Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command
Europe
Sembach, Germany

Army in Europe
Pamphlet 25-13*

12 September 2017

Information Management

Army in Europe Telecommunications and Unified Capabilities

This pamphlet supersedes AE Pamphlet 25-1, 31 October 2012; AE Form 25-1D, October 2012; AE Form 25-1F, October 2012; and AE Form 25-1G, October 2012.

For the Commander:

KAI R. ROHRSCHNEIDER
Brigadier General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This pamphlet provides Army in Europe procedures and USAREUR's best-business practices for implementing the policy and complying with the standards of AR 25-13.

Applicability. This pamphlet applies to all U.S. Army in Europe organizations and personnel as well as all other DOD and non-DOD organizations and personnel that use the Army in Europe networks.

Records Management. Records created as a result of processes prescribed by this pamphlet must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Forms. This pamphlet prescribes AE Form 25-13B, AE Form 25-13C, and AE Form 25-13D, which supersede AE Form 25-1D, AE Form 25-1F, and AE Form 25-1G respectively. AE and higher-level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at *http://www.eur.army.mil/aepubs/*.

Suggested Improvements. The proponent of this pamphlet is the Programs and Policy Branch, Programs, Policy and Projects Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR (mil 537-6223). Users may send suggested improvements to this pamphlet by e-mail to the USAREUR G6 (AEIM-A) at *usarmy.wiesbaden.usareur.list.g6-policy@mail.mil.*

Distribution. This pamphlet is available only electronically and is posted in AEPUBS at *http://www.eur.army.mil/aepubs/*.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

CONTENTS

SECTION I
GENERAL

SECTION II
FREQUENCY-SPECTRUM MANAGEMENT

SECTION III
VOICE NETWORKS

SECTION IV
NETWORK SERVICES IN GOVERNMENT QUARTERS

SECTION V
MOBILE SERVICES

SECTION VI
VIDEO-TELECONFERENCE SERVICES

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

Appendixes

Tables

Figures

SECTION I
GENERAL

1. PURPOSE

This pamphlet provides implementing guidance, procedures, and responsibilities for obtaining and maintaining information management (IM) and telecommunications equipment and services for information management officers (IMOs); telephone control officers (TCOs); other IM, information technology (IT), and telecommunications managers; and Army in Europe (glossary) network users and using organizations.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. RESPONSIBILITIES

AR 25-13 requires all Army in Europe units; leaders; IM, IT, and telecommunications managers; and network users to manage telecommunications assets in ways that conserve Government resources. In accordance with AR 25-13, the following duty positions and organizations are responsible for the associated tasks:

a. Chief of Staff (CoS), HQ USAREUR. The CoS, HQ USAREUR, is—

(1) The USAREUR concurrence authority for (approval authority for sending) requests to USEUCOM for Defense Red-Switched Network (DRSN) service (para 5b(2)).

(2) The USAREUR approval authority for requests for Government-funded, commercial Internet service provider (ISP)-in-Quarters service (para 17a).

b. Office of the Deputy Chief of Staff (ODCS), G3/5/7, HQ USAREUR. The ODCS, G3/5/7, HQ USAREUR, will—

(1) Serve as the approver for cell-phone authorizations (para 18a) and other commercial mobile device (CMD) authorizations (paras 19c and e) for HQ USAREUR staff offices and USAREUR major subordinate commands (MSCs).

(2) Manage and control cell-phone equipment for contingencies and exercises according to the procedures in paragraphs 18h and 18i respectively as well as other ODCS, G3/5/7, HQ USAREUR, internally developed procedures.

(3) Provide video-teleconference (VTC) scheduling services (para 21d).

c. ODCS, G6, HQ USAREUR. The ODCS, G6, HQ USAREUR will—

(1) Conduct technical validations of DRSN requests to support CoS, HQ USAREUR, concurrence decisions (para 5b(2)).

(2) Provide Army in Europe spectrum managers in the Frequency Management Office (FMO), Operations, Plans, and Exercises (OPLEX) Division, ODCS, G6, HQ USAREUR, who are responsible for the spectrum-management tasks listed in paragraph 6b(1).

(3) Serve as (that is, the Deputy Chief of Staff, G6, USAREUR) the designated accreditation authority (DAA) for Army in Europe voice over Internet protocol (VoIP) systems (para 10c).

(4) Prescribe the authorization policy for Preferred Subscriber Service (PSS) and (the Deputy Chief of Staff, G6, USAREUR) serve as the approval authority for exceptions to that policy (para 16c).

(5) Provide technical validations of ISP-in-Quarters service requests to support CoS, HQ USAREUR, review and decision regarding those requests (para 17c(2)).

d. 2d Signal Brigade (2d Sig Bde). The 2d Sig Bde will—

(1) Provide an individual (assigned or additional duty as applicable) to serve as the theater telephone control officer (TCO).

(2) Provide telecommunications ordering office (TOO) services according to paragraph 13c(1) and provide the USAREUR G6 with updates to the regional TOO contact information (table 1), as required.

(3) Supervise Army in Europe telephone Dial-Service Assistance system operations. Dial-Service Assistance operators are responsible for specific tasks identified in paragraphs 14b(3) and 14c(1).

Table 1
Telecommunications Ordering Offices

TOO Unit Address	Telephone and Fax	Local Address
Germany		
Grafenwöhr Area		
HHD, 69th Sig Bn (NETC-SER-EW) Unit 28310 APO AE 09114-8130	Mil: 314-521-2666/2175 Civ: 0049-(0)611-143-521-2666/2175	Lager Grafenwöhr Gebäude 501, Zimmer 9 92655 Grafenwöhr
Kaiserslautern Area		
102d Sig Bn (NETC-SER-FH) Unit 29800 APO AE 09165-9800	Mil: 314-483-6333 Civ: 0049-(0)631-411-6333 Mil fax: 314-483-8999	Kleber Kaserne Gebäude 3203, Zimmer 110 Mannheimer Strasse 67657 Kaiserslautern
Stuttgart Area		
52d Sig Bn (NETC-SER-DS) Unit 30401 APO AE 09131-0401	Mil: 314-430-5557/5430 Civ: 0049-(0)711-680-5557/5430 Mil fax: 314-430-5049	Patch Kaserne Gebäude 2319 Kurmärker Straße 70569 Stuttgart
Wiesbaden Area		
102d Sig Bn (NETC-SER-FH) Unit 29800 APO AE 09096-9800	Mil: 314-565-2196/2197 Civ: 0049-(0)611-143-565-2196 /2197 Mil fax: 314-337-5396	Clay Kaserne Gebäude 1008 Phelps Avenue 65205 Wiesbaden
Italy		
509th Sig Bn (NETC-SES-FU) Unit 31401, Box 47 APO AE 09630-0047	Mil: 314-637-2121/2536 Civ: 0039-0444-66-2121/2536 Mil fax: 314-637-6214	Caserma DelDin, Viale Ferrarin 36100 Vicenza ITALY
Belgium and Northern France		
39th Sig Bn (NETC-SER-JO) Unit 21602 APO AE 09708-1602	Mil: 314-361-5572 Civ: 0032-(0)68-27-5572	Building 70020 Grand Rue 56 7950 Chievres BELGIUM
Netherlands, Northern Germany, and the United Kingdom		
39th Sig Bn (NETC-SER-JS) Unit 21602 APO AE 09703-1602	Mil: 314-360-7304 Civ: 0031-(0)46-443-7304	Borgerweg 10 6365 CW Schinnen NETHERLANDS

