

Information Management
Information Technology Support and Services

*This pamphlet supersedes AE Pamphlet 25-1, 6 September 2012.

For the Commander:

JAMES C. BOOZER, SR.
Major General, GS
Chief of Staff

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This pamphlet provides guidance and best business practices for implementing the standards and policy in AR 25-1 with AE Supplement 1.

Summary of Change. This revision directs users to the USAREUR homepage to determine units that are authorized preferred subscriber service (table 2).

Applicability. This pamphlet applies to Army organizations in Europe and other organizations using Army in Europe networks.

Forms. This pamphlet prescribes AE Form 25-1D, AE Form 25-1F, AE Form 25-1G, AE Form 25-1H, AE Form 25-1J, and AE Form 25-1K. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at <https://aepubs.army.mil/>.

Suggested Improvements. The proponent of this pamphlet is the Policy and Programs Branch; Programs, Policy, and Projects Division; Office of the Deputy Chief of Staff, G6, HQ USAREUR (DSN 370-7792). Users may send suggested improvements to this pamphlet by e-mail to the USAREUR G6 (AEIM-A) at usarmy.badenwur.usareur.mbx.g6-policy@mail.mil.

CONTENTS

SECTION I GENERAL

1. Purpose
2. References
3. Explanation of Abbreviations

SECTION II KNOWLEDGE MANAGEMENT

4. Knowledge Management Portal Access and Operation

SECTION III MANAGEMENT

5. Information Management Officer
6. Microsoft Enterprise License Agreement
7. Army in Europe Information Technology Training Program
8. Army in Europe Telephone Control Officer Program
9. Exception to Policy for Increased Mailbox Size

SECTION IV ARMY IN EUROPE ENTERPRISE ARCHITECTURE

10. Army in Europe Enterprise Architecture

SECTION V COMMAND, CONTROL, COMMUNICATION, AND COMPUTERS/INFORMATION TECHNOLOGY SUPPORT AND SERVICES

11. Network Remote Access
12. Video-Teleconferencing
13. Spectrum Management
14. Long-Haul and Deployable Communications
15. Defense Switched Network (DSN 99 and DSN)
16. Preferred Subscriber Service Authorization
17. Precedence Dialing Authorization
18. Cell Phones
19. BlackBerry Devices
20. Voice Over Internet Protocol (VoIP)
21. Requesting Base Communications Service
22. Managing Official Commercial Telephones
23. Telephone Abuse
24. Telephone-Call Control Numbers
25. Integrated Services Digital Network (ISDN) in Quarters

Appendix

A. References

Tables

1. Comparison of Classes of Telephone Service
2. Positions in Army in Europe Units Authorized Preferred Subscriber Service
3. HQ USAREUR Positions Authorized Preferred Subscriber Service
4. Army in Europe DSN Precedence-Dialing Authorization Table
5. Telecommunications Ordering Offices (TOOs)

Figures

1. Sample IMO Appointment Order
2. Sample Memorandum for Trusted Agent Assignment and Responsibilities
3. Sample Request for Exception to Policy (Increase Mailbox Size)
4. Frequency Request Chain of Approval
5. Frequency Manager's Planning Tool

Glossary

SECTION I

GENERAL

1. PURPOSE

This pamphlet provides guidance for information management officers (IMOs), telephone control officers (TCOs), and other information technology (IT) and telecommunications managers. It also describes duties, guidance, and associated procedures for obtaining and maintaining information management (IM) and telecommunications equipment and services.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

SECTION II

KNOWLEDGE MANAGEMENT

4. KNOWLEDGE MANAGEMENT PORTAL ACCESS AND OPERATION

a. The Army in Europe Knowledge Management (KM) NIPRNET and SIPRNET portals do not replace Army Knowledge Online (AKO). The portals are primarily business-process oriented. They will be used as a tool to help evaluate and refine business processes in order to maximize customer support while minimizing the consumption of resources required for delivering products and services.

b. The USAREUR G6 has established the KM portal on the Army in Europe computer networks as an adjunct to AKO and Defense Knowledge Online (DKO). The KM portal is used primarily as a business tool that allows individuals to share information and collaborate. Additionally, it is used as a tool to help evaluate and refine business processes in order to maximize customer value while minimizing the consumption of resources required for delivering products or services. KM portals are available on both the NIPRNET and the SIPRNET. The URL for the NIPR portal is *https://portal.eur.army.mil*. The URL for the SIPR portal is *http://portal.eur.army.mil*.

c. Another benefit of using the KM portals is a more efficient use of bandwidth by storing large files on the portals instead of sending them as attachments through e-mail. The sender is required to include only the URL for the attachment in the e-mail, enabling the recipient to go straight to the stored document on the portal. KM improves the ability of all Army in Europe organizations to collaborate with one another, share information in a timely manner, and maintain an orderly structure.

d. The Army in Europe KM NIPRNET and SIPRNET portals are managed by the Joint and Coalition Information Systems (JCIS) Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR. The JCIS Division will perform the daily operations and maintenance functions of the portal as well as assist customers with new requirements.

e. Because of security restrictions, access to the KM portals requires the user to have a EUR domain account. Users desiring access to portal resources who do not have a EUR domain account may contact the Enterprise Service Desk (ESD) by dialing DSN 119. All users with a EUR domain account should automatically have access.

f. The KM portals were developed in Microsoft (MS) SharePoint. Users can receive training in MS SharePoint through the Army in Europe Information Technology Training (AE-ITT) Center. A list of courses can be found on the AE-ITT website at <https://itt.eur.army.mil>.

SECTION III MANAGEMENT

5. INFORMATION MANAGEMENT OFFICER

The role of the IMO becomes paramount as the Army in Europe transitions to newer and more mobile missions and roles to meet the threat posed by overseas contingency operations and challenges imposed by a host of cause-and-effect situations such as weather, humanitarian efforts, and regional crises. IMO roles and responsibilities are addressed in DA Pamphlet 25-1-1, paragraph 6-5; and AE Supplement 1 to AR 25-1. Figure 1 is a sample IMO appointment order.

6. MICROSOFT ENTERPRISE LICENSE AGREEMENT

Trusted agents are requested by members of the network enterprise center (NEC) to provide accountability and sustainability of MS products and services in support of the MS Enterprise License Agreement (ELA) contract. Approved memorandums will be forwarded to the USAREUR G6 (AEIM-A) for processing. Figure 2 is a sample memorandum.

Organizational Letterhead

OFFICE SYMBOL

Date

MEMORANDUM FOR *Local Director of Information Management*

SUBJECT: Designation of an Information Management Officer for the *Organization/Unit*

1. Effective *date*, I appoint the below-named individual as an information management officer (IMO) for the *organization/unit* to perform IMO functions according to AE Supplement 1 to AR 25-1.

a. IMO Name:

Grade:

DEROS:

Military occupational specialty:

Civilian job specialty code:

Contractor (yes/no):

b. Organization:

Unit's major subordinate command (MSC):

Unit's Department of Defense activity address code (DODAAC):

Supporting network enterprise center:

City/Country:

Kaserne:

DSN Telephone Number:

AKO e-mail address (unclassified):

c. Additional Information:

Authorized to submit information technology (IT) acquisition requests (yes/no):

Authorized to submit requests for Microsoft enterprise licenses (yes/no):

Agreement products (yes/no):

2. Authority: AR 25-1 and AE Supplement 1, Army Knowledge Management and Information Technology.

3. Purpose: To perform duties according to the references in paragraph 2.

4. Special Instructions:

a. This appointment supersedes all previous appointments to this duty and remains in force for 1 year or until the appointee is officially relieved or released from appointment, whichever comes first.

b. The appointee must understand DOD, Army, and Army in Europe policy; have a working knowledge of IT principles, techniques, hardware, and software; and have knowledge and an understanding of IT acquisition.

c. Newly assigned IMOs must complete IMO certification training within 90 days after being appointed. The appointee will contact the Army Europe Information Technology Training Office for available courses and registration procedures.

Commander or director
(Colonel, GS-15, or above)

CF:
USAREUR G6 IAPM

Figure 1. Sample IMO Appointment Order

Organizational Letterhead

OFFICE SYMBOL

Date

MEMORANDUM FOR USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351

SUBJECT: Trusted Agent Assignment and Responsibilities

1. In accordance with AR 25-1, this organization is in compliance with and will continue adhering to the following requirements for trusted agents regarding the accountability and sustainability of Microsoft (MS) software products and services in support of the MS Enterprise License Agreement (ELA) contract.

a. The agent must be assigned on orders or be employed as a systems administrator, information management officer (IMO), information assurance officer, or to other duties within the Army Knowledge Management, information technology, or information assurance field of expertise.

b. The agent is responsible for but not limited to direct downloads of MS software and product information available from the Computer Hardware, Enterprise Software, and Solutions (CHESS) and applicable Internet and intranet links.

c. The agent will ensure that his or her IMO assigned to order specific MS software applications through the CHESS webpage at <https://chess.army.mil> complies with all Army in Europe, Army, and DOD regulations pertaining to information management and license agreements.

d. The agent will maintain accountability for MS software distribution within his or her area of responsibility and report any misuse of the applications to his or her S3.

e. The agent will be responsible for ensuring the software distribution is in compliance with current Army in Europe policy and procedures.

f. The agent is responsible for sustaining MS software application update and upgrade support to his or her requesting IMOs.

g. The agent will ensure all expired or outdated application materials are destroyed in accordance with AR 25-1, paragraph 6-2k(4).

h. The assigning organization will ensure training on applications is provided.

2. Trusted Agent:

a. Name:

b. Signature:

c. Unit/Organization:

d. Organization mailing address:

e. E-mail address:

f. Duty telephone:

3. For immediate changes to the trusted agent-assigned personnel, contact the MS ELA POC by e-mail at mail.g6.acquire@eur.army.mil.

4. Verification of Trusted Agent: I hereby officially appoint the aforementioned individual as a trusted agent until further notification by a designated representative or myself. I can be contacted at *duty telephone*.

NEC

Figure 2. Sample Memorandum for Trusted Agent Assignment and Responsibilities

7. ARMY IN EUROPE INFORMATION TECHNOLOGY TRAINING PROGRAM

a. All USAREUR major subordinate and specialized commands and United States Army garrison organizations are required to use the AE-ITT program as the primary source for all instructor-led IT and information assurance (IA) training. The program—

(1) Provides cost-effective training solutions and mobile training as required.

(2) Is available at seven strategic locations throughout Europe to minimize the requirement for temporary duty (TDY) travel.

(3) Meets all requirements of DOD Directive 8570.01 by providing certified trainers and a variety of IT and IA courses. All seven training centers are testing sites for Pearson Virtual University Enterprise and ProMetric certifications that meet commercial industry standards.

(4) Ensures the Army Training and Certification Tracking System (ATCTS) is updated and accurately reports certifications, as required by DOD directives and the Federal Information Security Management Act. The program aligns and updates course completions and certificates in ATCTS at <https://atc.us.army.mil/iastar/login.php>.

b. Based on IA position-validation or command-determined training requirements, coordination with the AE-ITT POC at the Policy, Programs, and Training Branch; Information Assurance Program Management Division; Office of the Deputy Chief of Staff, G6, HQ USAREUR, will be necessary to determine training costs and locations, as well as scheduling and training requirements. Additional updates, information, and guidance are available at <https://itt.eur.army.mil/>.

8. ARMY IN EUROPE TELEPHONE CONTROL OFFICER PROGRAM

a. General. AR 25-1 requires that all units manage and conserve telecommunications assets. Unit commanders are responsible for the conservation of unit telecommunications. Unit TCOs are responsible for managing unit telecommunications for the commander.

b. Introduction. Units are required to have a TCO to manage telecommunications assets. To provide increased accountability, TCOs will be appointed at every level where program oversight and control is required. Dial central offices (DCOs) will normally receive automated local service requests (LSRs) that are verified through a valid Configuration Accounting and Information Retrieval System (CAIRS), but will not process the hard-copy DA Form 3938 unless CAIRS is not working or there is an emergency. DA Form 3938 must be submitted by the unit TCO or the alternate TCO.

NOTE: Because of the amount of work performed by the IMO and the TCO, responsibilities for these positions should not be assigned to the same individual.

c. Unit TCO Responsibilities.

(1) TCOs will manage unit telecommunications assets by—

(a) Monitoring DSN and commercial access (“99”) use and checking for abuse and inaccuracies.

(b) Monitoring detailed bills for cell phones and checking for unusually long calls and unofficial calls (for example, patterns of calls to civilian numbers).

(c) Issuing telephone control numbers to users (for limited commercial access), monitoring the use of these numbers, and obtaining a list of valid control numbers from the head telephone operator.

(d) Reviewing DSN-precedence use (if any) to ensure the precedence level is being used according to prescribed guidelines.

(e) Reviewing the use of official commercial telephones and fax machines using AE Form 25-1F.

(f) Ensuring the servicing DCO has an accurate list of unit-telecommunications services with the correct unit account code and the identification of all telephone lines by function. DCOs will periodically send unit TCOs a list of the DSN services the DCO believes the unit uses.

(g) Reviewing itemized calling-card bills from vendors to ensure accuracy and to check the nature of the calls.

(h) Ensuring that DSN service is not used with modems for dial-up into data services unless absolutely necessary and then only for a limited period. Dial-ups used for data transfer are very expensive and may violate security regulations (for example, if the computer used to dial-up is also connected to a Government local area network (LAN)).

(i) Reporting found or suspected misuse, abuse, and overuse to the unit commander and the supporting NEC.

(j) Obtaining personal identification numbers (PINs) for unit morale calls from the Unit Morale Call PIN Issuing Resource Europe (UMPIRE) System. AE Regulation 25-22 provides more information.

(k) Validating the unit's continuing need for telecommunications services. In particular, the TCO will—

1. Ensure that users of DSN and 99 access do not have higher access than needed to accomplish their mission, and validate the continuing need.

2. Validate the authorization and continuing need for cell phones, pagers, and BlackBerry devices and services.

3. Validate the continuing need for official commercial telephone service.

4. Validate the continuing need for fax machines.

5. Validate the authorization and continuing need for telecommunications services in quarters (preferred subscriber service (PSS)). TCOs will ensure that direct commercial access in quarters is not available as part of this service.

6. Ensure all long-haul (for example, DSN, Defense Red Switch Network (DRSN)) and fixed commercial services, integrated service digital network (ISDN), digital subscriber line (DSL), and Cable News Network (CNN) services have been canceled when a unit permanently relocates or deactivates. TCOs will also ensure all wireless services (cell phone, BlackBerry) are canceled when the unit deactivates or leaves the theater. The USAREUR G3 webpage at <http://g3operations.hqusareur.army.mil/StageCheckList/startup/default.htm> provides more information.

7. Ensure that connections to the DRSN (if any) are still required at their current location.

8. Ensure the servicing DCO has an accurate list of existing unit telecommunications services and ownership at a functional level. DCOs will periodically send unit TCOs a list of the services the DCOs believe the units own. Unit TCOs will confirm that those services belong to their unit and will give the servicing DCOs confirmation and corrections if necessary.

9. Review telecommunications services provided in quarters to ensure that those services are being used for official business and the current occupant is authorized the service.

10. Maintain a database of unit DSN telephone numbers and report errors in the Army in Europe Telephone Directory at <https://aepubs.army.mil/ae/public/links.aspx> to the unit webmaster.

(2) TCOs are responsible for—

(a) Requesting the addition, modification, and cancellation of installed telecommunications services (base communications (BASECOM) and long-haul) as necessary.

(b) Providing the USAREUR Telecommunications Programs Manager a copy of their appointment orders and a signature card.

(c) Initiating automated LSRs using the current ordering system.

(d) Processing DD Form 448 and DA Form 3953 for BASECOM services.

(e) Managing other long-haul services such as dedicated circuits.

(f) Requesting PINs for morale calls through the web-based UMPIRE system. AE Regulation 25-22 provides more information.

