accordance with standards established in reference architectures.

*b.* Use of encryption. Collaboration services must provide for the confidentiality, data integrity, availability, and message authenticity (including non-repudiation) of DOD information in accordance with the sensitivity level of the service (for example, For Official Use Only or Secret). Collaboration services will ensure proper encryption and use of strong authentication in accordance with AR 25–2.

*c.* Use of official Government-approved UC services. Only Government-approved services are authorized for official use. Public UC services are prohibited for Army business communications unless specifically authorized.

*d.* 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 and commands 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 at the same level of protection as the most sensitive data in the system.
- (4) Inactive accounts are terminated after a specified period of time, in accordance with AR 25–2.
- (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.

*e.* Collaboration records. Army records management policies apply to all UC traffic, including voice, video, instant messaging, chat, and screen sharing sessions. Designated records managers, records coordinators, and records custodians will monitor the application of records management procedures to collaboration 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).

*f.* Backup and storage. Systems administrators will ensure collaboration servers are backed up for a period of no less than 90 days in an offsite, secure storage facility. Backups will be conducted in accordance with local procedures.

#### **7–7. Installation information infrastructure**

*a.* During construction of a facility, LANs will be installed to meet the requirements of end users, as specified by the latest UCR and UC Framework. 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 and UC Framework provide specific requirements for non-ASLANs. The LANs will be designed to meet traffic engineering and redundancy requirements, as required by applicable mission needs. (See DA Pam 25–1–1).

*b.* ASLAN.

- (1) ASLANs can encompass unclassified and classified systems.
- (2) All ASLAN requests must be forwarded through the requestor’s chain of command to CIO/G–6 (SAIS–AOI).
- (3) USARCYBER will maintain a tracking mechanism for these requests.
- (4) ASLAN Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status.

*c.* 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 within the 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 5–12**

Army Use of the Electromagnetic Spectrum (Cited in para 2–6a(7).)

**AR 25–1**

Army Information Technology (Cited in para 2–6a(2).)

**AR 25–2**

Information Assurance (Cited in para 2–2h(8)(h).)

**AR 215–1**

Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities (Cited in para 4–5a(8)(c).)

**AR 215–4**

Nonappropriated Fund Contracting (Cited in para 4–5a(8)(c).)

**CJCSI 6250.01E**

Satellite Communications (Cited in para 5–1d.)

**DA Pam 25–1–1**

Army Information Technology Implementation Instructions (Cited in para 3–1g.)

#### **Section II**

##### **Related Publications**

A related publication is a source of additional information. The user does not have to read it to understand this publication. Army publications are available on the Army Publishing Directorate (APD) website at <http://www.apd.army.mil>. DOD publications are available at <http://www.dtic.mil/whs/directives>. USC material is available at <https://www.gpo.gov/fdsys/browse/collectionuscode.action?collectioncode=uscode>. The CJCSI are available at [http://www.dtic.mil/cjcs\\_directives/cjcs/instructions.htm](http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm).

**AD 2013–26**

Armywide Management of Printing and Copying Devices

**AR 1–1**

Planning, Programming, Budgeting, and Execution System

**AR 11–2**

Managers' Internal Control Program

**AR 15–1**

Committee Management

**AR 15–39**

Department of the Army Intergovernmental and Intragovernmental Committee Management Program

**AR 25–6**

Military Auxiliary Radio System and Amateur Radio Program

**AR 25–30**

Army Publishing Program

**AR 25–400–2**

The Army Records Information Management System (ARIMS)

**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 710–2**

Supply Policy Below the National Level

**AR 735–5**

Property Accountability Policies

**AR 740–26**

Physical Inventory Control

**Assistant Secretary of Defense Networks and Information Integration Memorandum**

Subject: Asynchronous Transport Mode (ATM) Phase-Out Plan, 8 June 2010 (Available at [http://ciog6.army.mil/linkclick.aspx?fileticket=\\_748647n8b8%3d&tabid=64](http://ciog6.army.mil/linkclick.aspx?fileticket=_748647n8b8%3d&tabid=64))

**C4IM Services List**

Command, Control, Communications, Computers, and Information Management Services List

**CJCSI 3110.08E**

Geospatial Information and Services Supplemental Instruction to Joint Strategic Capabilities Plan (JSCP)