e. Army in Europe Unit Commanders. Unit commanders are ultimately responsible for their unit's conservation of telecommunications assets. Commanders of units using Army in Europe networks will—

(1) Appoint additional duty TCOs to manage unit telecommunications assets, improve accountability, and provide program oversight and control, as required and as identified in (a) and (b) below and in accordance with AR 25-13. Appendix B (fig B-1) provides a sample TCO appointment order.

(a) For USAREUR MSCs, commands under the operational control of USAREUR (USAREUR OPCON commands (glossary), and any other commands directly subordinate to USAREUR through a command relationship (that is, assigned, attached, OPCON, or under administrative control (ADCON)), commanders at battalion level and above will appoint an individual with the additional duty of TCO. Units below battalion level may be directed to appoint a TCO based on geographic dispersion or as required.

(b) For other Army in Europe units and DOD or Army tenant units that use Army in Europe networks, commanders of brigade-level and above units will appoint (and commanders of battalion-level and below units may appoint or be directed to appoint) an individual with the additional duty of TCO.

(2) Identify a command frequency manager, as required and identified in (a) through (c) below, to the FMO, OPLEX, ODCS, G6, HQ USAREUR. The command's TCO may serve as the command frequency manager. If so, the duty should be incorporated in the TCO's additional-duty description.

(a) If required by mission volume, HQ USAREUR staff principals may appoint for their staff office a "command" frequency manager or rely on action-officer coordination with the FMO, OPLEX, ODCS, G6, HQ USAREUR, to support their frequency requirements.

(b) USAREUR MSCs, USAREUR OPCON commands, and any other commands directly subordinate to USAREUR through a command relationship will identify (appoint if required) a command frequency manager and inform the FMO, OPLEX, ODCS, G6, HQ USAREUR of the frequency manager's identity.

(c) Other Army in Europe units or Army and DOD units that rely on Army in Europe networks will identify (appoint if required) an individual from within the highest in-theater headquarters of their agency's units a command frequency manager to coordinate and synchronize frequency requirements with the FMO, OPLEX, ODCS, G6, HQ USAREUR.

f. Command Frequency Managers. Command frequency managers at HQ USAREUR staff offices and the higher headquarters of supported units will manage their organization's and subordinate units' frequency requirements and coordinate with the Army in Europe spectrum managers at the FMO, OPLEX Division, ODCS, G6, HQ USAREUR, according to the responsibilities in paragraph 6b(2).

g. Unit TCOs. Unit TCOs are responsible for managing all unit telecommunication assets for the unit commander to ensure mission effectiveness while conserving Government resources. TCOs are specifically responsible for the detailed tasks identified in paragraphs 6b(3), 7b, 14b(2), and 14c(2).

h. Army in Europe Network Users. Users of the Army in Europe networks are responsible for complying with all applicable telecommunications policy and procedures and particularly will—

(1) Use the frequency-request procedures in paragraph 6b(3) when requesting frequencies.

(2) Use appropriate answering machine and voicemail procedures (para 12b).

(3) Properly mark all secure telephone equipment (STE) (para 12c).

(4) Coordinate all user-level requests directly through their TCO or by using the 119/Information Technology Service Management (ITSM) (also known as Remedy) system (para 13a(1)) and all unit-level telecommunications (specifically voice-network) requirements (para 13) through their unit TCO according to base communications (BASECOM) ordering procedures (para 13b).

(5) As required, use proper telephone call-control procedures (para 14b) and, if applicable, monitor 99-Access and official commercial telephone service lines to limit potential abuse (para 14c(3)).

(6) If issued an Army in Europe CMD (includes cell phones), sign and comply with the Army in Europe Mobile Device User Agreement (AE Form 25-13A (formerly, AE Form 25-1M), paras 18b(4) and 19c(4)).

5. LONG-HAUL AND DEPLOYABLE COMMUNICATIONS

The Defense Information Systems Agency (DISA) is the DOD-mandated provider of all long-haul communications services, including long-haul communication services to support deployed operations.

a. Long-Haul Communication Services. Long-haul communication services are those that span distances of more than 20 miles or go outside an installation. DISA provides these services either directly through military telecommunications organizations or through the Defense Information Technology Contracting Organization (DITCO), DISA, which establishes contracts with commercial vendors. TCOs may request long-haul services by completing a web-based telecommunications request (paras 6c(4), 7b(3), and 13b).

b. Common DISA Long-Haul Communication Services. The Army pays for common DISA-operated network services (that is, the Defense Information Systems Network (DISN) services) that the Army uses. The following six categories comprise the most common DISN services (*http://www.disa.mil/network-services*) that the Army in Europe uses:

(1) The Sensitive But Unclassified (SBU) Voice Network. The SBU Voice network comprises both the Defense Switched Network (DSN) services and basic SBU (that is, VoIP) services. The DOD and the Chairman of the Joint Chiefs of Staff have mandated that all DOD command and control (C2) elements in theater must use the SBU Voice network as the primary voice solution.

NOTE: SBU Voice in Quarters is usually referred to as the PSS (para 16).

(2) The DRSN. The DRSN (sometimes known as the Multilevel Secure Voice network) is a cryptographically secured network that is part of the DISN, but independent of SBU Voice. Units will usually connect into a DRSN switch using STE.

(a) DRSN is usually reserved for use by general officers (GOs).

(b) To receive DRSN service, units must send a memorandum requesting service through the USAREUR G6 (AEIM-A) (for technical validation) and the CoS, HQ USAREUR (for concurrence), and to the USEUCOM J6 (for approval).

(3) The Army in Europe NIPRNET. The Army in Europe NIPRNET is an Internet-protocol (IP)-driven network that can be used to send information that is classified at no higher than controlled unclassified information (CUI) (for example, information marked For Official Use Only (FOUO), information containing personally identifiable information (PII), other unmarked information that is treated as sensitive or CUI).