(g) Requesting telephone control numbers for one-time use connections.

9. EXCEPTION TO POLICY FOR INCREASED MAILBOX SIZE

a. Individuals who have a valid requirement for increasing the standard 100 megabyte (MB) limit for e-mail will do the following:

(1) Call the ESD at 119. The ESD will create a trouble ticket and send an e-mail back to the user with the trouble-ticket number.

(2) Submit a memorandum by e-mail to mail.g6.acquire@eur.army.mil, referencing the trouble ticket and providing a description of his or her requirement. The user must describe why the increase in storage is needed and explain why a personal storage table (.pst) file cannot be used. A sample memorandum is at figure 3.

b. The Policy and Programs Branch; Programs, Policy, and Projects Division; Office of the Deputy Chief of Staff, G6, HQ USAREUR will notify the user if the request is approved or disapproved.

c. Individuals should allow 3 to 5 business days for the request to be processed.

Organizational Letterhead

OFFICE SYMBOL

Date

MEMORANDUM FOR USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351

SUBJECT: *Mailbox holder's name*, Request for Exception to Policy (Increase of Mailbox Size)

1. References.

- a. AR 25-1 and AE Supplement 1, Army Knowledge Management and Information Technology.
- b. NSS Remedy Ticket Number: (*obtained from the Army in Europe Enterprise Service Desk 119 online*).

2. I request that the limit of the mailbox be increased to *number* MB for *name, rank or grade, position, title*.

3. *Provide a justification (for example, explain why the .pst file on the personal computer hard drive is not being used to store mail as it provides a greater storage capacity than the standard 100-MB mailbox on the server).*

4. The POC for this action is *name*, DSN ###-#### or e-mail: *name*@us.army.mil.

(Supervisor's signature)
Supervisor's name
Grade
Position title

Figure 3. Sample Request for Exception to Policy (Increase Mailbox Size)

SECTION IV

ARMY IN EUROPE ENTERPRISE ARCHITECTURE

10. ARMY IN EUROPE ENTERPRISE ARCHITECTURE

The USAREUR G6 established the Enterprise Architecture Branch, Architecture Division, for the development of a strategic information asset base, which defines the mission, the technologies necessary to perform the mission, and the transitioned processes for implementing new technologies in response to changing mission needs in compliance with DA guidance established in AR 25-1. The outcome of this effort is referred to as the Army in Europe Architecture, which consists of USAREUR and IMCOM-Europe Architecture products that are in compliance with Department of Defense Architecture Framework (DODAF) version 1.5. Army in Europe customers will use the Army in Europe Architecture as the single-source reference for developing IT operational requirements. IMCOM-Europe-generated architecture views and products will support strategic IT asset identification and the transformation to Single NEC, the network service center construct, and other transformation efforts.

a. Army in Europe Architecture. The Army in Europe Architecture concept helps ensure that effective and efficient linkage exists between operational needs and the underlying information technologies that support operations. Army in Europe Architecture products provide a means to distribute information and facilitate the development of operational and technical objectives for the Army in Europe. This includes documenting and reporting information about—

- (1) Organizational structures.
- (2) Organization activities and functions.
- (3) IT systems that support organization activities and functions.

b. The Army in Europe Enterprise Architecture Development Process. Architecture development facilitates problem-solving and decisionmaking. The Army in Europe Architecture was developed in compliance with DODAF version 1.5, which distributes architecture artifacts across separate but integrated views. These include the following:

- (1) Operational views that identify operational requirements and capabilities.
- (2) System views that relate systems and characteristics to operational needs.
- (3) Technical views that describe prescribed standards and conventions.

c. DODAF. The intent of the DODAF is to ensure that architecture descriptions can be compared and related across organizational boundaries, including joint and multinational boundaries. This common language and architecture-description format enables the Army in Europe Architecture to integrate architecture products and objective operations with USEUCOM for theater operations as well as with the United States Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC(A)) for network operations activities and systems.

(1) The Enterprise Architecture Branch uses the architecture development process as outlined in the DODAF framework to—

- (a) Determine the intended use of the architecture.
- (b) Determine the scope of the architecture.
- (c) Determine the data required to support the architecture development.
- (d) Collect, organize, correlate, and store architecture data.
- (e) Conduct analyses in support of architecture objectives.
- (f) Document results according to the architecture framework.

(2) Part of this process is ensuring that the architecture is relevant and kept up to date. Periodic reviews of the architecture are conducted on a cyclic basis and updates are captured as necessary.

(3) The Enterprise Architecture Branch uses DODAF version 1.5. (DODAF version 2.0 will be implemented once released.)

d. Army in Europe Enterprise Architecture in Support of Army in Europe Transformation.

(1) The Army in Europe Enterprise Architecture enables the Enterprise Architecture Branch to provide customers tailored reports that enable them to analyze a potential problem set. The Enterprise Architecture Branch has used the Army in Europe Architecture to provide analysis tools to help with transformation planning and objectives based on architecture information. Consumers of architecture information want to see specific analyses, data, and products that they can recognize and use. Based on customer needs, the Enterprise Architecture Branch queries architecture data and produces formatted reports and analyses to help answer questions and propose solutions. Customers often serve as subject-matter experts (SMEs) in their respective domains and, with their participation, architecture information can be validated and enhanced. Sharing architecture products and information with SMEs will improve overall content and better support needs across the command.

(2) Once subordinate organizations become modular, they become operationally focused, which requires complex planning and execution of new organizational structures, roles and responsibilities, and enabling technologies. Army in Europe Architecture information and products can assist transformation planners by providing graphic representations of organizations, activities, and systems. Associated data and gap analyses will help evaluate the effect of change on command operations, personnel, and the systems that support them. Innovations in enabling technologies and the realignment of roles and responsibilities are examples of the Army executing transformation with the intent of achieving an Objective Force.

(3) The Enterprise Architecture Branch functions as the primary point of presence for Enterprise Architecture products in Europe by facilitative and collaborative processes to arrive at standardized tools and methodologies for use in USAREUR and 5th Signal Command to create, maintain, and use architectural artifacts.

(4) The Enterprise Architecture Branch promotes and supports Army KM efforts by providing an infrastructure and data repository to leverage architecture capabilities.

e. Products Available in the Army in Europe Architecture. The following products are available in the Army in Europe Architecture:

(1) Command, control, communications, computers, and information management (C4IM) services.

(2) Network operations activities.

(3) Organizational structures for Army in Europe organizations.

(a) Modification table of organization and equipment (MTOE) roles (HQ USAREUR).

(b) Augmentation table of distribution and allowances (TDA) roles (USAREUR G6 only).

(c) Mobile subscriber equipment (MSE) roles.

(4) Operational activities and organizational functions for USAREUR.

(5) Organizational structures for the Stryker brigade combat team (SBCT) and the military intelligence brigade (MIB).

- (6) Operational activities for SBCT and MIB.
- (7) Organizational structure for 5th Signal Command (headquarters only).
 - (a) MTOE roles.
 - (b) Augmentation TDA, MSE, and local national roles.
- (8) Operational activities for 5th Signal Command (headquarters only).
- (9) System Architecture products (general system information for the Army in Europe).
 - (a) High-level core mission area systems.
 - (b) Network backbone infrastructure devices.
 - (c) General post, camp, and station system devices.
 - (d) Architectural products developed to support specific projects and exercises.

SECTION V COMMAND, CONTROL, COMMUNICATION, AND COMPUTERS/INFORMATION TECHNOLOGY SUPPORT AND SERVICES

11. NETWORK REMOTE ACCESS

a. A “remote user” is a person who enters the Army in Europe NIPRNET from outside the physical or logical boundary of the internal LAN. The remote-access system creates a protected extension of the Army in Europe NIPRNET for authorized remote users. The NIPRNET remote-access system has the following components:

(1) **Access to the Network.** Users will connect through either the Terminal Server Access Control System (TSACS) or a commercial Internet service provider that provides dial-up, broadband, wireless, or leased-line services using a virtual private network (VPN). TSACS and these other network connections provide unencrypted connections to the network.

(2) **VPN.** The primary function of VPN is to encrypt the path from the user to the network. VPN will allow remote users to—

(a) Protect Army information that is sent and received during remote communications with other users and servers on the Army in Europe NIPRNET.

(b) Use the applications available to them in their normal office environment.

b. Remote access to the Army in Europe NIPRNET will be used only for official business.

(1) Remote access to the Army in Europe SIPRNET will tunnel the Type 1 encrypted connection through the 5th Signal Command-managed VPN architecture and use a 5th-Signal-Command-managed Type 1 as its entry point to the SIPRNET.

(2) Remote users will be subject to monitoring, and their connection will be terminated if it causes damage to any part of the network or if their computer is not configured correctly. Personnel who abuse or misuse remote-access capabilities may be disciplined in accordance with the Uniform Code of Military Justice or Office of Personnel Management directives, and may have their remote-access account terminated.

c. Only commanders who are captains and above or civilian equivalent supervisors (GS-13 and above) may approve requests for remote access. These approval authorities will also be responsible for—

(1) Pre-approving reimbursement for TDY or remote-access connection charges at the user's home station.

(2) Setting specific limits when pre-approving reimbursement for connection charges in (1) above. Generally, home-station remote-access users should not be reimbursed, because they normally can return to their office.

(3) Paying approved reimbursements for remote-access charges with internal operations and maintenance funds.

d. IMOs will—

(1) Use the appropriate Army in Europe remote-access request form (AE Form 25-1H or AE Form 25-1J) to request approval for remote access from their supporting NEC.

(2) Keep completed forms in (1) above in unit records and coordinate new and deleted accounts with the supporting NEC.

e. Employee-owned information systems are prohibited from connecting to the Army network for any purpose.

f. Army in Europe remote-access request forms (categories 1 and 2) will be used by personnel in Europe to request remote access to the Army in Europe NIPRNET.

(1) The category-1 form (AE Form 25-1H) will be used by DOD military personnel, DOD civilian employees, and permanently hired contractor personnel assigned to DOD agencies stationed in the European theater.

(2) The category-2 form (AE Form 25-1J) will be used by contractor personnel who are temporarily hired to accomplish specific official tasks that require remote access to the network.

(3) The forms must be completed by the requesting user, the unit IMO, and the approving authority (either a commander in the minimum grade of captain or a civilian equivalent supervisor (GS-13 and above)).

(4) Commanders approving remote access for their personnel must provide correctly configured Government-owned information systems to each user. AE Form 25-1K will be used to ensure and document correct equipment and configuration.

(5) The contracting officer's representative will also complete part of the category 2 form to validate that the requesting user is assigned to the contract and has an official requirement to remotely connect to the network.

(6) After the form has been completed and approved, the unit IMO will use it to complete an account request with the supporting NEC.

(7) AR 25-400-2 requires that these forms be maintained in official unit files until the account is terminated or closed by the IMO in coordination with the supporting NEC.

12. VIDEO-TELECONFERENCING

a. Introduction. This paragraph prescribes responsibilities and procedures for establishing and operating video-teleconferencing (VTC) systems in the Army in Europe.

(1) All multipoint VTCs with CONUS require connectivity through DVS-G, either through the Army in Europe hubs to the DVS-G, or directly to the DVS-G. To use the hubs, the VTC equipment must be registered with the Defense Information Systems Agency (DISA) (<http://www.disa.mil/Services/Network-Services/DISN-Connection-Process>). Once registered, VTC site managers can schedule VTC sessions online at <https://dvsops.scott.disa.mil>.

(2) All multipoint VTCs in the Army in Europe should be connected through the Army in Europe hubs. Once registered with the USAREUR G6, VTC facilitators can schedule VTC sessions by sending an e-mail message to usarmy.badenwur.usareur.mbx.g3-mcsd-vtc-schedulers@mail.mil.

(3) Army in Europe VTC systems must interoperate with other theater systems. This pamphlet defines acceptable communications methods, standards, and requirements for using VTC systems in the Army in Europe.

(4) VTC equipment will be procured through the IT technical validation process. AE Supplement 1 to AR 25-1, paragraph 3-8, provides more information.

(5) The Plans and Engineering Division, Office of the Deputy Chief of Staff, G3, Headquarters, 5th Signal Command, provides theater-level engineering support to the Army in Europe.

(6) 5th Signal Command, through a contract with Operation, Maintenance, and Supply - Europe, provides operation and maintenance to two Army in Europe VTC hubs in Heidelberg and Kaiserslautern, Germany.

b. Army in Europe Registration Procedures.

(1) Every Army in Europe VTC coder/decoder (CODEC) must be registered with the USAREUR VTC Program Manager (DSN 370-7346). The following documents are required for registration:

(a) A memorandum signed by the unit's designated approval authority. Electronic signatures are accepted.

(b) CODEC information (formerly AE Form 25-1D).

(c) VTC equipment location diagram.

(2) If electronic resources are not available, these documents may be sent by fax to DSN 370-8889 or civilian 06221-57-8889. The documents should be sent to the attention of the USAREUR G6 VTC Program Manager.

c. Standards. To ensure interoperability, Army in Europe organizations and tenant activities will procure and operate only standards-compliant VTC systems as indicated in (1) through (3) below. Questions on VTC equipment standards and compatibility requirements should be directed to the USAREUR G6 VTC Program Manager (DSN 370-7346).

(1) H.320 is the prevalent DOD standard for group and conference-room facilities that operate over ISDN telephone lines.

(2) H.323 is the DOD standard for VTC and data collaboration over Internet protocol (IP) data networks. This standard is associated with personal computer-based desktop VTCs. Large CODEC units, however, can also connect by IP as long as the system has been accredited by the USAREUR G6 Information Assurance Program Manager (IAPM). Instructions can be found at <https://portal.eur.army.mil/pages/default.aspx>. Because IP networks do not guarantee high-quality service, H.323 works well only on networks with high bandwidths and light traffic loads.

(3) The KIV-7 is the standard encryption device for secure dial-up VTC in the Army in Europe and must be procured with all new secure VTC systems. Exceptions to this policy must be coordinated with and approved by 5th Signal Command (NETC-SEC-O) (DSN 337-8614/8221).

d. Methods of Communication.

(1) The prevalent method of communication for VTC systems in the Army in Europe is commercial dial-up ISDN. ISDN is a digital telephone service that provides a 128 kilobyte-per-second (kb/s) channel. Two or three ISDN lines are usually bundled with a multiplexer (for example, inverse multiplexer (IMUX)) to provide either 256 kb/s or 384 kb/s VTC links.

(2) For H.320 VTC, Army in Europe VTC hubs operate at a data-transmission speed of 256 kb/s. Future upgrades to the hub will enable users to use VTC at different speeds. VTC users who need to use the hub should have at least two ISDN basic-rate interface connections for each H.320 system. An IMUX, which bonds or merges multiple 128 kb/s channels to provide a higher bandwidth connection, is also required. User IMUXs must support Bonding Mode 1.

(3) In the Army in Europe, H.323 VTC is performed over the Army in Europe SIPRNET. Both Army in Europe hubs are equipped to support IP multipoint sessions with an IP gateway. The use of H.323 VTC places heavy demands on data networks, which must be designed to support this application. IP networks are designed to communicate data, such as e-mail and file transfers. These networks tend to transmit bursts that are relatively insensitive to network-transmission delay and packet loss. In contrast to data, real-time audio and video communications are sensitive to transmission delay and packet loss, which causes poor audio and video quality. H.323 devices produce a continuous stream of IP packets that can congest networks and reduce performance. Successful transmission of real-time audio and video over IP networks requires the following:

(a) Networks with enough bandwidth to support H.323 traffic and essential-data transfer.

(b) Network protocols to reduce transmission delay, prioritize VTC traffic, and improve throughput. These network protocols must be implemented across the entire network that the VTC traffic will traverse in order to be effective.

(c) Controls on the number of H.323 terminals simultaneously using the network. (The H.323 gatekeeper provides terminal-access control.)

(4) Organizations are responsible for their internal LANs and may use H.323 VTC within the confines of their infrastructure.