**CJCSI 6211.02D**

Defense Information Systems Network (DISN) Responsibilities  
(Available at [http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/6211\\_02a.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02a.pdf))

**Defense Information Systems Network Connection Process Guide**

(Available at [http://www.disa.mil/network-services/~media/files/disa/services/disn-connect/references/disn\\_cpg.pdf](http://www.disa.mil/network-services/~media/files/disa/services/disn-connect/references/disn_cpg.pdf))

**DFAS–IN 37–1 Regulation**

Finance and Accounting (Available at <http://www.asafm.army.mil/offices/bu/dfas371.aspx?officecode=1200>)

**DISAC 310–55–9**

Base Level Support for the Defense Information System Network (DISN) (Available at [https://disa.deps.mil/org/op6/go62/references/DISA\\_Circular\\_310-55-9](https://disa.deps.mil/org/op6/go62/references/DISA_Circular_310-55-9) (4 April 2014) - Base Level Support for the DISN.pdf)

**DISAC 310–130–1**

Submission of Telecommunications Service Requests (Available at <https://disa.deps.mil/disa/org/nsf/pub/policyandprocessguide/disa%20circulars/disac%20310-130-1/disac%20310-130-1%20current%20doc.pdf>.)

**DOD 5500. 7–R**

Joint Ethics Regulation

**DOD Chief Information Officer Memorandum**

Subject: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014 (Available at [http://dodcio.defense.gov/portals/0/documents/cloud/dod%20cio%20-%20updated%20guidance%20-%20acquisition%20and%20use%20of%20commercial%20cloud%20serviices\\_20141215.pdf](http://dodcio.defense.gov/portals/0/documents/cloud/dod%20cio%20-%20updated%20guidance%20-%20acquisition%20and%20use%20of%20commercial%20cloud%20serviices_20141215.pdf).)

**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 8521.01E**

Department of Defense Biometrics

**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 8500.01**

Cybersecurity

**DODI 8510.01**

Risk Management Framework (RMF) for DoD Information Technology (IT)

**DODI 8530.1**

Cybersecurity Activities Support to DOD Information Network Operations

**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](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf))

**Network Services (NS) Customer Notice 2014-02**

Subject: Acceleration of DISN ATM Services (DATMS) Elimination Schedule, 5 May 2014 (Available at <http://www.disa.mil/network-services/~media/files/disa/services/network-services/notices/nscustomernotice-dams%20elimination-20140424.pdf>.)

**Secretary of the Army Memorandum**

Subject: Information Technology Management Reforms, 9 September 2011 (Available at <http://ciog6.army.mil/portals/1/policy/2012/20110909%20secarmy%20memo%20-%20it%20management%20reforms.pdf>)

**Technical Criteria for the Installation Information Infrastructure Architecture (I3A)**

(Available at <http://www.campbell.army.mil/siteassets/dpw/technical%20criteria%20for%20the%20i3a%20-%20feb%202010.pdf>)

**U.S. Comptroller General Decision B-217996**

**65 Comp. Gen. 19, 21 October 1985**

(Available at <http://www.gao.gov/products/422558>)

**Under Secretary of the Army Memorandum**

Subject: Migration of Army Enterprise Systems/Applications to Core Data Centers, 9 June 2014 (Available at [http://ciog6.army.mil/portals/1/policy/2014/usa\\_policy\\_memo\\_application%20migration%20to\\_core\\_data\\_centers\\_jun\\_9\\_2014.pdf](http://ciog6.army.mil/portals/1/policy/2014/usa_policy_memo_application%20migration%20to_core_data_centers_jun_9_2014.pdf))

**Unified Capabilities Requirements**

(Available at <http://www.disa.mil/ucco-files/ucr-2013-change1-main.pdf>)

**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, chapter 35**

Coordination of Federal Information Policy

**44 USC, chapter 36**

Management and Promotion of Electronic Government Services

**47 USC 226**

Telephone operator services

**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) website at [www.apd.army.mil](http://www.apd.army.mil). DD forms are available on the Office of the Secretary of Defense (OSD) website at [www.dtic.mil/whs/directives/infomgt/forms/index.htm](http://www.dtic.mil/whs/directives/infomgt/forms/index.htm).