(4) The 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.

(5) The Joint Worldwide Intelligence Communications System (JWICS). The JWICS is a G2 or J2 network service that can be used to send information classified up to Top Secret.

(6) The DISA VTC Hub Service. DISA routes both dial-up integrated service digital network (ISDN) VTC traffic and IP VTC traffic through its hub in Stuttgart, Germany. The DISA hub is intended mainly for transatlantic VTC traffic.

(7) USAREUR VTC Hubs. USAREUR maintains VTC hubs (supported by the DISA network) in Kaiserslautern, Germany, and Wiesbaden, Germany, for connecting to the DISA hub in Stuttgart or to other Army in Europe VTC hubs and sites.

c. Non-Common (as defined by DISA) Long-Haul Communication Services. DISA also provides the following categories of service for unique, including deployed operations, mission requirements:

(1) Dedicated Circuits. Dedicated circuits for voice or data to span distances of more than 20 miles must be provided by DISA. In accordance with AR 25-13, unit requests for exception to policy must be sent through the USAREUR G6 (AEIM-A) for approval.

(2) Iridium Telephones. Iridium telephones are hand-held satellite-radio telephones that can also be used to transmit data. The DOD currently has a contract with Iridium through October 2018 that pays for all service costs, but units must purchase the hardware with their own funds. Service can be ordered through DISA Direct at *https://www.disadirect.disa.mil/products/asp/welcome.asp*.

(3) International Maritime Satellite (INMARSAT). INMARSAT is a portable satellite radio telephone that can also transmit data.

(4) Regional (Global) Broadband Area Network (RGBAN). The RGBAN is a portable satellite-radio telephone that can also transmit data.

(a) The RGBAN system uses four newer INMARSAT satellites and provides a broadband IP instead of the usual INMARSAT analog and ISDN interface. The IP interface permits direct access to the Army in Europe NIPRNET and SIPRNET.

(b) The RGBAN model Hughes HNS-9201 offers IP data transfer rates of up to 492 kilobytes per second (Kb/s), as opposed to the ISDN INMARSAT, which provides only up to 64 Kb/s.

(c) RGBAN usage is computed by the megabyte (MB) as opposed to the ISDN INMARSAT, for which usage is computed by the minute.

(5) Thuraya Telephones. The Thuraya is a portable satellite-radio telephone that can also transmit data.

(6) Transponders. For emergencies, exercises, and temporary locations, a unit may rent a satellite transponder (from or through DISA) with a specified bandwidth.

SECTION II
FREQUENCY-SPECTRUM MANAGEMENT

6. SPECTRUM MANAGEMENT

In Europe, U.S. Armed Forces frequency-transmitting equipment requires approval by the host nation (HN) in which it will be used before the equipment can be used. Army in Europe units will not begin to use or continue operating equipment that emit radio frequency (RF) energy or uses a frequency spectrum without properly requesting and receiving authorization for a frequency assignment or validation of an existing assignment through the appropriate USAREUR POC (a below). DOD and other tenant agencies that use Army in Europe networks may also coordinate their frequency-authorization requirements through the USAREUR POCs using these Army in Europe procedures.

a. Army in Europe Spectrum-Management POCs. Table 2 lists the POCs in the FMO, OPLEX Division, ODCS, G6, HQ USAREUR, who provide spectrum management for the Army in Europe.

Table 2
Army in Europe Spectrum-Management POCs

Position	Military Telephone Number
Chief, FMO, ODCS, G6, HQ USAREUR	314-537-6378
Battlefield spectrum managers	314-537-6379/6365/6369/6373
Satellite requests	314-537-6364/6368

b. Spectrum-Management Responsibilities.

(1) Army in Europe Spectrum-Manager Responsibilities. The Army in Europe spectrum managers in the FMO, OPLEX Division, ODCS, G6, HQ USAREUR, will—

(a) Work directly with HQ USAREUR staff and Army in Europe unit planners and frequency managers to forecast and plan for frequency requirements.

(b) Coordinate frequency approval for new equipment fielding initiatives.

(c) Assess and validate frequency requests and request frequency assignments from USEUCOM and the HN.

(d) Enforce lead-time standards for frequency requests.

(e) After researching and validating that a frequency or frequencies are no longer required, return unused frequencies to the HN.

(f) Train and assist Army in Europe unit frequency managers.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

(2) Command Frequency Managers. Command frequency managers at HQ USAREUR staff offices (if applicable), USAREUR MSCs, 2d Sig Bde, 66th MI Bde, and other Army in Europe or DOD tenant units will—

(a) Receive, review, validate, and provide assistance with frequency requests from their subordinate organizations according to their command's internal procedures.

(b) Ensure frequency requests for use in the USEUCOM theater are processed through the established Army in Europe coordination routing ((3)(a) below) to request appropriate local or international approval.

(3) Frequency Requesters. Frequency requesters will—

(a) Send frequency requests in the Standard Frequency Action Format (SFAF) using one of the authorized Internet-based spectrum-collaboration applications (that is, either Mercury or Spectrum XXI) in a timely manner according to the procedures in subparagraph c below.

(b) Route requests through intermediate command frequency managers, if applicable, and to the FMO, OPLEX Division, ODCS, G6, HQ USAREUR.

(c) Contact their unit frequency manager (or command frequency manager (if applicable)) at the HQ USAREUR staff office, unit, or next higher headquarters unit for assistance and review of their request before sending any frequency requests directly to the FMO, OPLEX Division, ODCS, G6, HQ USAREUR (using either the Mercury or Spectrum XXI applications).

(d) Before purchasing any RF equipment or entering into any contractual obligations involving the use of RF-dependent devices, ensure the appropriate spectrum needed by the device can be supported (is not restricted in that HN). This likely requires coordination with frequency managers.

(e) Before actually requesting a frequency assignment, review their requirements to ensure the request is for only the minimum—

1. Number of frequencies necessary to accomplish the mission.

2. Transmitter power and antenna height or gain necessary to ensure adequate coverage.

(f) Revalidate existing frequency assignments and frequency-assignment parameters routinely (at least every 12 months) to ensure—

(a) Electromagnetic-radiating-equipment operations are in compliance with the authorized parameters in the frequency-assignment notification.

(b) The requirement still exists as stated and send appropriate modifications, renewals, or deletions to the unit, installation, and command frequency managers and to the Army in Europe spectrum managers, as required.