(a) H.320 and H.323 gateways have been installed at Army in Europe hubs, enabling H.323 users to interface with H.320 systems.

(b) All H.323 connectivity must be made through the Army in Europe SIPRNET. Units that want to connect to the Army in Europe VTC hub using H.323 standards must first obtain a certificate to operate (CTO). CTOs may be obtained from the USAREUR G6. The unit information assurance officer and IMO must coordinate with the USAREUR G6 IAPM to obtain a CTO.

(c) H.323 VTC systems must be registered at <https://portal.eur.army.mil/pages/default.aspx>.

e. VTC Hubs. VTC hubs will—

(1) Provide secure, multipoint VTC service at the Secret level to designated registered users.

(2) Support DOD VTC standards.

(3) Provide service and support to registered users.

(4) Conduct weekly VTC preventive maintenance/quality assurance (PM/QA) sessions to provide registered users the opportunity to perform scheduled preventive maintenance on local equipment and to align and test audio and video quality in a VTC environment.

(5) Provide troubleshooting assistance by telephone to help operators identify, isolate, and solve problems while conducting VTCs through the VTC hubs. If a problem cannot be solved within a reasonable time and continues to disrupt overall VTC service, the VTC network operations center will place the user in a waiting room to solve the problem. Once the problem is solved, the user will rejoin the conference with the microphone muted.

f. VTC Suite Operators.

(1) As a minimum, registered VTC suite operators will—

(a) Connect to the VTC hub for system operational testing and audio- and video-alignment checks each week. Operators may also request individual testing directly from VTC hub technicians to meet local requirements.

(b) Perform preventive maintenance on site according to original manufacturer manuals and applicable technical manuals.

(c) Keep records of all preventive maintenance conducted.

(d) Participate in weekly PM/QA sessions that meet periodic testing requirements. In addition, a test session is required when any of the following occurs:

1. New equipment is installed (for example, CODEC, IMUX).

2. Equipment is relocated or repaired.

3. VTC hub technicians identify user audio or video problems. (Failure to perform tests may result in long delays when establishing VTC sessions.)

4. An encryption key is superseded.

(2) VTC suite operators can report malfunctions attributable to communications circuits to the Army in Europe VTC Network Operations Center, which is located at the Heidelberg hub. (Operators may call DSN 370-6848.)

g. Network Operations Center Assistance. The Army in Europe Secure VTC Facility operates a Network Operations Center Help Desk at Campbell Barracks in Heidelberg, Germany (DSN 370-6895/7530). The help desk can assist VTC operators during normal operating hours, which can be found at <https://portal.eur.army.mil/pages/default.aspx>. If a VTC needs to be conducted outside normal operating hours, the user must contact the Army in Europe Facility Control Officer.

h. Multipoint Control Units.

(1) A multipoint control unit (MCU) enables two or more users to participate in one VTC. The 5th Signal Command operates several classified (Secret) MCUs. These MCUs provide common-user, multipoint service to all VTC users in the Army in Europe, including tenant agencies. ISDN and IP connections are also possible.

(2) Because the Army in Europe VTC hubs provide common-user service throughout the Army in Europe, dedicated connections to the hub are permitted only to meet special circumstances (such as interface to tactical systems) and critical C2 requirements. The standard means of connecting to the hub is by ISDN.

(3) DISA provides MCU service to DOD VTC users in theater through its DVS-G facility at Patch Barracks in Stuttgart, Germany.

(a) The DVS-G offers two levels of security (Secret and unclassified) and provides the primary link to VTC users and facilities in CONUS and in other theaters. The DVS-G also provides links to other components and to NATO and foreign systems.

(b) Users must register with DISA before they may use DVS-G services. Registration and use of DVS-G is at no cost to individual users and organizations. ISDN and other circuit-connection fees are the responsibility of the using unit.

(4) MCU service in theater is considered a common-user communications service, similar to telephone service and data networks.

(a) Army in Europe organizations and tenant agencies may not purchase H.320 MCUs for internal USAG use.

(b) Units implementing large-scale H.323 projects on their internal LAN may install an H.323 MCU to provide multipoint conferencing on the LAN. Units that do so will be responsible for providing funds for, operating, and maintaining these systems. The USAREUR G6 will review and approve requests to purchase H.323 MCUs on an individual basis.

i. VTC Hub Registration.

(1) Organizations that plan to use the hub service must complete AE Form 25-1D for each of their facilities. This information is needed to provide high-quality service and for planning hub upgrades and expansion. Forms will be submitted either online or by fax (DSN 370-8889) to the USAREUR G6 VTC Program Manager for approval. Units may call DSN 370-7346 if they need help completing the form.

(2) Secure hub service also requires a copy of the VTC facility-accreditation documentation, including the cover memorandum signed by the requesting unit commander. Interim access to VTC services by nonaccredited VTC sites may be granted only if a statement is included from the unit security manager certifying that accreditation is being processed and providing an estimated accreditation date.

(3) After the USAREUR G6 receives and processes AE Form 25-1D, requesting units will be granted hub service and be posted on the USAREUR G6 VTC webpage as authorized users.

j. Secure VTC Communications Security (COMSEC) Procedures.

(1) VTC COMSEC custodians will obtain, load, and initiate appropriate COMSEC keys before COMSEC changeovers, which occur every 90 days. The 43d Signal Battalion will send a notification before each changeover that indicates the COMSEC changeover identification and duration. Notifications will be sent to all registered users using the POC address on the VTC-user's database.

(2) The 181st Signal Company COMSEC Material Direct Support Activity (DSN 370-8425) distributes COMSEC keys 5 workdays before changeovers. The COMSEC changeover occurs at 0001Z on the first day of each 3-month period.

(3) Registered users should contact the Army in Europe VTC hub at DSN 370-6848/6895 any time after the COMSEC changeover to conduct a test VTC. The test is needed to verify system connectivity and operation after loading or updating the appropriate COMSEC fills.

k. Scheduling Video-Teleconferences.

(1) The Office of the Deputy Chief of Staff, G3, HQ USAREUR, is responsible for scheduling VTCs bridged by Army in Europe VTC hubs. Requesting offices may contact the VTC scheduler at DSN 370-6942/7695 or e-mail: usarmy.badenwur.usareur.mbx.g3-mcsd-rtc-schedulers@mail.mil.

(2) The VTC scheduler will—

(a) Advise the requester of the resource, site, and available time for VTCs.

(b) Issue the requester ISDN dial-in numbers for each resource requiring that capability.

(c) Schedule and reserve DVS-G sites bridged through the Army in Europe hubs with the video operations center at least 48 hours before the scheduled date and time of the VTC if the conference requires DVS-G sites.

(d) Schedule a 30-minute preparation time at the start of each VTC for audio and video checks to be conducted by the host site. This preparation time may be increased on request.

(e) Schedule one of the Army in Europe VTC-hub monitoring systems, as available, for each VTC being bridged by the Army in Europe VTC hubs.

(f) Post all scheduled Army in Europe VTCs on the Army in Europe portal schedule calendar at <https://portal.eur.army.mil/pages/default.aspx>.

(3) The requesting office's POC will—

(a) Provide the name and telephone number of the VTC POC.

(b) Assume responsibility for identifying, notifying, and coordinating with requested sites and participants in the scheduled VTC.

(c) Coordinate with the scheduler and the appropriate hub.

(d) Authorize additions and other changes to the scheduled VTC.

(4) The VTC POC is responsible for providing participating dial-in sites their dialing numbers.

(5) VTC participants will—

(a) Dial in and connect with the hub for the scheduled VTC in a timely manner.

(b) Notify the VTC POC if their site must withdraw from the scheduled VTC.

(c) Notify the scheduler of any user additions, deletions, or conference cancellations.

(d) Adhere to VTC etiquette (<https://portal.eur.army.mil/pages/default.aspx>).

13. SPECTRUM MANAGEMENT

a. General. U.S. Armed Forces frequency-transmitting equipment in Europe requires approval by the host nation in which it is to be operated. Units will not operate equipment that requires the use of frequency spectrum without properly requesting and receiving authorization. Contact numbers are as follows:

Chief, FMO	DSN 370-6780
NCOIC, FMO	DSN 370-7469
Battlefield spectrum managers	DSN 370-3317
Satellite requests	DSN 370-3094

b. Temporary Frequency Requests. Temporary frequency requests are requests for frequencies to be used for 90 days or less. Procedures for submitting temporary frequency requests in the Army in Europe are as follows:

(1) Frequency requests must be submitted to the Frequency Management Office (FMO), Command, Control, Communications, Computers, Intelligence, and Surveillance Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR, through the Spectrum Management Analysis and Record Tracking System (SMARTS) or Spectrum XXI. Requests must be submitted at least 75 days before the exercise or event using the standard frequency action format (SFAF). Late requests may be disapproved. The unit or next higher headquarters frequency manager should be contacted for assistance.

NOTE: The 75-day standard was established based on a host-nation standard of 70 days (USEUCOM Spectrum Management Manual, chap 3, para 5.6.a), which is strictly enforced. Many units did not receive frequencies for their exercises because they did not submit their requests within the 70-day standard.

(2) If a unit's frequency request is submitted less than 75 days before the exercise or event, the unit S3 or G3 must submit written justification stating the reason why the unit's request is being submitted late. The justification must be written in memorandum format on unit letterhead stationery and include the following as a minimum:

- (a) An explanation as to why the request is being submitted late.
- (b) A description of the effect a disapproval of the request will have on the unit.
- (c) A description of the steps the unit will take to mitigate the risk of future late requests.
- (d) The signature of the first colonel (O6) in the chain of command.

(3) Justifications may be sent by e-mail (usarmy.badenwur.usareur.list.dl-g6-frequency-management-office@mail.mil).

c. Permanent Frequency Requests. Permanent frequency requests are requests for frequencies that are needed for more than 90 days. Requests must be submitted in SFAF using SMARTS or Spectrum XXI at least 185 days before the exercise or event for which the frequency is needed. Units will use the guidance in subparagraph b above for requests submitted less than 185 days before the event or exercise.

d. Processing Late Requests. The FMO is authorized to deny late requests. These requests, however, will be processed after the justification for the lateness is received. Late requests may not be approved by the host nation (National Allied Radio Frequency Agency (NARFA)).

e. Satellite Access Requests (SARs) and Gateway Access Requests (GARs). Requests to use satellite communications, frequencies, and equipment must be submitted in the proper SAR or GAR format. The leadtime for SARs and GARs is 90 days for super high frequency and 30 days for extremely high and ultrahigh frequency.

f. Frequency Request Hierarchy. Figure 4 provides the frequency-request hierarchy for units requesting frequencies through the approving authority (NARFA). Users should pay particular attention to the leadtimes on the far right of the figure. The FMO enforces the chain of approval.

g. Spectrum Manager. The spectrum manager—

- (1) Works directly with unit planners to forecast and plan for frequency requirements.
- (2) Coordinates frequency approval for new equipment fielding initiatives.
- (3) Assesses and validates frequency requests, and requests frequency assignments from USEUCOM and the host nation.
- (4) Enforces leadtime standards for frequency requests.
- (5) Researches and returns unused frequencies to the host nation.
- (6) Trains and assists subordinate command frequency managers.

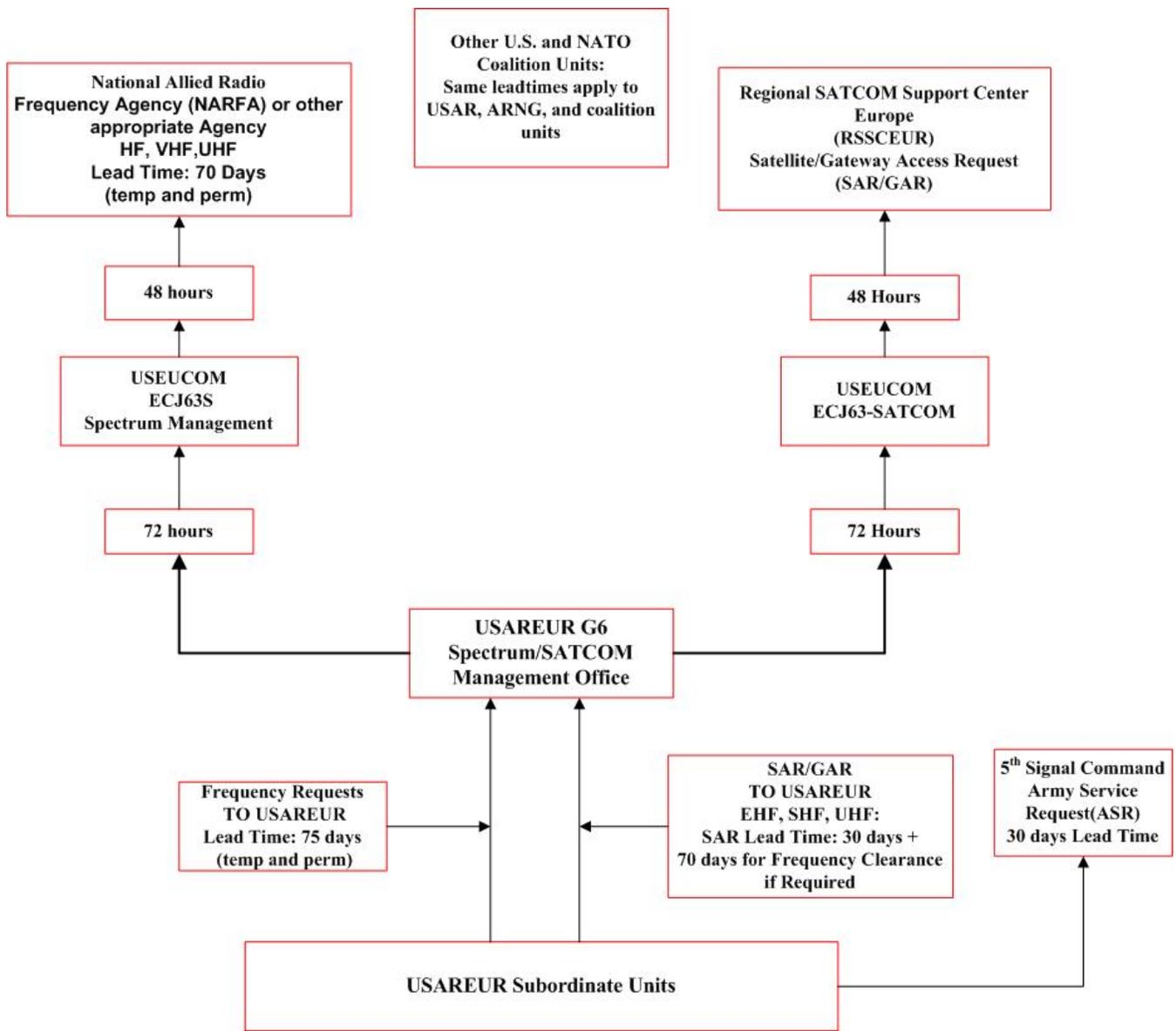


Figure 4. Frequency Request Chain of Approval

h. Frequency Manager’s Tool. Figure 5 is a frequency manager’s tool for determining frequency needs during the G3 or S3 operations planning cycle.

i. User Responsibilities. Requesters are responsible for submitting requests for frequency assignments in a timely manner. The local frequency manager receiving the frequency assignment application will process the application through established channels to request appropriate local or international approval. The disposition of the frequency-assignment request will be sent to the user through SMARTS or Spectrum XXI. The request may be approved, completely disapproved, or partly approved with operating limitations. An approved DD Form 1494 is required before a frequency assignment will be granted.