**DA Form 11-2**

Internal Control Evaluation Certification

**DD Form 1367**

Communication Work Order, Commercial

**DD Form 1494**

Application for Equipment Frequency Allocation

**DA Form 2028**

Recommended Changes to Publications and Blank Forms

## 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)) website 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) website 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, must be considered prior to approving commercial service.

#### **B–4. Army Morale, Welfare, and Recreation programs and nonappropriated 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).

*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 offices of 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 are 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 as-needed basis, provided the capacity exists and they do 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). AAFES commercially contracted concessions will use commercial telephone service. However, 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 foreign exchange lines for the exclusive use of the contractor. In the absence of tariff rates, or in the case of 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 will reimburse 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 DRUs 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 a military and a civil works function. The mix of service types 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 mission-command 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, APF 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 APF, 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. APF 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 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 A 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 (not including cellular) service for Soldiers who reside in barracks will be compliant with current E911 telephone requirements and the service will be provided by Installation-approved, non-governmental telephone providers. 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) 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

#### C–1. Function

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

#### C–2. Purpose

The purpose of this evaluation is to help HQDA, ACOMs, ASCCs, DRUs 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, or other). 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 information management/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 the IT is still required and meets user needs? (HQDA, ACOM, ACSS, DRU)
- e. Are quarterly reviews of current IT within the APMS-Army Information Technology Repository being conducted and verified by the users, and are they still required and meet user needs? (HQDA, ACOM, ACSS, DRU)
- f. Are evaluations being conducted of existing systems for obsolescence? (HQDA, ACOM, ACSS, DRU)
- g. Is an accurate inventory being maintained and validated annually for IT equipment? (NEC, IMO)
- h. Are continuation of operations and procedures documented, distributed, and tested at least annually? (ACOM, ACSS, DRU, NEC)
- i. Has guidance been provided to ensure that all software is checked for viruses before being loaded? (NEC)
- j. Are existing capabilities and assets considered prior to upgrading, improving, or implementing local area networks? (Theater-level signal command, NEC)
- k. Are uneconomical IT service contracts identified and terminated? (All)
- l. Has the NEC coordinated the acquisition of licenses with the CHES office prior to entering into an agreement with a COTS vendor? (NEC)
- m. Are spare capacity and the functional expansion of IT being considered or used when new requirements are identified? (All)
- n. Has the NEC reported its server consolidation status for all of its Army tenants to the Army CIO/G–6? (NEC)
- o. Are measures being taken to ensure that hard drives are disposed of properly? (NEC)
- p. Are criteria established to justify and approve the acquisition of multifunction mobile devices, cellular phones, and pagers? (Theater-level signal command, NEC)
- q. Has guidance been provided to review and revalidate multifunction mobile devices, cellular phones, and pagers every 2 years? (Theater-level signal command, NEC)
- r. 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)
- s. Is there a requirement for multifunction mobile devices, cellular phones, and pagers to be recorded in the property book? (Theater-level signal command, NEC)
- t. Has the NEC implemented accountable billing procedures? (NEC)
- u. 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, ACSS, DRU)
- v. 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)

w. 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)

x. 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 evaluation replaces the evaluation for the administration of Army telecommunications and UC previously published in AR 25-13.

#### **C-6. Comments**

Help make this a better tool for evaluating internal controls. Submit comments to CIO/G-6 (SAIS-PR) at cio-g6. army.ciog6.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

**ADCCP**

Army Data Center Consolidation Plan

**AEA**

Army enterprise architecture

**AF SMC**

Air Force Space and Missile Center

**AKO**

Army Knowledge Online

**APF**

appropriated funds

**APL**

approved product list

**APMS**

Army Portfolio Management Solution

**AR**

Army regulation

**ARNet II**

Army Reserve Network II

**ARNG**

Army National Guard

**ASA (FM&C)**

Assistant Secretary of the Army (Financial Management & Comptroller)