(g) Obtain approval from the appropriate Army in Europe spectrum manager before modifying emitters or antennae (for example, increase power, change antenna height or gain).

c. Frequency-Request Types and Suspenses. Army in Europe units and the HQ USAREUR staff will use the procedures in (1) through (4) below to request frequencies (temporary, permanent, satellite or gateway, and other frequency services). An approved DD Form 1494 is required before a frequency may be assigned. The appropriate approving or notifying agency will send the disposition of the frequency-assignment request to the requester through the Mercury or Spectrum XXI application. Requests may be approved, completely disapproved, or partly approved with limitations.

(1) Temporary Frequency Requests. Temporary frequency requests are requests for frequencies that will be used for 90 days or less.

(a) Suspense for Temporary Requests. Requesters must send temporary frequency requests at least 75 calendar days before the start-of-use date or the start of the event or exercise. The FMO may disapprove late requests.

NOTE: USEUCOM established and strictly enforces the 75-day standard based on a HN standard of 70 calendar days that the HN requires to process each request.

(b) Late Temporary Requests. If a requester submits a frequency request later than 75 calendar days before the start-of-use date, the FMO may deny the request. The FMO will, however, process the request if the FMO receives a memorandum (usually coordinated through S3 or G3 staff channels) with the request explaining why the request is late and justifying the need.

1. Even if processed by the FMO, late requests may still be disapproved by the HN (that is, the responsible agency of the applicable HN:, usually named the National Allied Radio Frequency Agency (NARFA)–Nation-X (for example, NARFA–Germany)).

2. Units may send digital copies of signed justification memorandums to the FMO by e-mail at *usarmy.wiesbaden.usareur.list.dl-g6-frequency-management-office@mail.mil*.

3. The justification memorandum must be on unit letterhead stationery, be signed by the first colonel (or civilian equivalent) in the chain of supervision, and include at least the following information:

a. An explanation as to why the request is late.

b. A description of the effect a disapproval of the request will have on the unit.

c. A list of steps the unit will take to mitigate the risk of future late requests.

(2) Permanent Frequency Requests. Permanent frequency requests are requests for frequencies that will be used for longer than 90 days.

(a) Requests. Units must send permanent frequency requests (in the SFAF and using the Mercury or Spectrum XXI application) by at least 185 calendar days before the intended start-of-use date or the exercise or event for which the frequency is needed.

(b) Late Permanent Requests. If a requester submits a permanent frequency request later than 185 calendar days before the start-of-use date, the FMO may deny the request. The FMO will, however, process the request if the FMO receives a memorandum with the request explaining why the request is late and justifying the need. For late permanent frequency requests, requesters will follow the procedures in (1)(b) above.

(3) Satellite-Access Requests (SARs) and Gateway-Access Requests (GARs). Requests to use satellite-communication frequencies and equipment must be sent in the proper SAR or GAR format. Units must usually send SARs and GARs by 30 calendar days before the required start-of-use date.

(4) Other Army Service Requests (ASRs). The 2d Sig Bde is responsible for processing ASRs through the web-based Army Centralized Access System to request DISN services (for example, telephone numbers, IP addresses). For any frequency requirements not identified in (1) through (3) above, requesters should coordinate through their TCO chain to use the usual ASR process.

d. Acquisition of Frequency-Emitting Equipment. Commanders and units will ensure that any frequency-transmitting equipment being considered for purchase (particularly, commercial off-the-shelf (COTS) equipment) or issue (for example, lateral transfer) is coordinated with the USAREUR FMO. Units may contact the FMO directly for help in determining if equipment operates in an authorized band.

(1) Equipment Purchase Restrictions. No frequency-emitting COTS equipment acquisition is authorized without prior coordination with the USAREUR FMO. Commanders and leaders at all levels must ensure that Government funds are not wasted on equipment that is not supportable by an authorized frequency in the HN where it is intended to be used.

(2) European Union Certified Equipment. Equipment that was manufactured or is 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 also be eligible for an expedited approval process. Units must still contact the USAREUR FMO for details before purchasing EU-certified COTS equipment.

(3) Non-EU-Certified Equipment. Equipment that was manufactured in the United States may not be EU-certified. Because the United States and Europe use different portions of the electromagnetic spectrum for different purposes, equipment manufactured for use in the United States may operate in a band that is reserved for other purposes in Europe. If the equipment is not EU-certified but operates in an authorized band, the requester must complete DD Form 1494 and use the spectrum-certification process (also called the frequency-allocation or JF-12 process) to acquire the equipment.

e. Frequency Request Process. The USAREUR FMO will enforce the use of the official chain of approval.

(1) Workflow and Chain of Approval. Figure 1 provides the workflow (applicable agencies up through the approving authority) and identifies the approval agencies for the various types of frequency requests. Requesters should pay particular attention to the total lead time in the dashed box for each request category.