Unit name	
Equipment being used	
Frequencies needed (temporary or permanent)	
Date of exercise or event	
Number of days until exercise or deployment	
Inside/outside of leadtime?	-----
Letter of justification needed?	-----
Turn-off date	-----
Turn in to USAREUR FMO	-----

Figure 5. Frequency Manager’s Planning Tool

j. User Mandatory Considerations When Requesting and Using Frequencies. Users must—

- (1) Obtain a frequency assignment before using devices that emit radio frequency (RF) energy.
- (2) Request the minimum number of frequencies necessary to accomplish the mission.
- (3) Request the minimum transmitter power and antenna height or gain necessary to ensure adequate coverage.
- (4) Ensure electromagnetic radiating equipment operations comply with authorized parameters identified in the frequency-assignment notification.
- (5) Review all unit frequency assignments at least every 12 months to validate existing parameters and submit a modification, renewal, or deletion to the spectrum manager as required.
- (6) Ensure the appropriate spectrum needs will be supported before purchasing any RF equipment or entering into any contractual obligations involving the use of RF-dependent devices.
- (7) Obtain approval from the spectrum manager before modifying emitters or antennae (for example, increase power, change antenna height or gain).
- (8) Identify and request deletion of frequencies no longer required with the unit or installation spectrum manager.

k. Spectrum Management Analysis and Record Tracking System. SMARTS has been implemented in the Army in Europe to enable units without Spectrum XXI access to submit their unclassified frequency proposals. Information on SMARTS is available at <https://smarts.hqusareur.army.mil>.

(1) System Description. SMARTS is an information support system designed to store and relay frequency proposals and assignments between units with and units without Spectrum XXI access throughout the European theater.

(2) Network Interconnectivity. Users may connect to SMARTS through the Army in Europe NIPRNET. This is a network of Government-owned IP routers used to exchange unclassified but sensitive information between DOD users.

(3) Security.

(a) Domain Restrictions. Users connecting to SMARTS must originate from a *.gov* or *.mil* domain. Users whose IP address does not belong to a *.gov* or *.mil* domain will be denied access. This ensures that only persons with access to a Government or military terminal will be able to connect to SMARTS.

(b) User Accounts. Users must acquire a SMARTS user account before being able to access the system. The SMARTS login page provides a link to an account request form, which can be found at <https://smarts.hqusareur.army.mil/Smarts/RequestAccount.asp>. Users must complete the request form and submit it through the system to the site administrator. The site administrator will create the account and send account logon information to the e-mail address the user submitted.

(c) Data Classification Restriction. Use of the Army in Europe NIPRNET for data transfer restricts SMARTS to handling only unclassified frequency proposals. Users are responsible for ensuring that any frequency-related data entered in the system is unclassified.

(d) HTTPS. Users must access SMARTS using an HTTPS, Hypertext Transfer Protocol over a Secure Sockets Layer enabled web-browser. Users should refer to the Help module of their web-browser to find out how to activate secure sockets layer (SSL) 2.0 or 3.0 and transport layer security (TLS) 1.0. Users must use a common access card (CAC) to access the system.

(4) User Resources. SMARTS provides the following resources to the user to aid in the frequency proposal process:

(a) Template Quick-Help Icons. When completing the frequency request form template, users may view additional information about a particular line item by placing their cursor on the  icon next to the line item.

(b) MCEB Publication 7. Military Communications-Electronics Board (MCEB) Publication 7 establishes the Frequency Resource Record System. The SFAF is issued under the authority of DOD Directive 5100.35. The main menu of SMARTS provides a link to MCEB Publication 7 on the left side of the screen. Users may also access this publication while creating a frequency proposal by clicking on the appropriate link on the left side of the screen.

(c) SFAF Reference Chart. This chart provides users a list of SFAF line-item numbers and the corresponding line-item name and category. The main menu of SMARTS provides a link to this chart on the left side of the page. Users may also access the chart while creating a frequency proposal by clicking on the appropriate link on the left side of the page.

(d) SMARTS Help. SMARTS Help provides users instructions on performing basic system functions.

l. Commercial Off-the-Shelf (COTS) Equipment. Commanders and units will ensure that any frequency-transmitting equipment considered for purchase is coordinated with the FMO. No acquisition is authorized without prior coordination with the FMO. Commanders and all other leaders must ensure that they do not waste money on equipment that is not supportable in the host nation.

(1) EU-Certified Equipment. COTS equipment that was manufactured or intended for sale in Europe may already be certified for operation in the European Union (EU). In Germany, low-powered equipment that is EU-certified may be eligible for an expedited approval process. The FMO may be contacted for details when deciding to purchase this type of equipment.

(2) Non-EU-Certified Equipment.

(a) COTS equipment that was manufactured in the United States may not be EU-certified. Because the United States and Europe use different parts of the spectrum for different purposes, U.S.-manufactured equipment may operate in a band that is reserved for other purposes in Europe. The FMO may be contacted to ensure the equipment operates in an authorized band.

(b) If the equipment is not EU-certified but operates in an authorized band, the user must use the spectrum certification process (also called frequency allocation or JF-12 process) using DD Form 1494 to acquire it.

m. Frequency Usage in U.S. Training Areas in Europe.

(1) Unit rotations to training areas in Hohenfels and Grafenwöhr can be greatly enhanced by conducting coordination meetings with the training area's G6 or S6 personnel at least 70 days in advance. The POC for the Seventh United States Army Joint Multinational Training Command (JMTC) in Grafenwöhr is the Frequency Manager at DSN 475-7940 or e-mail: jmtc.g6@eur.army.mil. The POC for the United States Army Joint Multinational Readiness Center (JMRC) in Hohenfels is the Frequency Manager at DSN 520-5925 or civilian 09472-835925.

(a) During the coordination meeting, the unit must be prepared to provide the training areas with a list of all MTOE signal emitters that it will bring on the rotation.

(b) COTS radios, including Motorola walkabouts, will not be brought on the training rotation unless they have been approved through the JMRC or JMTC Frequency Manager.

(c) Rotation signal operating instruction (SOI) requirements will be discussed at the initial meeting. All SOI data will be generated from the training area S6 personnel for all rotating units, including allied units. When planning networks, frequency requests will be sent to the FMO using SMARTS (<https://smarts.hqusareur.army.mil>) or Spectrum XXI. The FMO may be contacted to establish a SMARTS account (DSN 370-3371).

(2) At JMTC (Grafenwöhr) and JMRC (Hohenfels), units are responsible for producing their own SOI for Single Channel Ground and Airborne Radio System (SINCGARS) combat net-radio systems. Only frequencies approved by the appropriate training area frequency manager are to be used. Use of home-station SOI or frequency lists is forbidden. Failure to comply with this restriction may result in harmful radio frequency interference of training area electronic systems and, ultimately, degradation or loss of training feedback data.

14. LONG-HAUL AND DEPLOYABLE COMMUNICATIONS

a. Long-Haul Services. Long-haul services are those provided by DISA. DISA provides these services either directly through a MIL path or through the Defense Information Technology Contracting Organization (DITCO), which sets up contracts with commercial vendors. DOD regulation states that all C2 long-haul services will be provided by DISA. Service may be requested using a web-based telecommunications request completed by the TCO.

b. Common Defense Information Systems Network (DISN) Services. DA pays for common DISN services. These services, however, were frozen at 2005 levels. Common services include DSN, DRSN, the Army in Europe NIPRNET and SIPRNET, the Joint Worldwide Intelligence Communications System (JWICS), and VTC DISA hub service. At each installation, all common services (whether IP-based or not) are considered to represent a certain bandwidth. For example, an increase in DSN use will result in a greater demand on the DSN bandwidth, and USAREUR will be charged for the difference.

(1) **DSN.** DSN use is mandated by DOD and the Chairman of the Joint Chiefs of Staff for all C2 elements in theater.

(2) **DSN in Quarters.** DSN in quarters is also known as preferred subscriber service (PSS).

(3) **DSN Precedence.** DSN precedence is no longer authorized in the Army in Europe except for automated fire alarms and lines dedicated to foreign police and firefighters.

(4) **Defense Red Switch Network (DRSN).** DRSN is a secure telephone system that is part of the DISN but independent of DSN. Its use is normally reserved for general officers. It is possible to connect into a DRSN switch using a secure telephone unit (STU) or secure telephone equipment (STE). Requests for DRSN service must be sent to the USAREUR G6 (AEIM-A); recommended for approval by the Chief of Staff, HQ USAREUR; and approved by the USEUCOM J6. A typical installation costs \$70,000.

(5) **Army in Europe NIPRNET.** The Army in Europe NIPRNET is an IP-driven network that can be used to send information marked no higher than “unclassified but sensitive.”

(6) **Army in Europe SIPRNET.** The Army in Europe SIPRNET is an IP-driven network that can be used to send information classified up to Secret.

(7) **JWICS.** The JWICS is a G2 or J2 service.

(8) **DISA VTC Hub Service.** DISA routes both dial-up ISDN VTC traffic and IP VTC traffic through its hub in Stuttgart. The hub is intended mainly for transatlantic VTC traffic. USAREUR maintains its own hubs in Heidelberg and Kaiserslautern.

c. Non-Common Service Long Haul (as Defined by DISA).

(1) **Dedicated Circuits.** Dedicated circuits for voice or data to span distances of more than 20 miles must be provided by DISA. Requests for exception to policy must be submitted to the USAREUR G6 (AEIM-A) for approval.

(2) **Iridiums.** Iridiums are handheld satellite radio telephones. They can also be used for data. The user pays a flat fee (\$163.13 per month) for use.

(3) **International Maritime Satellite (INMARSAT).** INMARSAT is a portable satellite radio telephone. It can also be used for data.

(4) **Transponders.** For emergencies, exercises, and temporary locations, a unit may rent a satellite transponder with a specified bandwidth.

(5) **NOVA.** NOVA is a G2 system.

NOTE: The most current cost for portable SATCOM equipment can be found at <http://www.disa.mil/Services/Network-Services>.

15. DEFENSE SWITCHED NETWORK (DSN 99 AND DSN)

a. BASECOM Management Procedures for DSN 99.

(1) Commanders of Army in Europe units, through their appointed TCOs, will—

(a) Review and reduce the number of subscribers who are authorized DSN 99 access. DSN 99 access is for official and authorized personal use only. Offices with limited, official DSN 99 access requirements will consolidate and share DSN 99 access.

(b) Review the need for 99 access periodically and add or delete lines as necessary. Each switch requires at least 99-access lines to support incoming calls from the commercial network and to provide emergency communications in case access to the DSN network trunk is temporarily lost. A certain number of outward trunk lines are also required to provide an adequate grade of service for subscribers authorized 99 access. The greater the number of subscribers who are authorized 99 access, the more trunk lines will be required. Units will limit their 99-access lines to help minimize the need for costly trunk lines.

(c) Review CAIRS reports monthly to detect, identify, and discipline telephone abusers. USAG and tenant personnel will be made aware that DSN and 99 telephone usage will be reviewed. Disciplinary actions may include warning letters, requests for reimbursement, punitive actions, and counseling those who use 99-access lines to call locations that also have DSN lines (except during switch emergencies).

(d) Ensure calls to long-distance calling-card numbers, which are used extensively for personal calls, do not overload 99 access. Although using these numbers is at no cost to the Government, frequent calls may severely limit 99 access for official calls. These numbers may need to be blocked in the DSN switch to prevent overloading the 99 access.

(e) Tightly control host-nation and worldwide commercial access.

(f) Control fax use. TCOs will—

1. Inspect telephone control logs monthly and compare telephone control logs to CAIRS report data.
2. Monitor the use of fax telephone lines equipped with a greater class of service to ensure these lines are not used to make unauthorized or excessive DSN or commercial calls.

(2) The 5th Signal Command will review nonappropriated fund (NAF) and Army and Air Force Exchange Service, Europe (AAFES-Eur), facility use of DSN and DSN 99 access lines.

(a) NAF and AAFES-Eur activities with a large number of incoming calls from the military area will be provided one or more restricted-use DSN lines. This will minimize 99 access by individuals calling from DSN telephones.

(b) NAF and AAFES-Eur activities are encouraged to contact the local telecommunications company directly for commercial services. The 5th Signal Command will provide DSN 99 access to NAF and AAFES activities on a reimbursable basis when in the best interest of the U.S. Army.

(c) In remote locations where the service provided is not compensated for by profits (for example, a small exchange at a U.S.-Romanian training site or in an isolated small facility in the Balkans) and where there are no adequate commercial services, the 5th Signal Command may provide temporary communications on a nonreimbursable basis until commercial services can be secured by the organization.

b. Management Tools. Several valuable management tools are available to unit TCOs and resource managers to improve BASECOM resource management and reduce costs. These tools include the following:

(1) **CAIRS.** CAIRS provides visibility of DSN and 99 use for each DSN telephone number by organization. Usage data is presented by month, with search features available.

(2) **The Consolidated BASECOM File.** This Excel file is generated monthly by the 5th Signal Command G8. This file is a record of DSN 99 costs and other leased-communication bills paid to commercial vendors. Unit resource managers and TCOs may request these files to balance against ordering and usage telephone logs.

(3) **DSN Switch Reports.** DSN switches and billing systems can directly generate reports that identify assigned telephone numbers and classes of service.

(4) **Telephone Logs.** Commercial-service users may be required to keep telephone logs (AE Form 25-1F) indicating the time, duration, and purpose of calls, as well as the persons, organizations, and locations called. Keeping telephone logs will result in more conscientious telephone use.

c. DSN. The DSN serves as the primary, official, administrative telephone network in the European theater. DSN calls constitute long-haul usage. In the Army in Europe, the following supplemental guidance applies:

(1) **DSN Management.** The cost of DSN service is a major part of the Department of the Army's telecommunications budget. Managing DSN service will help reduce cost and improve service.

(2) Multilevel Precedence and Preemption. DSN service includes multilevel precedence and preemption (MLPP) capability. The DSN MLPP capability allows authorized users to rapidly complete calls critical to national security interests. Authorized MLPP users must be familiar with precedence categories and the types of calls that may be assigned precedence. In the Army in Europe, DSN precedence is no longer used except in special cases. When placing DSN MLPP calls, users must consider whether or not a call requires precedence and will not use precedence higher than what is required.

(3) DSN Account Codes. Account codes will be used to associate DSN telephone numbers with the organization to which they are assigned. The use of DSN account codes allows USAG personnel to identify use by unit. The 5th Signal Command may request reimbursement for DSN 99 usage.

(a) NECs will assign account codes to ensure they are uniform throughout the DSN system. Information received from USAGs on their tenant units will be used to generate the list of account-code assignments.

(b) The DSN system assigns account numbers to each distinct organization.

1. Each telephone number served by the switch will be coded with an account number associated with the unit to which the number is assigned.

2. Each switch will reserve numbers for additional assignments, exercises, and contingencies.

3. Unassigned account codes will not be entered in the switch.

(c) Additional information and assistance may be obtained from 5th Signal Command (NETC-SEC-O-SCC), CMR 421, APO AE 09056.

NOTE: DSN commercial-access military service (99 access) and official commercial telephone service will not be used to call areas that have DSN capability.

d. Telephone Systems and Networks. Official commercial telephone service is defined as the installation and use of telephone service provided directly from a host-nation telecommunications company switch. The costs associated with this type of service are of the BASECOM category. The following policy applies to official commercial telephone service:

(1) Except for locations not served by DSN, commercial telephone service exceeds the requirements provided by normal telephone service.

(2) Routine business will not be conducted over official commercial telephone services.

(3) Official commercial telephone service will not be installed—

(a) Where military telephone service exists. Exceptions to this policy are emergency and lifesaving activities (for example, ambulances, fire stations, military police) and other activities that require 100-percent backup communications on a time-sensitive basis (for example, crisis-control centers, operations centers).

(b) In the quarters of PSS customers. Violations of this policy are violations of public law.

e. Telephone Abuse. The ready availability of DSN services and access to commercial networks through 99 access, official commercial telephone service, and cell phones can lead to abuse. In the Army in Europe—

(1) DSN and commercial calls, including those placed from cell phones, will be monitored for abuse.

(2) Individuals abusing telephone service are subject to disciplinary and administrative action and will be required to reimburse the U.S. Government.