**ASCC**

Army service component command

**ASLAN**

Assured service local area network

**AS-SIP**

Assured Services Session Initiation Protocol

**ATM**

asynchronous transport mode

**ATO**

approval to operate

**BASECOM**

base communications

**BPA**

blanket purchase agreement

**C4IM**

command, control, communications, computers and information management

**CAC**

Common access card

**CG**

Commanding General

**CHESS**

Computer Hardware, Enterprise Software and Solutions

**CIO**

Chief Information Officer

**C-ISP**

commercial Internet service provider

**CJCSI**

Chairman of the Joint Chiefs of Staff Instruction

**CNDSP**

Computer network defense service provider

**CNGB**

Chief, National Guard Bureau

**COMSATCOM**

commercial satellite communications

**COMSEC**

communications security

**CONUS**

Continental United States

**COTS**

Commercial off-the-shelf

**CSA**

Communications service authorization

**DA**

Department of the Army

**DA Pam**

Department of the Army pamphlet

**DATMS**

DISN ATM Services

**DeCA**

Defense Commissary Agency

**DISA**

Defense Information Systems Agency

**DISAC**

Defense Information Systems Agency Circular

**DISN**

Defense Information Systems Network

**DOD**

Department of Defense

**DODCIO**  
Department of Defense Chief Information Officer

**DODD**  
Department of Defense directive

**DODI**  
Department of Defense instruction

**DODIN**  
Department of Defense Information Network

**DRSN**  
Defense Red Switched Network

**DRU**  
Direct reporting unit

**DSAWG**  
Defense Information Assurance Security Accreditation Working Group

**DSN**  
Defense Switched Network

**DWP**  
Department of Defense Information Network waiver panel

**ELA**  
enterprise license agreement

**ESA**  
enterprise service agreement

**EVoIP**  
enterprise sensitive but unclassified Internet protocol voice

**FAR**  
Federal acquisition regulation

**FSS**  
fixed satellite services

**FX**  
foreign exchange

**FY**  
fiscal year

**GETS**  
Government Emergency Telecommunication Service

**GPS**  
global positioning system

**GuardNet**  
Army National Guard network

**GVS**  
global video services

**HMW**  
health, morale, and welfare

**HQDA**  
Headquarters, Department of the Army

**I3C2**  
Installation Information Infrastructure Communications and Capabilities

**IATO**

Interim approval to operate

**IMO**

Information management officer

**INMARSAT**

international maritime satellite

**IP**

Internet protocol

**IPv6**

Internet protocol version 6

**ISDN**

integrated services digital network

**ISP**

Internet service provider

**ISP-PSTN**

Internet service provider – public switched telephone network

**IT**

information technology

**ITAS**

Information Technology Approval System

**JACO**

Joint Action Control Office

**JCS**

Joint Chiefs of Staff

**JFHQ-State**

Joint force headquarters-state

**JWICS**

Joint Worldwide Intelligence Communication System

**LAN**

local area network

**LandWarNet**

Land Warrior Network

**LMR**

land mobile radio

**MATDEVs**

Materiel developers

**MCU**

multipoint control units

**MHz**

megahertz

**MILSATCOM**

military satellite communications

**MSS**

mobile satellite services

**MWR**

morale, welfare, and recreation

**NAF**  
nonappropriated funds

**NAFI**  
nonappropriated fund instrumentalities

**NATO**  
North Atlantic Treaty Organization

**NEC**  
Network Enterprise Center

**NETCOM**  
Network Enterprise Technology Command

**NGB**  
National Guard Bureau

**NIPRNET**  
Non-secure Internet protocol router network

**NSA**  
National Security Agency

**OCONUS**  
outside the continental United States

**OMS**  
organizational messaging service

**OSD**  
Office of the Secretary of Defense

**OSP**  
outside plant

**PAO**  
public affairs officer

**PDA**  
personal digital assistant

**PED**  
portable electronic device

**PKI**  
public key infrastructure

**PM**  
program manager

**PM I3C2**  
program manager - installation information infrastructure communications and capabilities

**POM**  
program objective memorandum

**PPS**  
precise positioning service

**PSTN**  
public switched telephone network

**RMF**  
risk management framework

**SATCOM**  
satellite communications

**SBU**  
sensitive but unclassified

**SCI**  
sensitive compartmented information

**SDB**  
satellite database

**SIPRNET**  
secure Internet protocol router network

**SNAP**  
system network approval process

**SPS**  
standard positioning service

**SSC**  
SATCOM support center

**SSRA**  
spectrum supportability risk assessment

**STIG**  
security technical implementation guide

**T&E**  
testing and evaluation

**TCO**  
telephone control officer

**TDM**  
time-division multiplex

**UC**  
unified capabilities

**UCR**  
unified capabilities requirements

**URL**  
uniform resource locator

**USACE**  
United States Army Corps of Engineers

**USARCYBER**  
U.S. Army Cyber Command

**USC**  
United States Code

**USSTRATCOM**  
United States Strategic Command

**VoIP**  
voice over Internet protocol

**VoSIP**  
voice over secure Internet protocol

**VTC**  
video teleconference

**WGS**  
wideband global satellite



**WPS**

wireless priority service

**Section II****Terms****Activity**

A unit of effort that, when executed, produces a useful result. Activities are composed of one or more tasks. Within the context of the Army Enterprise Architecture, 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.

**Application**

Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, or facilitating email. For purposes of reporting in APMS, applications may be reported as a separate investment or included in an IS registration. If reported as a separate investment, applications will identify in the dependency tab, the host system it resides on as the parent IS.

**Army business enterprise architecture**

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