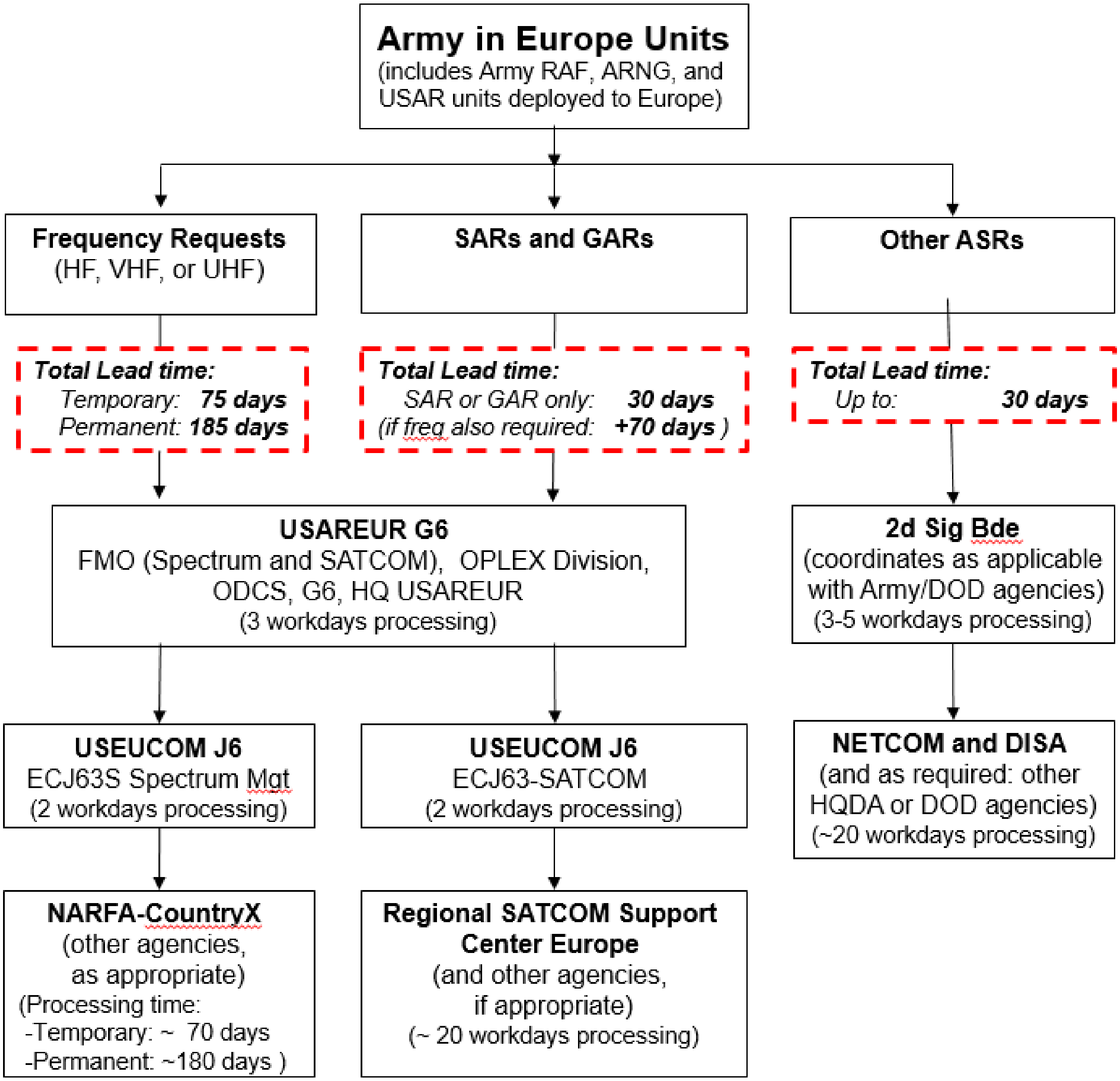
Army in Europe Units
(includes Army RAF, ARNG, and USAR units deployed to Europe)
Frequency Requests
(HF, VHF, or UHF)
SARs and GARs
Other ASRs
Total Lead time:
Temporary: 75 days
Permanent: 185 days
Total Lead time:
SAR or GAR only: 30 days
(if freq also required: +70 days)
Total Lead time:
Up to: 30 days
USAREUR G6
FMO (Spectrum and SATCOM), OPLEX Division, ODCS, G6, HQ USAREUR
(3 workdays processing)
2d Sig Bde
(coordinates as applicable with Army/DOD agencies)
(3-5 workdays processing)
USEUCOM J6
ECJ63S Spectrum Mgt
(2 workdays processing)
USEUCOM J6
ECJ63-SATCOM
(2 workdays processing)
NETCOM and DISA
(and as required: other HQDA or DOD agencies)
(~20 workdays processing)
NARFA-CountryX
(other agencies, as appropriate)
(Processing time:
-Temporary: ~ 70 days
-Permanent: ~180 days)
Regional SATCOM Support Center Europe
(and other agencies, if appropriate)
(~ 20 workdays processing)

Figure 1. Frequency Request Workflow and Chain of Approval

(2) Frequency Manager's Planning Checklist. Table 3 provides a sample format of a tool for frequency managers at all levels to help them manage the request process while determining frequency needs and requesting authorizations to support those needs. Such a table or checklist is particularly useful for S3 or G3 offices during their exercise and operations planning cycles.

Table 3
Frequency Manager's Planning Checklist

Data Element	Unit 1	Unit 2	Unit 3
Unit name:			
Equipment being used:			
Frequencies needed: (Identify if request is temporary (temp) or permanent (perm) after each frequency.)			
Start date of use, exercise, or event:			
Number of days until exercise or deployment			
Required submission date (Y/N): (Y/N: Is request late?)			
Letter of justification needed? (Yes or No):			
Anticipated turn-off date:			
Date sent to USAREUR FMO:			

(3) Mercury. USAREUR implemented the Mercury application in the Army in Europe to enable units without Spectrum XXI (classified-network) access to send unclassified frequency proposals. More information about Mercury is available at *https://mercury.dreamhammer.com/mercury.html*.

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

(b) Connectivity and Security. Users may connect to Mercury through the (NIPRNET) Internet using secure connectivity when their system complies with the restrictions in 2 below.

1. Secure Connectivity. Users must access Mercury using a "hypertext transfer protocol over a secure-sockets layer (SSL)" (https)-enabled web-browser. Users should refer to the help module of their web-browser to find out how to activate SSL 2.0 or 3.0 and transport-layer security (TLS) 1.0.

2. DOD-Access and Domain Restrictions. Users connecting to Mercury 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. Users must also use a DOD common access card (CAC) to access the system.

(c) User Accounts. Users must acquire a Mercury user account to access the system by providing the requested information at the Mercury login and account-request page (*http://mercury.dreamhammer.com/*). After users send the request through the system, the site administrator will create an account and send logon information to the user-provided e-mail address.

(d) Data-Classification Restriction. Because Mercury uses the NIPRNET (Internet) for data transfer, the Mercury system is restricted to handling only unclassified frequency proposals. Users are responsible for ensuring that any frequency-related data entered in the system is unclassified data.

(e) User Resources. Mercury provides the following features and aids to help the user during the frequency-proposal process:

1. Template Quick-Help Icons. When completing the frequency request according to the template, users may view additional information about data requirements for a particular line item by placing their cursor on the ? icon next to the line item.

2. MCEB Publication 7. Military Communications-Electronics Board (MCEB) Publication 7 established the Frequency Resource Record System and issued the standards for the SFAF. The main menu of Mercury provides a link to MCEB Publication 7 on the left side of the screen so users can verify formats and data requirements while creating their frequency proposal.

3. 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 Mercury 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.

4. Mercury Help. Mercury Help provides users instructions on performing basic system functions.

f. Special Criteria for Frequency Use at U.S. Training Areas in Europe. Units conducting exercises or training events at training areas in Grafenwöhr or Hohenfels should be prepared to conduct a coordination meeting with the training area S6 or G6 by at least 70 calendar days before the event and to produce their own signal operating instruction (SOI) for Single Channel Ground and Airborne Radio System or other combat radio-net systems.

(1) The POC at the ODCS, G6, Headquarters, 7th Army Training Command (7th ATC), in Grafenwöhr is the 7th ATC Frequency Manager at military 314-475-7940, civilian 0049-(0), or e-mail: *usarmy.grafenwoehr.jmtc.list.g6-all@mail.mil*.