(3) Commanders will enforce commercial-call limits, investigate the improper use of official telephones, and take corrective action if necessary.

(4) The USAREUR G6 may identify suspected unofficial telephone calls, inform 5th Signal Command or unit commanders, and direct that an investigation be made. A report of the investigation findings will be sent to the USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351.

(5) Unauthorized individuals will not tamper with communications equipment. Violations may result in the equipment being disconnected or confiscated, or in the service being discontinued.

f. Classes of Telephone Service in the Army in Europe. In the Army in Europe, official classes of service designations are different from those in CONUS.

(1) The digital telephone switches used in the DSN allow numerous “class marks” to be assigned to each subscriber line. This capability allows telephone service to be customized to meet the requirements of individual users and to help control DSN costs.

(2) In CONUS, official telephone services include the Federal Telecommunications System, DSN, and commercial telephones with international access. In the Army in Europe, services include DSN worldwide, DSN Europe and CONUS, DSN Europe, DSN nationwide, DSN local with the possibility of adding to any preceding service, DSN 99 worldwide, DSN 99 Europe, DSN 99 nationwide, and DSN 99 local. For this reason, services in the Army in Europe and CONUS cannot be easily compared. Table 1 provides Army in Europe services and the approximate equivalent services available in CONUS.

Table 1 Comparison of Classes of Telephone Service	
Army in Europe	CONUS Class Designation
DSN worldwide with DSN 99 worldwide	A1
DSN worldwide with DSN 99 local	A2/A3
DSN local with DSN 99 local	A4
DSN worldwide	C1
DSN CONUS and Europe	C2
DSN Europe-wide	C3
DSN nationwide	C4
DSN local	C5

g. Requesting Telephone and Telephone-Related Service.

(1) BASECOM Services.

(a) For acquisition and funding purposes, several telecommunications services that support routine installation operations have been grouped together as BASECOM services. BASECOM services include DSN 99 access, official commercial telephones, cell phones, BlackBerry devices, data and other special circuits, and other leased services.

(b) Requirements for BASECOM services are divided into two categories:

1. Indefinite requirements (more than 89 days).
2. Temporary or exercise requirements (89 days or less).

(2) Requesting BASECOM Services. To request BASECOM services, requesters must submit an automated LSR request through CAIRS. In addition, the following forms may also be required:

(a) **DA Form 3953.** If required, this form must be forwarded to the supporting NEC.

(b) **DD Form 448.** DD Form 448 is required if no funding agreement exists between the unit requesting the service, the USAREUR G8, and 5th Signal Command.

h. Call-Forwarding.

(1) Enabling call-forwarding on DSN telephones is allowed if forwarding calls to—

(a) An official cell phone for a period not to exceed 12 hours.

(b) A personal cell phone for a period not to exceed 12 hours for the purpose of being reached for work-related calls.

(c) Another DSN telephone for a limited time.

(2) Enabling automatic forwarding of DSN telephones is not allowed—

(a) To forward calls to a private commercial or residential telephone.

(b) To forward calls to any fixed or cell phone (whether permanently or temporarily) outside the country of origin.

(c) In any way that transfers personal costs to the U.S. Government.

i. Single-Line Service.

(1) The “single-line concept” is the goal for providing DSN telephone service in the Army in Europe. Under this concept, one telephone number is provided for each customer. Local conditions may require the use of extensions (for example, insufficient DCO or cable plant capacity). DSN telephone extension service is limited to one primary telephone instrument with no more than five extensions for each line. This requires approval by the supporting NEC. In addition, no more than two of the instruments will have ringing capability.

(2) Because of the limited infrastructure, the NEC will validate the requirement for every extension. This validation will be kept on file until the extension is removed and single-line service is installed. The NEC will revalidate the need for each extension every 5 years.

j. STUs and STE. Secure telephones must display DD Form 2056 with the “DO NOT DISCUSS CLASSIFIED INFORMATION” portion removed or marked out. For STE only, DD Form 2056 must be attached to the bottom under the L-3 communications logo. This label warns users not to remove the Fortezza Plus Card while the telephone is off the hook or in use. Removing this card under these conditions can cause the card to be erased.

k. Answering Machines and Voice Mail. Connecting commercial answering machines to DSN is permissible. Voice mail is allowed but is costly and normally funded by the unit. Requests for voice-mail service must be submitted to the supporting NEC. Those using voice mail or answering machines should adhere to the following:

(1) No Privacy Act-protected information or sensitive information will be recorded. Simple messages should be used to establish contact between parties.

(2) Proper use of voice mail should include leaving one’s cell-phone number in the message, if available, as an alternative to the costly forwarding from the DSN line to a cell phone.

16. PREFERRED SUBSCRIBER SERVICE AUTHORIZATION

Tables 2 and 3 list PSS authorizations. Individuals serving in the positions indicated are authorized PSS (official telephone service in their quarters).

a. If the quarters do not have DSN in place, a line may be leased. The user’s organization is responsible for the associated costs.

b. Under no circumstances will official telephone service in quarters include direct commercial 99 access.

c. Requests for exception to policy may be sent to the USAREUR G6 (AEIM-A) for approval. An example of a valid exception would be a rear detachment commander who must deal with casualties and health, morale, and welfare issues while the unit is deployed in a war zone. This DSN service would end once the unit returns to the USAG.

Table 2 Positions in Army in Europe Units Authorized Preferred Subscriber Service					
Position	USAREUR Commands*	Divisions or Equivalent Organizations*	Brigades or Specified Commands*	USAGs	Tactical Battalion MTOE Units
Commander	X	X	X	X	X
Deputy commander	X	X			
Chief of staff	X	X			
Command sergeant major	X	X		X	
Deputy chief of staff, operations; G3; support operations officer	X	X			
General officers	X	X	X	X	
Distinguished-visitor guestroom occupants				X	
*NOTE: Authorized units can be found on the USAREUR homepage at http://www.eur.army.mil/organization/units.htm .					

Table 3
HQ USAREUR Positions Authorized Preferred Subscriber Service
CG, USAREUR
CG Executive Officer
CG Aide-de-Camp
DCG, USAREUR
Chief of Staff, HQ USAREUR
Deputy Chief of Staff, HQ USAREUR
Command Sergeant Major, USAREUR
Secretary of the General Staff
Chief, Staff Actions Division, Office of the Secretary of the General Staff
Deputy Chief of Staff, G1
Assistant Deputy Chief of Staff, G1
Deputy Chief of Staff, G2
Assistant Deputy Chief of Staff, G2
Deputy Chief of Staff, G3
Assistant Deputy Chief of Staff, G3
Chief, Operations Division, Office of the Deputy Chief of Staff, G3
Deputy Chief of Staff, G4
Assistant Deputy Chief of Staff, G4
Deputy Chief of Staff, Engineer
Assistant Deputy Chief of Staff, Engineer
Deputy Chief of Staff, G6
Assistant Deputy Chief of Staff, G6
Deputy Chief of Staff, G8
USAREUR Chaplain
Chief, Public Affairs
Command Surgeon
Deputy Command Surgeon
Inspector General
Judge Advocate
Provost Marshal
Deputy Provost Marshal
General officers

17. PRECEDENCE DIALING AUTHORIZATION

a. Precedence.

(1) DSN precedence has been eliminated in the Army in Europe by order of the Chief of Staff, HQ USAREUR. This elimination was based on two factors. One factor was the improvement in DSN service that occurred when the number of Soldiers in the Army in Europe was greatly reduced while the existing DSN infrastructure remained the same. The second factor was the high cost of DSN precedence.

(2) Since the implementation of DISN subscriber service, DISA no longer charges USAREUR for DSN precedence. The Department of the Army, however, is still charged for this service. In the Army in Europe, DSN precedence is not needed except for a few automated fire alarms. From an operational standpoint, DSN precedence will be based on operational needs. The maximum authorized precedence will be determined by the special C2 position of the recipient. For example, in the Army in Europe, only a four-star general officer in a commander position is authorized “flash override.”

b. Dialing Authorization. If the DCG, USAREUR, or the Chief of Staff, HQ USAREUR, determines that DSN precedence-dialing capability is required for the C2 of military forces, this capability will be limited to the individuals, precedence level, and calling areas shown in table 4.

c. Exceptions to Policy. Requests for exception to policy for DSN precedence-dialing capabilities beyond those shown in table 4 may be sent by memorandum to the USAREUR G6 (AEIM-A). The memorandum must provide operational justification for precedence.

18. CELL PHONES

a. General. Because of the high cost of using cell phones, management control over active subscriber identity module (SIM) chips is required. A cell phone is defined as the combination of an active SIM chip with either a cell phone or personal digital assistant (for example, BlackBerry) handset.

b. Responsibilities. HQ USAREUR staff principals; commanders of USAREUR major subordinate commands (MSCs); the Director, IMCOM-Europe; and USAG commanders are designated as approving authorities for cell phones for their units. Each unit and staff office will—

(1) Be authorized to approve new requests for cell phones. They are also responsible for the management and use of cell phones issued under this authority. Specifically, issuing authorities—

(a) Are authorized to approve the acquisition and activation of SIM chips to support mission requirements, including local command exercises.

(b) Must manage the use of cell phones in their units and ensure payment is made for all associated costs.

(c) Will not authorize the use of prepaid cell-phone service in the Army in Europe until the service becomes available on Army blanket purchase agreements through the USAREUR G6 or NETCOM/9th SC(A). If a blanket purchase agreement for prepaid cell-phone service becomes available, unit TCOs will implement procedures to validate that cards were used for official or authorized purposes (for example, written user certification that provides detailed and itemized call information).

**Table 4
Army in Europe DSN Precedence-Dialing Authorization Table**

Position	Four-Star Command	Three-Star Command	Two-Star Command	One-Star Command	Colonel Command	Lieutenant Colonel Command
Commander	FOG	IC	IC	IC	PC	PC
Deputy commander/executive officer	FG	IC	IC	PC	PC	PC
Chief of staff	IC	IC	IC			
Command sergeant major	PC	PC	PC			
Deputy chief of staff	IC	IC	IC			
Secretary of the general staff	IC	PE	PE			
Deputy chief of staff, personnel/G1/S1	IC	PC	PC			
Deputy chief of staff, intelligence/G2/S2	IG	IE	IE	PC		
Intelligence center	IG	IE	IE			
Deputy chief of staff, operations/G3/S3	IG	IC	IC	PC		
Command center	FG	FC	FC	IC		
Deputy chief of staff, logistics/G4/S4	IC	PC	PC	PC		
Deputy chief of staff, engineer	IC	PE	PE			
Deputy chief of staff, information management/ assistant deputy chief of staff, information management/ G6/S6	IC	PE	PE			
Deputy chief of staff, resource management/G8	IC	PE	PE			
Chaplain	IC	PE	PE			
Public affairs officer	IC	PE	PE			
Inspector general	IC	PE	PE			
Judge advocate	IC	PE	PE			
Provost marshal	IC	PE	PE			
Principal assistant responsible for contracting	IC					
S2/S3					PE	

NOTES: 1. Precedence: F = Flash; I = Immediate; P = Priority; FO = Flash Override
2. Access: G = Global; C = CONUS; E = Europe
3. USEUCOM (Joint Chiefs of Staff) approval is required for all precedence and area-dialing capabilities above routine. Routine CONUS or routine global authorization will be requested through the supporting NEC.
4. The principal deputy for each position shown is authorized the same precedence unless otherwise noted.
5. When a greater precedence is required or a position is not identified above, requests for authorization will be sent through the USAREUR G6 and the CG, USAREUR, to the CG, USEUCOM.

(2) Disapprove requests to activate cell phones if the requested telephone is to be used under any of the following conditions:

(a) For convenience.

(b) Instead of fixed telecommunications systems.

(c) Instead of a tactical communications system in a field environment.

(d) To back up other cell phones.

(e) To send classified or sensitive information. Exceptions may be granted if the cell phone is an approved encryption device listed on the U.S Army Cryptographic Modernization Device Portfolio (<https://www.kc.us.army.mil/cryptomoddp.nsf/index.html?OpenPage>).

NOTE: Cell phones used to send unclassified sensitive one (US1) information will be encrypted. This requirement may not be waived (AR 25-2). Information designated as unclassified sensitive two (US2) information may also require protection. Radios used for public safety and communications with civil-aviation channels are exempt from this policy.

(3) Appoint a TCO to help manage cell phones issued within the unit. The TCO will be designated in writing for a specific period. If no TCO is appointed, the issuing authority must perform the TCO functions listed below. TCOs must conduct periodic validations of cell-phone service. The TCO will—

(a) Maintain a unit cell-phone database with the following data:

1. Name of the user assigned the cell phone.
2. Name of the unit or subordinate unit to which the individual is assigned.
3. DSN telephone number of the user and name of the subordinate TCO (if applicable).
4. Cell-phone SIM chip serial number.
5. Cell-phone handset model and serial number and cell-phone telephone number.
6. DA Form 3953 purchase voucher number (PVN).

(b) Send a list of cell-phone activations and deactivations each quarter to the USAREUR G6 (AEIM-A). The list must include the following information for each activated or deactivated cell phone:

1. Name and duty position of the user assigned the active SIM chip.
2. Cell-phone handset make, model, and serial number.
3. Cell-phone SIM chip serial number.
4. Cell-phone number.
5. PVN (as shown on the order form (DA Form 3953)).

(c) Send a validation report each quarter to the USAREUR G6 (AEIM-A). The report must include the following:

1. Unit or staff name and account number.
2. TCO contact information, including telephone number and e-mail address.
3. List of cell-phone numbers and total costs for each by month.
4. TCO statement of validation and actions taken for any invalid use found.

(4) Train cell-phone users on the proper use of cell phones. Particular attention will be paid to discussing the consequences of roaming charges and the use of “1-800” services.

(5) Require cell-phone users to sign a user agreement acknowledging that they have read and understand the rules on the proper use of cell phones. This statement will include an agreement to reimburse the Government if improper use is identified and the cost is assessed.

(6) Review itemized cell-phone bills on receipt for unofficial or improper use. Most countries send cell-phone bills every month, while Italy sends cell-phone bills every 2 months. TCOs will notify the issuing authority concerning extremely high-volume cell-phone users and when improper use is apparent.

(7) Compile statistics on cell-phone use. These statistics will be used to revalidate cell phones and may include the following:

- (a) Number of unit cell phones.
- (b) Frequency of use for each cell phone.
- (c) Calling areas called (national and international).
- (d) Average monthly use costs.
- (e) Documented cases of improper use of cell phones and reimbursement obtained.
- (f) The continuing requirement and justification for each unit cell phone.

NOTE: Once the specified statistics are compiled, the TCO will provide the commander a validation report that recommends either continued service or termination of unit cell phones.

(8) Provide commanders information to help them identify and reduce improper use of cell phones and to prevent abuse.

c. Procedures for Requesting Cell Phones. Cell-phone service must be requested and approved by submitting an IT technical validation package to the servicing NEC and using DA Form 3953. Issuing authorities will not approve DA Form 3953 for cell-phone activation without the following information:

(1) Critical Operational Needs. These needs include potential loss of life or limb, actions or decisions that are critical to the operations of the U.S. Forces overseas, and short-notice actions or decisions that will save the command or theater significant resources. Requests to activate a cell phone for convenience will not be approved.

(2) Monetary Savings and Mission Effectiveness. Monetary savings and improved operations must clearly justify the cost of activating a cell phone. The justification will include the following criteria as applicable:

(a) Area of Operation. If units are widely dispersed, describe the information to be transmitted, and the operations or savings that the ability to communicate faster will improve.

(b) Command and Control. Describe how using a cell phone will increase C2 responsiveness and prevent waste or eliminate the need for other communications systems.

(c) Communications Upgrade. Describe why the cell phone needs to be replaced or upgraded.

(d) Economics. Describe the direct tradeoff in total costs that will be achieved by replacing an existing communications system with a cell phone. The justification must provide an economic analysis, statistics, and the amount of savings to be achieved.