**Army enterprise architecture**

See also enterprise architecture. The AEA transforms operational visions and associated required capabilities of the business and warfighting missions into a blueprint for an integrated and interoperable set of information systems and NSS that implement horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA supports the LandWarNet and is the combined total of all the Army's operational, technical, and system architectures.

**Army enterprise infrastructure**

The systems and networks that comprise the LandWarNet.

**Army Reserve Network II**

ARNet II is a separate network providing LandWarNet services that connect the United States Army Reserve to the DISA DODIN.

**Army website**

A collection of hypertext markup language 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 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 Network Enterprise Center. 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, PDAs, 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 Army Enterprise Architecture 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. The ability to achieve a desired effect under specified standards and conditions.

**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.

**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.

**Compliance**

A system that meets, or is implementing an approved plan to meet, all applicable Technical Architecture mandates. A condition in which a person or a system meets applicable mandates, such as standards, policies, and procedures.

**Defense Telephone System**

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

**Department of Defense Information Network**

The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

**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 enterprise architecture includes baseline architecture, target architecture, and a sequencing plan (44 USC 3601).

**Enterprise license agreement**

An IT license or an Enterprise Services Agreement that has been required and validated by two or more ACOMs or Army staff elements, and whose designation as an enterprise asset would lead to economies of procurement at sufficient

levels to warrant consolidation of the license or service with the CIO in conjunction with contract support provided by the Army Contracting Command-designated offices and programmatic support from CHSS.

**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.

**GuardNet**

GuardNet is the IT infrastructure of the National Guard, securely supporting the NGB Joint team with nationwide information systems 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.

**Hardware**

The generic term that describes physical items, as 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 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 information management 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 information management processes and resources that enable the organization's business and mission processes.

**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).)

**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 Clinger-Cohen Act).

**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.

**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.

**Internet service provider**

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

**Interoperability**

The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.

**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.

**Land Warrior Network**

The Army's portion of the DODIN. LandWarNet is a universally accessible, standardized, protected, and economical network enterprise. LandWarNet seamlessly delivers network capabilities and services supporting the Army's Joint, inter-agency, intergovernmental, multinational operations, and business missions.

**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.

**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 Partners**

Those with whom the DOD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

**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 information system 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 Clinger-Cohen Act).

**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.

**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.

**Organizational messaging**

Correspondence used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies official position, or issues official guidance is considered an organizational message.

**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 website (or public website) on the World Wide Web**

Army website with access unrestricted by password or PKI user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a website 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 6250.01E).

**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.

**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.

**Software**

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

**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 SATCOM capabilities.

**Unified capabilities**

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

**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, facilities, and policy 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.

**Voice precedence**

A designation assigned to a message by its originator to indicate to communications personnel the relative order of handling, and to the addressee the order in which the message is to be noted. The ascending order of precedence for military messages is ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH OVERRIDE.

**Website**

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 website can mean a single HTML file or hundreds of files placed on the Internet by an enterprise.

**Web portals**

Websites 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.

**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”).

**UNCLASSIFIED**

**PIN103366-000**