(2) The POC for the ODCS, S6, Headquarters, United States Army Joint Multinational Readiness Center (JMRC), 7th ATC, in Hohenfels is the JMRC Frequency Manager at military 314-520-5060, civilian 0049-(0)9472-83-5060, or e-mail: *usarmy.jmrc.7atc.list.dl-jmrc-s6@mail.mil*.

(3) During the initial coordination meeting, the unit must be prepared to do the following:

(a) Provide the training-area POC with a list of all modified table of organization and equipment (MTOE) and non-MTOE frequency-emitting equipment that the unit will bring to the training event. Units will not bring COTS radios, including Motorola walkabouts, to the training rotation unless the JMRC or 7th ATC Frequency Manager has approved.

(b) Discuss event SOI requirements. The training area S6 or G6 will be responsible for generating all SOI data for all the event-participating units, to include Allied units. The unit will be responsible for publishing and distributing the actual SOI.

(4) When planning networks for the event, the unit remains responsible for sending frequency requests to the USAREUR FMO using the Mercury (*http://mercury/dreamhammer.com/*) or the Spectrum XXI applications according to the procedures in subparagraphs 6e(3)(a) through (e) above. The unit may contact the USAREUR FMO to request help with establishing a Mercury account if required.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

(5) If training units fail to comply with frequency restrictions at Grafenwöhr (7th ATC) and Hohenfels (JMRC), the units may cause harmful radio-frequency interference with training-area electronic systems and cause degradation or loss of training feedback data for their own unit or other training units. Therefore, units training at Grafenwöhr and Hohenfels—

(a) Are forbidden from using home-station SOIs or frequency lists.

(b) Will use frequencies only approved by the appropriate training area frequency manager.

SECTION III
VOICE NETWORKS

7. THE ARMY IN EUROPE TELEPHONE CONTROL OFFICER PROGRAM

In the Army in Europe, unit TCOs are responsible, usually as an additional duty, for managing, monitoring, and modifying unit telecommunications assets to support the mission while conserving Government resources.

a. General. To improve accountability, conserve resources, and comply with AR 25-13, Army in Europe units will appoint TCOs at every level where program oversight and control are required. Brigade-level organizations should direct battalion-level and lower units to appoint a TCO if the amount of equipment or volume of use exceeds the planned workload for the single brigade-level additional-duty TCO.

(1) Appendix B provides a sample TCO appointment order.

(2) Based on the usual workload associated with an IMO (usually full-time) position, an IMO should never be assigned as the primary unit TCO. An individual in a different duty position should be appointed as the primary additional-duty TCO.

b. Detailed Responsibilities of TCOs. TCOs in units using Army in Europe networks will—

(1) Provide the Theater TCO, HQ, 2d Sig Bde, a copy of their appointment orders and a signature card.

(2) Register themselves and establish TCO accounts in the Configuration Accounting and Information Retrieval System (CAIRS).

(3) Request the addition, cancellation, and modification of installed telecommunication services (BASECOM and long-haul) as necessary by initiating automated local service requests (LSRs) using CAIRS, the 119/ITSM (Remedy) system, or, if required, by sending other requests or forms by e-mail.

(4) Ensure the servicing dial central office (DCO) has an accurate list of unit-telecommunication services with the correct unit account code and a current list identifying all telephone lines by function.

(5) Process DD Form 448 and DA Form 3953 for BASECOM service requests, as required.

(6) Manage other long-haul services (for example, DRSN, INMARSAT) and dedicated circuits.

(7) Monitor the unclassified military voice networks (including the SBU Voice Network, VoIP systems, and the DSN) to check for abuse and inaccuracies in system-access settings. TCOs will particularly monitor the use of commercial-network access (also known as, 99-access (that is, dialing "99" to access civilian numbers from a Government telecommunications service)) for excess long-distance charges.

(8) Monitor detailed bills for cell phones to check for possible abuse (for example, unusually long calls, unofficial calls, patterns of calls to civilian numbers).

(9) Obtain and issue telephone control numbers (for one-time commercial access) to users through CAIRS and monitor the use of these numbers through CAIRS.

(10) Review usage of official commercial telephone service (glossary) (phone and fax use) using AE Form 25-13C (formerly, AE Form 25-1F).

(11) Report found or suspected abuse, misuse, and overuse to the unit commander.

(12) Ensure telecommunication services such as military voice networks, fixed commercial services, ISDN and analog and digital subscriber line (DSL) services, and all wireless services (for example, cell phones, BlackBerrys, other CMDs) are canceled when a unit deactivates or otherwise leaves the theater.

(13) Validate a unit's continuing need for telecommunications service on a regular and recurring basis. Specifically, TCOs will review, at least annually, their unit's authorizations and requirements to—

(a) Validate a continuing need for official commercial telephone service. When revalidating a continuing need, TCOs will ensure that users of military-voice networks with 99-access do not have a higher level of access than the level needed to accomplish their mission.

(b) Validate the authorization and a continuing need for cell phones, CMDs, and other mobile telecommunication services.

(c) Validate a continuing need for fax machines.

(d) Validate the authorization and a continuing need for Government telecommunications services in quarters (also known as PSS). To do this, TCOs will ensure that—

1. Direct commercial-access (99-access) is not available as part of any PSS authorization.

2. PSS is being used for official business and the current occupant is the person authorized the service.

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

(f) Ensure the servicing DCO has an accurate list of unit telecommunication services and owners at the functional level ((4) above).

8. SINGLE-LINE-OF-SERVICE CONCEPT

The “single-line-of-service concept” is the basic operating concept the Army in Europe uses to provide telephone service. Under this concept, one telephone number, usually SBU, is provided for each customer.

a. Local conditions (for example, insufficient capacity at the local DCO, insufficient cable plant capacity) may require the use of extensions of a single number to support multiple users.

b. Extension of SBU service is limited to one primary telephone instrument with no more than five extensions of that line. In addition, no more than two of the instruments will have ringing capability.

c. Requests for extension of SBU service require approval by the supporting network enterprise center (NEC).

(1) Because of the limited infrastructure, the NEC will validate the requirement for every extension.

(2) NECs will keep validations on file until extension of SBU service is removed and single-line service is reinstalled.

9. THE SENSITIVE BUT UNCLASSIFIED VOICE NETWORK

The SBU Voice network comprises both the DSN service and SBU service. These services have numerous levels of service that can generally be grouped into two categories: basic access (identified in this publication as, SBU or DSN) (that is, service limited to calling within the military-network (a(2)(a) below)) and 99-access (identified primarily in this publication as SBU 99-access, but also includes DSN 99-access and the general term 99-access) (that is, telephone service that enables callers to call outside the military network to civilian numbers (a(2)(b) below)).

a. Classes of Telephone Service in the Army in Europe. In the Army in Europe, official classes of telephone service designations are different from those in CONUS. The digital telephone switches used in the SBU Voice network allow numerous “class marks” to be assigned to each subscriber line. This capability allows telephone service levels to be customized to meet the requirements of individual users and to help control SBU Voice costs.