(e) Position. Explain how the duty position of the proposed cell-phone user relates to anticipated operational improvements or savings that will be achieved by the mobility of a cell phone.

(f) Time. Describe the amount of duty time spent on the road, the required call load, and the improved operations or savings that will result from the ability to communicate faster by using a cell phone.

(3) Identification of Resources. Explain who will pay for cell-phone activation and recurring service charges. BASECOM funds will not be provided for cell-phone service. Units must budget for cell-phone service in the appropriate mission or base-operations account.

d. Revalidation of Requirements. HQ USAREUR staff offices, USAREUR MSCs, IMCOM-Europe, and USAGs will revalidate their number of and requirements for cell phones each year by reporting the previous fiscal year data by 1 December to the USAREUR G6 (AEIM-A). The report must include the following:

(1) Total number of cell phones in use for each HQ USAREUR staff office, USAREUR MSC, and IMCOM-Europe organization. USAREUR MSCs and IMCOM-Europe will report quantities by organization at the lieutenant colonel level, which includes battalions and indirect-reporting USAGs.

(2) Total cost of cell-phone use for the previous fiscal year (1 Oct through 30 Sep).

(3) Total dollar value recouped for unofficial call charges discovered by examining the service provider call records.

(4) Expected or anticipated increases or reductions in quantities or use.

(5) Any special data required. The USAREUR G6 (AEIM-A) will distribute the annual data call memorandum by 1 November each year and include special requirements to be reported.

e. Procurement.

(1) Procurement Options. Units that need cell phones for contingency-support missions will submit a request according to the specific needs of the mission. Issuing authorities are authorized to approve cell phones using one of two procurement options for cell-phone activation and payment of services. If a cell-phone request cannot be met under the first option, the commander may use the second option.

(a) Option 1: Procuring service through 5th Signal Command under the DITCO-awarded Vodafone enterprise contract. International cell-phone services may be procured under this contract, which covers services based in 26 countries. For unit travel or deployment, TCOs will compare the cost of procuring local services in the country with the cost of taking existing cell phones across borders to determine the most mission- and cost-effective means of cellular communications for the unit. Roaming costs will be compared with local calling costs, and local service quality and coverage will be analyzed for effectiveness.

1. On obtaining approval from the issuing authority, the TCO must submit DA Form 3953 and the IT technical validation package to an authorized 5th Signal Command telecommunications ordering office (TOO) to ensure proper billing and contracting procedures are used.

2. Funding for cell-phone service will be requested by sending DD Form 448 to 5th Signal Command (NETC-SEC-RM). 5th Signal Command will assign a corresponding customer account number that the TCO will annotate on all orders to be paid from that account.

3. The TOO will assign a PVN to each service request and send requests to 5th Signal Command (NETC-SEC-RM) for funding certification. 5th Signal Command will process service requests once funding has been provided and will return the approved DA Form 3953 to the TOO. 5th Signal Command will inform the unit budget analyst (as noted on the DA Form 3953) of the funds required and will not process the request until DD Form 448 is received.

4. According to the terms of the DITCO Vodafone enterprise contract, billing statements must have the mailing address of Headquarters, 5th Signal Command (NETC-SEC-RM), Building 1009, Room 213, Boyd Avenue, 65205 Wiesbaden, Germany. The 5th Signal Command G8 will receive monthly billing reports, which provides access to details of itemized calls through the Vodafone Portal.

(b) Option 2: Procuring service through a local vendor. Users will—

1. Ensure cell-phone activation is done as part of the service agreement with the commercial service provider.

2. Pay for acquired cell-phone equipment and related services.

3. Ensure that they receive monthly, itemized billing statements for TCO review.

(2) Procurement Standard: European Cell-Phone Networks.

(a) The Global System Mobile (GSM) standard permits cell phones to be used almost anywhere in Europe (900/1,800 megahertz (MHz)). Some U.S. digital cell phones also use the GSM standard, but operate on different frequencies (900/1,900 MHz). Tri-band (900/1,800/1,900 MHz) handsets are required to interface with GSM-based systems used in the United States. (Quad-band handsets also function in the new GSM band 950 MHz in South America.)

(b) The Universal Mobile Telecommunications System (UMTS) (sometimes called “3G” (third generation GSM)) is a new network that has been implemented in most European countries. Some newer GSM cell phones may also be UMTS-capable. This additional capability may be used for higher speed connections when possible or appropriate.

f. Proper Use of Cell Phones. Because of the additional cost of using cell phones in Europe and the potential effects of electromagnetic emanations (cell phones used inside buildings can affect alarms and sensitive electronic circuitry), the following policy applies:

(1) Cell phones will not be used—

(a) Whenever normal fixed telephone devices are present (for example, DSN, desk telephone) or unless one is calling a cell phone that is on the Army in Europe cell-phone contract.

(b) For international personal use. Limited local personal use as prescribed by AR 25-1, paragraph 6-1e, is allowed. Commanders may choose to limit this to within a user's included monthly national minute plans. This should be noted in the user agreement.

(c) As the primary means of communications on post, in USAGs, and in facilities where other, less costly means of communication exist (for example, DSN, official commercial telephones). Personnel will always use the least expensive means of communication.

(d) For health, morale, and welfare calls.

(e) For transmitting data when less costly systems are available (for example, direct connections, DSN, LAN, modem, tactical communications systems).

(f) In medical treatment facilities. In areas where cell-phone use may disrupt medical equipment, signs will be posted to indicate where cell phones must be turned off and not used. Cell phones will not be used within 6 feet of the signs.

(g) To access the Internet or the World Wide Web, including wireless application protocol connections (often possible with European cell-phone handsets). The only exception is the approved use of a UMTS connect card, which is available on the DITCO Vodafone enterprise contract.

(h) At meetings or in areas where sensitive or classified information is being discussed. Cell phones will not be taken to these meetings or into these areas unless the battery has been removed.

NOTE: Even when a cell phone is turned off, a person with malicious intent could remotely use the cell phone as a microphone and transmitter to listen to conversations in the vicinity of the cell phone. The user of the cell phone would not realize that the telephone is in the diagnostic mode and transmitting all nearby sounds until an attempt is made to place a call. For this reason, cell-phone users must remove the battery from their cell phones before attending meetings or entering areas where sensitive or classified information is to be discussed, or not bring cell phones into those areas.

(i) To subscribe to download services such as ring tones, novelty pictures, or film clips, and news services.

(j) While operating privately owned vehicles or Government-owned vehicles unless the vehicle is safely parked or the cell phone is used with a hands-free device. The only exceptions to this prohibition are emergency responders, such as ambulances, explosive ordnance disposal teams, fire emergency services, hazardous material responders, and military police. Bluetooth technology, including Bluetooth hands-free solutions for cell phones, is not authorized in the Army in Europe.

(2) Authorizations for cell-phone service apply only to the designated user or unit. Authorized users and units will not issue cell phones to users or units that are not authorized the service. Users will, however, share cell-phone resources within their units for efficiency and cost reduction.

(3) Lost and stolen cell phones must be reported immediately to the TCO. The TCO or user will immediately contact the TOO or the service provider (whichever is more quickly available) to deactivate the SIM chip. This measure will help ensure that the Government is not charged for unauthorized use.

(4) The TCO will issue SIM chips that include active PINs. PINs will not be deactivated by users. Users should memorize their PIN. If someone tries to activate the cell phone with the wrong PIN, the cell phone cannot be activated after the third try. To restore service, users must give their unit TCO the SIM chip serial number or telephone number to obtain the PIN unblock key.

(5) Cell phones should be portable. Cell-phone approval authorities will review requests for telephone-installation kits and car antennas and approve requests only when the use of nonportable cell phones is operationally necessary to accomplish the mission.

g. Exceptions to Policy. Requests for exception to policy governing cell phones must be submitted by memorandum to the USAREUR G6 (AEIM-A). The memorandum should include sufficient justification for the exception, including the five Ws (who, what, when, where, and why) and funding information.

(1) Support for Contingencies and Exercises. Subparagraphs h and i below provide exceptions for issuing cell phones to support contingencies and exercises.

(2) Tactical Cell Phones. Subparagraph j below identifies unique procedures for procuring tactical cell phones.

h. Cell Phones for Contingency-Support Missions. The rapid development of contingencies may require that deploying units or personnel have voice-communications capability for C2. In planning cell-phone use for operational contingencies, requesters must determine whether or not a cell-phone infrastructure exists in the deployed area. If it does, the requester will contact the Crisis Action Team, Current Operations Division, Office of the Deputy Chief of Staff, G3, HQ USAREUR, to request the cell phone. The Crisis Action Team validates and approves the need for cell phones for contingencies. Units deployed in operational areas will procure service from local cell-phone providers through deployed DOD contracting agents or organizations.

(1) Requests for cell phones for contingency-support missions must explain the following:

- (a) Why other communications systems cannot meet contingency needs.
- (b) The estimated period of time the cell phone is needed.
- (c) The name of the user or unit to which the cell phone will be assigned.

(2) When the contingency mission has ended, the activating authority will terminate the cell-phone service through the contracting agency with the local service provider.

(3) The unit requesting the contingency cell-phone support will provide full funding for the requirement.

i. Cell Phones for Exercise Support.

(1) The Crisis Action Team will control the issue, turn-in, and reissue of exercise cell phones used by HQ USAREUR staff offices.

(2) The USAREUR G3, USAREUR MSCs, IMCOM-Europe, and USAG TCOs will—

- (a) Procure exercise cell phones using contracts.

(b) Control the issue, turn-in, and reissue of exercise cell phones used by organizations in their command or on their staff.

(c) Maintain the following information on exercise cell phones:

1. Make, model, and serial number of the cell-phone handset.
2. SIM chip serial number, telephone number, and the PVN (on DA Form 3953).
3. Name and duty position of the assigned user.
4. Date issued and date of expected return.
5. Location of the unit during the exercise.

(3) Cell phones used for exercises will—

(a) Be temporarily hand-receipted to the requester and turned in to the controlling office after the exercise.

(b) Not be used to send sensitive or classified data.

(c) Not be used when tactical or other communications systems are available.

(d) Not be issued for purposes other than the exercise. Exercise cell phones will not be used merely to supplement permanent cell phones.

(4) Requests for cell-phone service for use in exercises directed by the Joint Chiefs of Staff will be submitted to the USAREUR G3 (AEOP-OMT), Unit 29351, APO AE 09014-9351. The USAREUR G3 has been delegated authority to approve cell-phone service in the Army in Europe for exercises not sponsored or directed by the Joint Chiefs of Staff. Exercise requirements must be for 89 days or less. Requests for extensions must be sent to the USAREUR G3 (AEOP-OMT) at least 30 days before the authorization period ends.

(5) Approved exercise cell phones will not be converted to permanent cell phones. TCOs will ensure cell-phone service contracts are terminated at the end of the exercise and all cell-phone equipment is accounted for or returned to the service provider.

j. Tactical Cell Phones.

(1) Commercial cell phones will not be used in place of on-hand tactical communications equipment.

(a) Urgent requirements for cell phones used in place of or as tactical communications equipment must be approved through the operational-needs statement process according to AR 71-9.

(b) For routine requirements, requesters will complete DA Form 2028 and DA Form 4610-R, and submit these forms for approval through Vertical - The Army Authorization Documents System (VTAADS).

(2) Approved cell phones will be identified in the equipment section of a unit's MTOE or TDA. These cell phones must be accounted for through standard Army property accountability procedures (AR 710-1). Sensitive information may not be discussed on cell phones.

19. BLACKBERRY DEVICES

a. BlackBerry devices provide remote e-mail access to the NIPRNET to support official business. Because BlackBerry devices are easy to use and tightly integrated with existing infrastructure, they are authorized for personnel to allow encrypted and continuous access to e-mail. The infrastructure to support this technology will be implemented by the Army in Europe, but each organization will pay for its own devices and services. Personnel authorized to approve the acquisition of BlackBerry devices (e below) must consider the overall long-term cost to their organizations before approving the acquisition. BlackBerry devices should be acquired only for personnel who require a "24/7" mobile e-mail capability as a mission-critical tool.

b. The consolidation of BlackBerry services for the Army in Europe has redefined support responsibilities for the BlackBerry program:

(1) The USAREUR G6 is responsible for policy on and oversight of the BlackBerry program. In addition, the USAREUR G6 will provide configuration guidance on all changes that deviate from the DISA Wireless Security Technical Implementation Guide (STIG) and the DISA Wireless STIG BlackBerry Security Checklist. STIGs are available at <http://iase.disa.mil/stigs/index.html>.

(2) 5th Signal Command will—

(a) Provide for the operation and maintenance of Army in Europe BlackBerry Enterprise Servers (BESs).

(b) Designate the appropriate number of support personnel to help units with troubleshooting issues that cannot be resolved at the unit level.

(c) Test and develop configuration documentation for new BlackBerry devices before they are approved for use.

(d) Maintain copies of all required licenses and documentation for the operation of BlackBerry Enterprise services, which includes copies of the server router protocol (SRP) licenses for the BESs, all support-agreement documentation, and the nondisclosure agreement.

(e) Implement configuration changes in accordance with Army in Europe guidance, the DISA Wireless STIG, and the DISA Wireless STIG BlackBerry Security Checklist. 5th Signal Command will maintain a BES configuration document and a log that documents all changes to the BES. The documentation will include the date and time the change was made, the person who made the change, and the person who authorized the change. Only the USAREUR G6 may approve exceptions to this policy.

(3) Units will—

(a) Purchase, upgrade, license, install, configure, and provide basic troubleshooting for all assigned BlackBerry devices. Units are the first line of support for all BlackBerry users within their organization. All units supported on the Army in Europe BES (regardless of their unit affiliation) are required to purchase a client access license, a CAC reader, and a secure/multipurpose Internet mail extension (S/MIME) license for each device. Licenses may be purchased in bulk to reduce cost.

(b) Designate the appropriate number of personnel to support BlackBerry devices within their organization.

(c) Incur all recurring and nonrecurring costs associated with the purchase and use of BlackBerry devices, and training for support personnel.

(4) Perform a “wipe” using JavaLoader on new or reissued BlackBerry devices. BlackBerry devices are prohibited from connecting to the BES with “out-of-the-box” device software.

(a) After a wipe, the latest handheld software and desktop software authorized by the BES administrator will be loaded.

(b) After loading the latest software, unit personnel will run the Autoberry software on the device.

(5) Local TCOs will maintain all user client access licenses and S/MIME licenses for their unit.

c. BlackBerry systems used in the Army in Europe must be certified to meet the Federal Information Processing Standard (FIPS). FIPS certification protects unclassified Government information when leaving DOD-owned and -controlled networks. BlackBerry systems must use S/MIME software to be public key infrastructure (PKI)-compliant. S/MIME-enhanced BlackBerry systems are subject to DOD, DA, and Army in Europe policy governing the security and use of unclassified information systems.

d. In addition to general security regulations and policy, the following controls govern the use of BlackBerry systems in the European theater:

(1) The use of BlackBerry devices must be included in the using organization’s system security accreditation agreement (SSAA). The BES must be included in the same SSAA as its host MS exchange server.

(2) BlackBerry devices will not be used to process classified information (Confidential and above). There are no sanitation products approved for use with BlackBerry devices. If a device is accidentally used to process classified information, the device must be treated as a classified item until it is destroyed according to applicable Army regulations.

(3) BlackBerry devices are not permitted in sensitive compartmented information facilities (SCIFs) according to Director of Central Intelligence Directives 6/3 and 6/9.

(4) BlackBerry devices will not be taken into areas where classified information is discussed or electronically processed except as provided for in (3) above and AR 25-2, paragraph 4-29. When the exception meets the criteria for approval, the user will receive security-awareness training.

(5) BlackBerry devices will not be configured to work with or be connected to any device other than a Government-owned unclassified computer. BlackBerry devices will not be connected to a Government-owned system in a SCIF at any time. Auto-forwarding official mail (from a .mil e-mail address) to unofficial accounts (for example, a .com e-mail address) or unofficial devices is prohibited.

(6) BlackBerry devices will use a PIN for the SIM (for example, SIM chip, a password for the device (hand-held password)) and a password for the certificate store (key store password). Devices will be configured with a timeout of 15 minutes, a password history of five, and maximum password attempts of three. On the third failed attempt, all data on the device will be wiped automatically. Based on this password policy and the limitations of the device, passwords must be five alphanumeric characters with at least one alpha and one numeric character. BlackBerry passwords will be changed every 90 days.

(7) The cell-phone guidance in paragraph 18 applies to the voice and telephony capabilities of BlackBerry devices.

(8) All BlackBerry devices will be configured on the Army in Europe centrally managed BES. Every BES must comply with the latest DISA Wireless STIG and the latest DISA Wireless STIG BlackBerry Security Checklist. The checklist can be found at <http://iase.disa.mil/stigs/checklist/index.html>. The USAREUR G6 may implement additional policy requirements as needed. (This additional configuration policy is available from the USAREUR G6 (AEIM-I), DSN 379-5056.) All BESs must have USAREUR G6 approval before being purchased or connected to Army in Europe networks.

(9) If a BlackBerry device is lost or stolen, it must be reported immediately to the BES administrator. The BES administrator will immediately issue a “kill” command for the device, wiping all data from it.

(10) Each BlackBerry device has a unique hardware address know as a PIN. PIN-to-PIN messaging (sending messages between BlackBerry devices using the PIN instead of an e-mail address) is authorized as long as the message is sent using DOD PKI encryption. The USAREUR G6 may authorize PIN-to-PIN messaging in plain text for limited periods during critical situations when normal communication infrastructure is unavailable.

(11) To maintain the efficiency of the BlackBerry infrastructure, 5th Signal Command will remove all dead accounts from the BES immediately. Inactive accounts will be removed after 30 days of inactivity.

(12) BES-support personnel will ensure that the following procedures are implemented for the wireless activation of BlackBerry devices:

(a) BlackBerry users may not wireless-activate their BlackBerry device unless they do so under the direction of a BES administrator.

(b) Wireless activation is not permitted for initial device activation.

(c) An authorized BlackBerry systems administrator must perform wireless-device reactivations based on critical mission requirements (for example, if a BlackBerry device of a general officer on TDY becomes corrupted and requires reactivation).

(d) When wireless activation is performed, the activation password must be given to the user in a secure manner (for example, encrypted and sent by e-mail to a trusted individual traveling with the general officer).

(13) Any time a user or support personnel suspect a BlackBerry may be compromised, they will immediately notify the USAREUR G2 for further guidance. All personnel traveling to restricted areas (as determined by the USAREUR G2) will run the Autoberry program before leaving and will run it again after returning. Any change denoted will be reported to the USAREUR G2.

e. BlackBerry devices may be provided to personnel in the grades of lieutenant colonel or the civilian equivalent (GS-14), sergeant major, and above as long as they require “24/7” mobile e-mail capability. Personnel who do not meet the criteria must request approval from their MSC commander; HQ USAREUR staff principal; or the Director, IMCOM-Europe, as applicable. This authority cannot be delegated. Personnel who have a BlackBerry device but do not meet the grade requirements must request approval to keep their device. Approval must be granted before service on their device will be renewed. Approval to purchase BlackBerry devices will be based on a valid requirement for “24/7” mobile e-mail capability.

(1) BlackBerry devices will be purchased with the necessary service as part of the Army in Europe cell-phone contract at the requesting unit’s expense. No other contract source is authorized. Units are responsible for all costs for the device, licenses, monthly charges, and usage. Units must be prepared to purchase new equipment when the current device or sled does not meet current messaging or security requirements. In some cases, the life cycle of a BlackBerry may be shorter than the actual contract (2 years). Units must be able to defray the cost of upgrading to new equipment in the event of a security issue that deems the current model as life cycled. Life-cycled equipment must not be recycled to other members in the organization. Once a life-cycled BlackBerry is replaced, it will be wiped and disposed of using standard logistic turn-in procedures.

(2) BlackBerry devices must be used with the appropriate CAC reader. This will allow for the use of CAC certificates for PKI-enabled e-mail. BlackBerry is an extension of Army in Europe official messaging; therefore, the use of digital signatures on all official message traffic is mandatory. The only Bluetooth device authorized for use with BlackBerry devices is the Research in Motion Smart Card Reader. No other Bluetooth device is authorized for use and the reader must not be configured to work with any other device (for example, workstation). Only the Army Chief Information Officer/G-6 may approve exceptions to this policy.

(3) The use of internal Bluetooth on BlackBerry devices for voice profiles (for example, “headset” and “hands-free”) is not authorized and must be disabled from the BES.

(4) BlackBerry devices must be maintained on property books. BlackBerry devices will remain with the unit when the user leaves the unit.

f. Authorized BlackBerry users in the Army in Europe will automatically be given the capability to view e-mail attachments and browse the Internet when a device is issued. Internet restrictions that apply to desktop and laptop computer systems also apply to BlackBerry devices (for example, blocked websites). Because of security concerns, the following BlackBerry features are currently not authorized:

(1) Bluetooth (the only exception for Bluetooth use is outlined in e(2) above).

(2) Global Positioning System (GPS) and maps.

(3) Tethered modems.

NOTE: Downward-directed information condition instructions may restrict some Blackberry features that are otherwise not restricted.

20. VOICE OVER INTERNET PROTOCOL (VOIP)

a. Only VoIP systems that have been tested, certified, and appear on the DISA-approved products list may be connected to the DSN. VoIP systems must also be fielded in the Joint Interoperability Test Command (JITC)-approved configuration in order to meet all the service requirements and specifications of the DISA DSN Generic Switching Center. Systems deployed in this manner can provide C2 services. Organizations, however, should maintain traditional DSN connectivity for critical C2 requirements.

b. USAREUR G6 approval is required before USAREUR or IMCOM-Europe units may procure, install, or use VoIP systems to store, process, or transmit information. In addition, non-USAREUR units must request USAREUR G6 permission to connect VoIP equipment to any network that is operated and maintained by 5th Signal Command. The VoIP request memorandum must be sent through the servicing NEC to the USAREUR G6 (AEIM-A). The USAREUR G6 will review the request and approve or disapprove.

(1) If approved, the requester must complete a system accreditation signed by the responsible designated approving authority, then submit an “authority to connect” request to the DISA Voice Connection Approval Office.

(2) A copy of the “authority to connect” approval memorandum will be provided to the 5th Signal Command G3, who will submit the engineering change proposal to the DISA Europe DSN Configuration Control Board (CCB) to authorize, engineer, and integrate the new system into the DSN. The VoIP system will not be connected to the network until the unit receives an “authority to connect” and approval from the DISA Europe CCB.

(3) The VoIP system and all necessary telephone switch and network interface equipment must be purchased by the requesting unit.

c. VoIP systems that use the Army in Europe NIPRNET or SIPRNET must obtain a CTO. This is to ensure compliance with overall network-security architecture and appropriate enclave security requirements, as well as to prevent a negative effect on the operation of these networks.

d. VoIP traffic between employee-owned information systems and Army in Europe information systems is prohibited.

21. REQUESTING BASE COMMUNICATIONS SERVICE

a. Indefinite BASECOM Requirements.

(1) **NECs.** After a unit’s BASECOM requirements have been validated, the requesting TCO will submit DA Form 3953 to the regional TOO. The TOO will—

(a) Assign a NEC-unique, DA Form 3953 PVN. The PVN ensures correct billing for the service. The PVN is an 11-digit numeric code:

1. Digits 1 through 3 represent the NEC.
2. Digits 4 through 7 represent the month and the year.
3. Digits 8 through 11 represent the sequential number of the request.

(b) Send the DA Form 3953 by fax (DSN 337-8832) or e-mail (basecom1@hq.5sigcmd.army.mil) to the 5th Signal Command (NETC-SEC-RM) for funding.

(c) Keep the original DA Form 3953, which may be needed in the future by the 5th Signal Command G8, the contracting office, or the Office of the Inspector General, HQ USAREUR.

(2) Deputy Chief of Staff, G8, 5th Signal Command. On receipt of a validated DA Form 3953 for BASECOM services from a USAG DRM, the 5th Signal Command G8 will—

(a) Contact the regional TOO listed in table 5 (for units in areas supported by a TOO).

(b) Send the DA Form 3953 to the Office of the Deputy Chief of Staff, G3, 5th Signal Command (for units in NATO-supported countries without TOOs (France, Portugal, and Spain)).

(3) TOOs. On receipt of a validated and funded DA Form 3953 for telecommunication services, the TOO will—

(a) Contract for the services with the host-nation telecommunications company.

(b) As part of the contracting process, provide a service date to the NEC, track the service installation, and send a copy of the commercial workorder to the 5th Signal Command (NETC-SEC-RM), Unit 29623, Box 0029, APO AE 09096-0029, to ensure proper billing.

b. Temporary and Exercise BASECOM Requirements. In addition to the requirements in subparagraph a above, requests for BASECOM services for exercises and temporary requirements will be submitted as follows:

(1) The requesting unit will send a copy of the exercise DA Form 3953 by fax to 5th Signal Command (NETC-SEC-RM) (DSN 337-8832).

(2) The Office of the Deputy Chief of Staff, G3, Headquarters, 5th Signal Command, will give a copy of the DA Form 3953 to the Deputy Chief of Staff, G8, Headquarters, 5th Signal Command, to ensure the correct start and end billing dates, and the availability of funds.

(3) 5th Signal Command (NETC-SEC-RM) will track the status of temporary and BASECOM requirements.

Table 5 Telecommunications Ordering Offices (TOOs)		
TOO	Telephone and Fax Number	Local Address
Germany		
Grafenwöhr Area HHD, 69th Signal Battalion (NETC-SER-EW) Unit 28130 APO AE 09114-8130	DSN 475-6563 Fax DSN 475-8491 Civilian 09641-83-xxxx	Lager Grafenwöhr Gebäude 313, Zimmer 201 92655 Grafenwöhr
Heidelberg/Kaiserslautern Area 43d Signal Battalion (NETC-SER-BNH) Unit 29227 APO AE 09014-9227	DSN 370-9592/9593 Fax DSN 370-9595 Civilian 06221-57-xxxx	Campbell Kaserne Gebäude 7N, Zimmer 116 Römerstraße 168 69126 Heidelberg
Stuttgart Area 52d Signal Battalion (NETC-SER-DOP) APO AE 09107	DSN 430-5557/8178 Fax DSN 430-5102 Civilian 0711-680-xxxx	Patch Kaserne Gebäude 2319 Kurmärker Straße 70569 Stuttgart
Wiesbaden Area 102d Signal Battalion (NETC-SER-FC) APO AE 09096	DSN 337-6576 Fax DSN 337-5396 Civilian 0611-705-xxxx	U.S. Army Airfield Gebäude 1007 Boyd Avenue 65205 Wiesbaden
Italy		
Livorno Area 509th Signal Battalion (NETC/SER-IDD) Unit 31301, Box 18 APO AE 09613-0018	DSN 634-7855/7999 Fax DSN 634-7099 Civilian 0444-51-xxxx	Camp Darby Tirrenia, Building 5131 (Livorno Depot Area) Pisa 56018 Italy
Vicenza Area 509th Signal Battalion (NETC-SER-IO/S3) Unit 31401, Box 47 APO AE 09630-0047	DSN 634-7855/7999 Fax DSN 634-7099 Civilian 0444-51-xxxx	Caserma Ederle Building 131 Via Della Pace 193, Vicenza 36100 Italy
Belgium, Netherlands, and Northern Germany		
39th Signal Battalion (NETC-SER-JS) Unit 21602 APO AE 09703-1602	DSN 360-7301/5566 Fax DSN 360-7252 Civilian 0031-46-443-xxxx	Borgerweg 10 6365 CW Schinnen The Netherlands

22. MANAGING OFFICIAL COMMERCIAL TELEPHONES

To help manage and control the cost of official commercial telephone service—

a. USAG commanders or their designated representatives will do the following:

- (1) Review the need for official commercial telephone services each year.
- (2) Assign each official commercial telephone to an individual designated in writing.
- (3) Ensure a separate AE Form 25-1F is maintained for each official commercial telephone.

(4) Review copies of AE Form 25-1F for official commercial telephones in their command, as appropriate. This review will identify—

(a) Under-used official commercial telephones that may no longer be required. These users will be requested to turn in these telephones to eliminate the possibility of abuse.

(b) Over-used official commercial telephones that may indicate unnecessary faxing, large-scale telephone abuse, or extensive use of dial-up modems with personal computers.

(5) Investigate meter units and local billings that do not match recorded logs. The local post, telephone, and telegraph billing system may sometimes generate incorrect bills.

(6) Consider seeking reimbursement from tenants who have DSN lines and also lease commercial telephones.

b. Units using official commercial telephone service will send completed copies of AE Form 25-1F to their designated USAG TCO for review at least once a year. The forms should be compared with telephone billing data provided by the 5th Signal Command G8 before submission, and reviewed for completeness and accuracy.

c. Individuals responsible for official commercial telephones will control access to and use of the telephone.

23. TELEPHONE ABUSE

Ready access to official telephone systems provides Army activities in the European theater the rapid communications required to accomplish their mission. With this access comes the potential for abuse. In addition to procedures in AR 25-1 and DA Pamphlet 25-1-1, TCOs will monitor DSN, 99 commercial access, official commercial telephone, and cell-phone service for abuse. The following also applies:

a. Calls to Be Investigated. The following are examples of DSN calls that management officials should investigate to prevent telephone abuse:

(1) “99+0” calls. Calls made to commercial numbers in Europe outside the local dialing prefix area should be reviewed for numbers that are called regularly and for calls placed late at night. Some calls for unofficial business or to commercial establishments that have no connection with the military may be justified. Commanders will decide which calls are authorized.

(2) “99+00” calls. These calls are to areas outside Europe and require a specific “class mark” on the telephone. The class mark indicates the capability of the telephone line. Investigators must ask the local wire chief at the local telephone exchange if the particular telephone is class-marked for “99+00” calls and has written authorization on file. These calls are often made to areas that have DSN service. Unless the call is a valid emergency and approved by the commander, it should be made using DSN “off-netting” or require a control number. Many “99+00” calls are made for routine business, such as to check on schools, promotions, reassignments, new arrivals, and job interviews. According to Army policy, routine business that does not constitute a valid emergency will be conducted through the mail or over a military-owned system.

(3) Calls lasting longer than 1 hour. Official business normally takes less than 1 hour to conduct over the telephone. Many longer calls are used to send data to a higher headquarters in the United States. Data transmission should be made through local Army in Europe networks according to the classification of the data to be transmitted.

(4) Calls costing more than \$25. Calls for official business normally cost less than \$25. Those costing more than \$25 should be investigated. These calls often result from extended modem use, “hung” switching equipment, or abuse.

NOTE: Since the implementation of DISN subscription service, DSN calls are not charged separately. DSN abuse, however, can still occur. For this reason, TCOs should review these calls for duration and frequency.

(5) Accidental zeroing. Accidental zeroing of official commercial telephone instruments equipped with unit meters will be investigated and reported on AE Form 25-1F.

(6) Other calls that should be investigated include the following:

(a) Calls to destinations outside Europe. To call these destinations, the caller must have specific authorization. If not authorized, the caller is liable for the cost of the calls.

(b) Repeated calls to the same number.

(c) Common military business calls to DSN numbers made on or through commercial systems (for example, pay inquiries, promotion information, communications checks).

b. Investigation Procedures.

(1) If telephone abuse is identified, the command of the unit involved in the abuse must be notified.

(a) The commander will investigate and identify the abuses and abusers and initiate action to collect reimbursement from abusers.