(1) In CONUS, official telephone services include the Federal Telecommunications System, SBU (including DSN), and commercial telephones with international access.

(2) In the Army in Europe, class marks include

(a) Standard access levels of SBU-Worldwide, SBU-Europe, SBU-Nationwide, or SBU-Local.

(b) Various levels of 99-access. Units may request to add any of the following types of 99-access to any basic-access level service: SBU 99-Access Worldwide, SBU 99-Access Europe, SBU 99-Access Nationwide, or SBU 99-Access Local.

b. SBU Service. The SBU Voice network serves as the primary, official, administrative telephone network in the European theater and the basic SBU service is the default solution. In some cases, SBU calls constitute long-haul usage. In the Army in Europe, the following supplemental guidance applies:

(1) SBU Management. The cost of SBU services is a major portion of the Department of the Army's telecommunications budget and proper management of that service can help reduce costs and improve service (para 14). In particular, the SBU Voice 99-access service will not be used to dial other SBU (military) numbers over the civilian switch.

(2) SBU Account Codes. The SBU Voice network uses account codes to associate SBU telephone numbers with the organization to which they are assigned. The use of SBU account codes allows customers to identify usage. Because "99-access" service is considered an above baseline service, 2d Sig Bde requires reimbursement for SBU 99-access.

(a) The 2d Sig Bde assigns telephone prefix numbers in the SBU system to each organization.

1. Each telephone number within a set of prefix numbers is coded with a work-breakdown structure (WBS) account number or a unit identification code (UIC) to associate the number with the assigned unit.

2. Certain prefix numbers are reserved and will be assigned temporarily to units, as required, for exercises and contingencies.

(b) For more information about or assistance with SBU account codes, users may contact the 2d Sig Bde (NETC-SEC-O-SCC) by e-mail: *usarmy.wiesbaden.5-sig-cmd.list.hq-tco@mail.mil*.

c. DSN. Although DSN is a principal component of the SBU Voice network and remains the primary solution for providing transmission, switching, and support services for STEs, SBU remains the default solution and the solution applicable to most Army in Europe network users.

10. VOICE OVER INTERNET PROTOCOL SERVICE

a. Units may usually connect to the SBU Voice network using only SBU service and only with VoIP systems that have been tested, certified, and appear on the DISA approved products list (APL). VoIP systems must also be fielded in the Joint Interoperability Test Command (JITC)-approved configuration to meet all the service requirements and specifications of the DISA SBU Generic Switching Center. Systems deployed in this manner can provide C2 services. If required for critical C2 requirements, organizations may request to retain traditional SBU Voice network (that is, DSN) connectivity.

b. VoIP systems that use the Army in Europe NIPRNET or SIPRNET must have a valid certificate to operate (CTO). A CTO ensures the equipment complies with overall network-security architecture and appropriate enclave security requirements. A CTO also helps preclude adverse effects on network operations from unverified equipment.

c. USAREUR G6 approval, as the Army in Europe VoIP-system DAA, is required before any unit may use VoIP systems to store, process, or transmit information on the Army in Europe network.

(1) HQ USAREUR staff offices and USAREUR MSCs must request USAREUR G6 DAA approval before they may procure, install, or use such systems.

(2) Although USAREUR OPCON commands, other Army in Europe units, and tenant units may procure such equipment through their administrative headquarters procedures (pre-coordination with USAREUR G6 is recommended), they must also request USAREUR G6 DAA permission to connect VoIP equipment to or use VoIP equipment on any network operated and maintained by 2d Sig Bde.

(3) A VoIP request memorandum must be sent through the servicing NEC to the USAREUR G6 (AEIM-A). The USAREUR G6 will review the request for approval or disapproval.

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

(b) A copy of the “authority to connect” approval memorandum will be provided to the Deputy Chief of Staff, S3, 2d Sig Bde, who will send the engineering change proposal to the SBU Configuration Control Board (CCB), DISA Europe, to authorize, engineer, and integrate the new system into the SBU network. The VoIP system will not be connected to the network until the unit receives an “authority to connect” and approval from the CCB, DISA Europe.

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

11. OFFICIAL COMMERCIAL TELEPHONE SERVICE

Official commercial telephone service is the installation and use of telephone service, DSL service, or both that are provided directly from a HN telecommunications company. The Army considers and budgets for this type of service in the BASECOM category of telecommunication support. The following policy applies to official commercial telephone service:

a. Except for locations not served by SBU, commercial telephone service exceeds the requirements provided by normal telephone service and therefore requires an exception for official use.

b. Routine business will not be conducted over official commercial telephone services.

c. Official commercial telephone service will not be installed—

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

(2) In the quarters of PSS customers.

12. OTHER VOICE NETWORK EQUIPMENT AND SERVICES

a. Call-Forwarding.

(1) Enabling call-forwarding on SBU 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 SBU telephone for a limited time.

(2) Enabling automatic forwarding of SBU 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 other way that transfers personal costs to the U.S. Government.

b. Answering Machines and Voicemail. Telecommunication-system users may use answering machines and voicemail according to the following procedures:

(1) Commercially purchased answering machines may be connected only to non-VoIP phones.

(2) For VoIP phones, voicemail is generally authorized and units may routinely send requests for voicemail service to the supporting NEC as a request-for-change (RFC) action. Because voicemail usually incurs a cost to the unit, the RFC action must be sent by the unit TCO or be routed through the TCO for approval before the NEC will act on the RFC action. The NEC will send unendorsed requests to the unit TCO for review before acting on the request.

(3) All users who have answering machines or voicemail will adhere to the following:

(a) Users will not record information protected by the Privacy Act or sensitive information on answering machines or in recorded voicemail messages.

(b) Users recording messages to say they are unavailable should provide the minimal amount of information needed for callers to contact the intended party.

(c) Users should consider including their cell-phone number, if available, in the unavailable message as an alternative to forwarding a Government line to a cell phone.

c. Secure Telephones. STEs and other secure telephones must display DD Form 2056 with the “DO NOT DISCUSS CLASSIFIED INFORMATION” portion removed or marked out. DD Form 2056 must be attached to the bottom of the front face of the device (for L-3 Communications devices, below the manufacturer logo). This label warns users not to remove the Fortezza Plus Card while the telephone is off the hook or in use, which can cause the card to be erased.