(b) The NEC, TCO, and commercial telephone management personnel at 5th Signal Command will help commanders identify and collect reimbursements. The NEC and the TCO will help document the abuse, identify the caller and the places called, determine the cost, and collect the reimbursement.

1. If a person accepts responsibility and is willing to reimburse the Government, reimbursement procedures will be initiated (c below).

2. If a person refuses to sign either form required to initiate the reimbursement process (c below), a Financial Liability Investigation in accordance with AR 735-5 is recommended.

(2) To compute the cost of an unauthorized call, investigators must determine the number of units used for the call.

(a) For commercial telephones, the meter will show the number of units used. This number should be annotated in the log.

1. If the log has been falsified, no overt action will be taken that may alert the abuser. Instead, the commander or supervisor will monitor the telephone to determine the extent of the abuse.

2. Unit commanders may prepare a request (DA Form 3953) for the local telephone and telegraph service to place a PIN register on the telephone. They may also request a copy of AE Form 25-1F through the USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351, showing details on commercial calls made.

(b) For DSN telephones, CAIRS reports show the duration of DSN and commercial (99) calls made, as well as the estimated cost of commercial calls.

(3) Investigators will prepare a brief written explanation of the investigation results or situation.

c. Reimbursement Procedures.

(1) Based on the results of the investigation or an employee's willingness to reimburse the Government, the unit's resource management (RM) personnel will prepare either a DD Form 1131 to collect funds in cash, which is the preferred method, or a DD Form 139 to collect funds by payroll deduction from the employee responsible for telephone abuse. To ensure the reimbursed funds are credited to the unit affected by the abuse, the RM personnel will enter the unit's line of accounting on DD Form 1131 or DD Form 139.

(2) To initiate deductions from an employee's pay, RM personnel will prepare DD Form 139 and send it to the local finance customer support team (FCST).

(3) To collect reimbursement funds in cash, the following steps must be taken:

(a) RM personnel will prepare a DD Form 1131.

(b) The employee responsible for the telephone abuse will sign the form and take it to the local FCST for processing.

(c) The FCST will prepare a deposit ticket. The employee will take the deposit ticket to the community bank and deposit the reimbursement funds in the 266th Financial Management Center (266th FMC) account.

(d) The employee will return to the FCST with the deposit voucher.

(e) The FCST will provide the employee a copy of DD Form 1131 with the number of the deposit ticket annotated on the form.

(f) The employee will provide his or her unit RM office a copy of the DD Form 1131. RM personnel will send a copy of the form to the USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351.

(g) The FCST will scan and send a copy of DD Form 1131 to the 266th FMC for processing.

24. TELEPHONE-CALL CONTROL NUMBERS

a. Telephone-call control is a tool signal managers use to maintain a responsive and cost-effective telephone system. Users who are not authorized direct-dial CONUS or international DSN access must obtain a control number from the responsible TCO for each call outside the theater.

b. Call-control procedures are as follows:

(1) Users who need to make official CONUS or international calls will contact the designated TCO and provide the desired telephone number, precedence, and an adequate justification for the calls.

(2) TCOs will—

(a) Obtain a set of valid control numbers from the Vaihingen Dial Service Assistance head operator each month.

(b) Verify the official nature of the requested call.

(c) Provide requesters a control number for each justified call. The format for a control number is as follows:

1. The letter *C* or *I* will be used to indicate a CONUS or international control number.

2. Two letters will be used to identify the control-number account established with the NEC.

3. A number between 00001 to 99999 will indicate the control numbers issued in the current month.

4. The letter *R* for routine, *P* for priority, *I* for immediate, and *F* for flash will be used to indicate the precedence established by the TCO.

Example: Control number *CAA00001P* would be issued for a CONUS call by control-number account AA. It was the first control number issued during the month. The TCO established priority precedence for the call.

(d) Record the required information as a line entry on AE Form 25-1G. The remarks column will validate the official purpose of the call. A control number for a CONUS call is valid for 7 days after the date of issue. A control number for an international call is valid until midnight of the day it was booked with the operator.

(e) Validate that the control numbers on the AE Form 25-1G were issued for official calls by signing the bottom of the form.

(f) Provide control-number logs to the dial-service attendant, as required.

(3) Telephone operators will—

(a) Verify call-control numbers by comparing them to the validated AE Form 25-1G before completing each call.

(b) Log calls to ensure control numbers cannot be reused.

25. INTEGRATED SERVICES DIGITAL NETWORK (ISDN) IN QUARTERS

a. Introduction. Commercial services in quarters paid for with appropriated funds are prohibited by public law. DA has obtained a limited exception to policy for commanders at division level or higher who are special C2 users as defined by Chairman of the Joint Chiefs of Staff Instruction 6215.01C. Each request for ISDN in quarters requires a legal review by the Office of the Judge Advocate, HQ USAREUR, and approval by the Chief of Staff, HQ USAREUR.

b. Requesting ISDN in Quarters. Requests for commercial ISDN in quarters will be prepared as a formal memorandum with the following information:

- (1) Name of the individual for whom the ISDN service is being requested.
- (2) Duty position.
- (3) Grade.
- (4) Primary duty location (installation, building number, and room number).
- (5) The primary network and e-mail server the individual will access through the ISDN.
- (6) The type and telephone number of dial-in telephone service currently installed to the server (for example, analog, ISDN).
- (7) The name and telephone number of the system administrator responsible for the server.
- (8) The location of both the individual's quarters and of the requested ISDN connection in those quarters.
- (9) A list of data services in use or that the individual will need in quarters. (Current and projected average daily use must be included for each type of service listed.)
- (10) The type of telecommunications service currently being used by the individual to access data services in quarters.
- (11) The typical, maximum data-transmission rates provided by the telecommunications services being used by the requester (for example, 9,600 to 56,000 bytes per second).
- (12) A justification for the request. The justification must explain why existing telecommunications services in the quarters do not adequately support the individual's requirements for data services.
- (13) The type of computer and operating system that will be connected to the ISDN line in the individual's quarters.
- (14) The signature of a HQ USAREUR staff principal (if the request is for someone assigned to HQ USAREUR) or that of a commander of a USAREUR command (if the request is for someone assigned to a USAREUR organization) or a USAG commander (if the request is for someone assigned to IMCOM-Europe).

c. Processing Requests. After the request is prepared and signed, the requester will send it—

(1) Through the USAREUR G6 (AEIM-A), Unit 29351, APO AE 09014-9351, for technical validation.

(2) Through the USAREUR Judge Advocate (AEJA-KF), Unit 29351, APO AE 09014-9351, for legal review.

(3) To the Chief of Staff, HQ USAREUR, Unit 29351, APO AE 09014-9351.

d. Approved Requests. If the Chief of Staff, HQ USAREUR, approves the request, the commercial ISDN service in quarters is subject to the following conditions:

(1) Only Government-provided computers will be connected to the commercial ISDN service.

(2) Organization system administrators must configure the computer connected to a commercial ISDN line in a way that denies unauthorized users access to servers other than those listed in the original request for service.

(3) Users will not be given the commercial ISDN telephone number.

(4) Commercial ISDN service may be used to send e-mail and other data through Army hosts only when the data is official business directly related to the C2 of military forces.

(5) Commercial ISDN service will not be used for routine voice communications, VTC, or mere convenience. Monthly billing statements list these and other types of connections and include a record of each call (for example, time, number called, duration, cost).

(6) The user's resource management office will—

(a) Review monthly billing statements and watch for evidence of potential abuse.

(b) Certify billing statements after reviewing them.

(c) Keep billing statements on file for annual revalidations.

(d) Notify the USAREUR G6 (AEIM-A) immediately on finding evidence of potential abuse of an ISDN line. The USAREUR G6 will coordinate the evidence with the Office of the Judge Advocate, HQ USAREUR, to determine whether or not abuse has occurred and if action is required.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

Chairman of the Joint Chiefs of Staff Instruction 6215.01C, Policy for Department of Defense (DOD) Voice Networks With Real Time Services (RTS)

DOD Directive 5100.35, Military Communications-Electronics Board (MCEB)

DOD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management

DOD 8570.01-M, Information Assurance Workforce Improvement Program

Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems

Director of Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

AR 25-1 and AE Supplement 1, Army Knowledge Management and Information Technology

AR 25-2, Information Assurance

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 71-9, Materiel Requirements

AR 710-1, Centralized Inventory Management of the Army Supply System

AR 735-5, Policies and Procedures for Property Accountability

DA Pamphlet 25-1-1, Information Technology Support and Services

AE Regulation 25-22, Use of U.S. Government Telecommunications Systems for Health, Morale, and Welfare Purposes

USEUCOM Spectrum Management Manual

USAREUR Tasking Order, DOD Directive 8570.01, Information Assurance Certification Compliance, message # 1104081, 18 May 2011

Military Communications-Electronics Board Publication 7, Frequency Resource Record System (FRRS) Standard Frequency Action Format (SFAF) (<http://jitc.fhu.disa.mil/>)

United States Army Joint Multinational Readiness Center Exercise Rules of Engagement

Information Assurance Best Business Practice, Training and Certification Update, 6 August 2010

SECTION II FORMS

DD Form 139, Pay Adjustment Authorization

DD Form 448, Military Interdepartmental Purchase Request

DD Form 1131, Cash Collection Voucher

DD Form 1494, Application for Equipment Frequency Allocation

DD Form 2056, Telephone Monitoring Notification Decal

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 3938, Local Service Request (LSR)

DA Form 3953, Purchase Request and Commitment

DA Form 4610-R, Equipment Changes in MTOE/TDA

AE Form 25-1D, Video Teleconferencing (VTC) Hub Registration

AE Form 25-1F, Commercial Telephone Log/Report

AE Form 25-1G, Telephone Control-Number Log

AE Form 25-1H, Army in Europe LandWarNet Remote-Access Request - Category 1

AE Form 25-1J, Army in Europe LandWarNet Remote-Access Request - Category 2

AE Form 25-1K, Army in Europe Remote-Access Computer-Security Compliance Inspection

GLOSSARY

18th Engr Bde	18th Engineer Brigade
266th FMC	266th Financial Management Center
AAFES-Eur	Army and Air Force Exchange Service, Europe
AE	Army in Europe
AE-ITT	Army in Europe Information Technology Training
AEPUBS	Army in Europe Library & Publishing System
AFNE	American Forces Network, Europe
AKO	Army Knowledge Online
APO	Army post office
AR	Army regulation
ARNG	United States Army National Guard
ATCTS	Army Training and Certification Tracking System
BASECOM	base communications
BES	BlackBerry Enterprise Server
C2	command and control
C4	command, control, communications, and computers
C4IM	command, control, communications, computers, and information management
CAC	common access card
CAIRS	Configuration Accounting and Information Retrieval System
CCB	configuration control board
CG	commanding general
CG, USAREUR	Commanding General, United States Army Europe
CHESS	Computer Hardware, Enterprise Software, and Solutions
CNN	Cable News Network
CODEC	coder/decoder
COMSEC	communications security
CONUS	continental United States
COTS	commercial off-the-shelf
CTO	certificate to operate
DA	Department of the Army
DCG, USAREUR	Deputy Commanding General, United States Army Europe
DCO	dial central office
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITCO	Defense Information Technology Contracting Organization
DKO	Defense Knowledge Online
DOD	Department of Defense
DODAAC	Department of Defense activity address code
DODAF	Department of Defense Architecture Framework
DRM	directorate of resource management
DRSN	Defense Red Switch Network
DSL	digital subscriber line
DSN	Defense Switched Network
DVS-G	Defense Video Services - Global
EHF	extremely high frequency
ELA	Enterprise License Agreement

ESD	Enterprise Service Desk
EU	European Union
FCST	finance customer support team
FIPS	Federal Information Processing Standard
FMFO	Frequency Management Field Office
FMO	Frequency Management Office, Command, Control, Communications, Computers, Intelligence, and Surveillance Division, Office of the Deputy Chief of Staff, G6, Headquarters, United States Army Europe
G2	deputy chief of staff, G2 (intelligence)
G3	deputy chief of staff, G3 (operations)
G4	deputy chief of staff, G4 (logistics)
G6	deputy chief of staff, G6 (information management)
G8	deputy chief of staff, G8 (resource management)
GAR	gateway access request
GS	General Schedule
GSM	Global System Mobile
HF	high frequency
HQ USAREUR	Headquarters, United States Army Europe
IA	information assurance
IAPM	information assurance program manager
IFSO	International Frequency Support Office
IM	information management
IMCOM-Europe	United States Army Installation Management Command, Europe Region
IMO	information management officer
IMUX	inverse multiplexer
INMARSAT	International Maritime Satellite
IP	Internet protocol
ISDN	integrated service digital network
IT	information technology
J2	deputy chief of staff, intelligence (joint staff)
JCIS	Joint and Coalition Information Systems
JFMO	joint frequency management office
JITC	Joint Interoperability Test Command
JMRC	United States Army Joint Multinational Readiness Center
JMTC	Seventh United States Army Joint Multinational Training Command
JNN	joint network node
JWICS	Joint Worldwide Intelligence Communications System
kb/s	kilobyte per second
KM	knowledge management
LAN	local area network
LSR	local service request
MB	megabyte
MCEB	Military Communications-Electronics Board
MCU	multipoint control unit
MHz	megahertz
MIB	military intelligence brigade
MLPP	multilevel precedence and preemption
MS	Microsoft
MSC	major subordinate command

MSE	mobile subscriber equipment
MTOE	modification table of organization and equipment
NAF	nonappropriated fund
NARFA	National Allied Radio Frequency Agency
NATO	North Atlantic Treaty Organization
NCOIC	noncommissioned officer in charge
NEC	network enterprise center
NETCOM/9th SC(A)	United States Army Network Enterprise Technology Command/9th Signal Command (Army)
NIPR	Unclassified but Sensitive Internet Protocol Router
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
PIN	personal identification number
PKI	public key infrastructure
PM/QA	preventive maintenance/quality assurance
POC	point of contact
PSS	preferred subscriber service
PVN	purchase voucher number
RF	radio frequency
RGBAN	Regional (Global) Broadband Area Network
RM	resource management
RSSC	regional satellite communications support center
S2	intelligence officer
S3	operations and training officer
S4	logistician
S6	information management officer
SAR	satellite access request
SATCOM	satellite communications
SBCT	Stryker brigade combat team
SCIF	sensitive compartmented information facility
SFAF	standard frequency action format
SIM	subscriber identity module
SINGARS	Single Channel Ground and Airborne Radio System
SIPR	Secret Internet Protocol Router
SIPRNET	Secret Internet Protocol Router Network
S/MIME	secure/multipurpose Internet mail extension
SMARTS	Spectrum Management Analysis and Record Tracking System
SME	subject-matter expert
SOI	signal operating instruction
SSAA	system security accreditation agreement
SSL	secure sockets layer
STE	secure telephone equipment
STIG	security technical implementation guide
STU	secure telephone unit
TCO	telephone control officer
TDA	table of distribution and allowances
TDY	temporary duty
TLS	transport layer security
TOO	telecommunications ordering office
TSACS	Terminal Server Access Control System

UHF	ultrahigh frequency
UMPIRE	Unit Morale Call Personal Identification Number Issuing Resource Europe
UMTS	Universal Mobile Telecommunications System
URL	uniform resource locator
U.S.	United States
US1	unclassified sensitive one
US2	unclassified sensitive two
USAG	United States Army garrison
USAR	United States Army Reserve
USAREUR	United States Army Europe
USAREUR G2	Deputy Chief of Staff, G2, United States Army Europe
USAREUR G3	Deputy Chief of Staff, G3, United States Army Europe
USAREUR G6	Deputy Chief of Staff, G6, United States Army Europe
USAREUR G8	Deputy Chief of Staff, G8, United States Army Europe
USEUCOM	United States European Command
VHF	very high frequency
VoIP	voice over Internet protocol
VPN	virtual private network
VTAADS	Vertical - The Army Authorization Documents System
VTC	video-teleconferencing/video-conference