13. REQUESTING TELEPHONE AND TELEPHONE-RELATED SERVICES

a. General–Base-Communications (BASECOM) Services. For acquisition and funding purposes, several telecommunication services that support routine installation operations are grouped together under the general category name BASECOM services. This category includes SBU, SBU 99-access, official commercial telephone service, and other leased services. Mobile services (sec V) and commercial leased-line services are grouped under the Central Base Fund (CBF) services category. BASECOM services are managed in the following three subcategories:

(1) LSRs. LSRs are requests for new service for individuals (not groups or units) or modifications of existing services that are usually managed using the 119/ITSM (Remedy) system without any requirement for a DA Form 3953 as a service request.

(2) Indefinite BASECOM Requirements. Indefinite BASECOM requirements are those of a permanently stationed unit that will continue for the duration of the unit's stationing.

(3) Temporary and Exercise BASECOM Requirements. Temporary and exercise BASECOM requirements are requirements for a rotational unit, an exercise, or other training event.

b. Requesting BASECOM Services. To request any BASECOM service, requesters must send a local service request through the 119/ITSM (Remedy) system (if sent by users, it will be routed thru applicable TCO reviewers) or the CAIRS (sent by the TCO) to a TOO. Table 1 lists Army in Europe (2d Sig Bde) TOOs. The following forms may also be required:

(1) DA Form 3953. If required (for all except LSRs), the purchase request serves as the service request and must be sent to the TOO at the servicing NEC.

(2) DD Form 448. DD Form 448 is required if no funding agreement exists between the unit requesting the service, the USAREUR G8, and 2d Sig Bde.

c. Processing of Indefinite BASECOM Requests. After the unit TCO has validated the unit's indefinite BASECOM requirements, the requesting TCO will send a DA Form 3953 to the appropriate regional 2d Sig Bde TOO.

(1) TOO. The TOO will do the following:

(a) Assign a NEC-unique, request-unique purchase voucher number (PVN) to the DA Form 3953. The PVN ensures correct billing for the service and comprises an 11-digit numeric code in the following format:

1. Digits 1 through 3 represent the NEC.

2. Digits 4 through 7 represent the year and the month (YYMM).

3. Digits 8 through 11 represent the sequential number of the request (for example, 0001).

(b) Keep the original DA Form 3953, which the 2d Sig Bde S8, the contracting office, or the Office of the Inspector General, HQ USAREUR, may need in the future.

(c) Send a digital copy of the DA Form 3953 by e-mail to the 2d Sig Bde (NETC-SEC-RM) (*usarmy.wiesbaden.5-sig-cmd.list.5sc-g8-basecom@mail.mil*) for funding.

(d) If the requesting unit is in a NATO-supported country without an assigned TOO, send a digital copy of the DA Form 3953 to the ODCS, S3, 2d Sig Bde

(e) After receiving a validated and funded DA Form 3953 for telecommunication services back from the 2d Sig Bde S8 ((2) below),—

1. Contract for the services with the HN telecommunications company.

2. As part of the contracting process, track the service requests and process the service delivery or issue with copies of the receipt documents provided to the customers.

(2) Deputy Chief of Staff, S8, 2d Sig Bde. On receipt of DA Form 3953, the 2d Sig Bde S8 will coordinate with the appropriate U.S. Army garrison (USAG) directorate of resource management (DRM) and request validation. On receipt of a validated DA Form 3953 for BASECOM services from a DRM, the 2d Sig Bde S8 will contact the appropriate regional TOO (table 1) and provide a copy of the validated form.

d. Processing Temporary and Exercise BASECOM Requests. After a unit TCO or exercise signal planner has verified the exercise or other temporary BASECOM requirements, the requesting agency or unit will send a DA Form 3953 by fax to the 2d Sig Bde (NETC-SEC-RM) (mil fax: 314-565-0832 or civ fax: 0049-(0)611-143-565-0832) and the form will be processed as follows:

(1) The ODCS, S3, HQ, 2d Sig Bde (NETC-SEC-RM), will—

(a) Provide the ODCS, S8, Headquarters, 2d Sig Bde, with a copy of the DA Form 3953 for the G8 to ensure that funds are available and that billing operations use the correct start and end dates.

(b) Track the status of temporary and exercise BASECOM requirements.

(2) The ODCS, S8, HQ, 2d Sig Bde, will coordinate with the appropriate funding agency to validate the funding. On receipt of funding validation for the BASECOM services, the 2d Sig Bde S8 will notify the ODCS, S3, HQ, 2d Sig Bde (NETC-SEC-RM), and provide copies of appropriate forms.

14. MANAGING AND MONITORING VOICE SERVICES

Unit commanders, leaders, and TCOs are responsible for managing the unit telephone system and monitoring the system for responsible use.

a. Management Tools. Unit TCOs and other leaders and managers have the following valuable resource-management (RM) and asset-management tools available to improve the management of BASECOM and long-haul services units receive and thereby reduce the associated costs:

(1) CAIRS. CAIRS provides visibility over the SBU Voice network and 99-access use for each SBU telephone number that is grouped to that organization. Unit TCOs should review CAIRS reports and provide applicable reports to applicable unit leaders, managers, and the commander.

(2) The Consolidated BASECOM File. This Microsoft Excel file is generated monthly by the ODCS, S8, 2d Sig Bde. This file is a record of SBU 99-access costs and other leased-communication bills paid to commercial vendors. To review charges versus ordering and usage telephone logs for the applicable periods, unit TCOs and RM personnel may request this file or files by sending an e-mail message to *usarmy.wiesbaden.5-sig-cmd.list.hq-tco@mail.mil*.

(3) Telephone Logs. Commercial-service users may be required to keep telephone logs (AE Form 25-13C (formerly AE Form 25-1F)) indicating the time, duration, and purpose of calls, as well as the persons, organizations, and locations called. Units that direct their users to keep telephone logs will encourage more conscientious telephone use.

b. Telephone-Call Control. Telephone-call control is a tool telecommunications managers use to maintain a responsive and cost-effective telephone system while supporting users who are not authorized 99-Access service on their instrument.

(1) Users. When a monitored group line with 99-access is unavailable, users who are not authorized 99-access may obtain a call-control number from the responsible TCO for each call they need to place to a civilian (commercial) number. Users who need to make an official CONUS or international call will contact the applicable TCO and provide the telephone number to be dialed, a precedence, and a justification for the call.

(2) TCOs. TCOs can request call-control numbers through CAIRS (preferred method), individual call-control numbers directly from telephone operators, or a set of call-control numbers from the Dial-Service Assistance head operator on a monthly basis. When issuing call-control numbers, TCOs will—

(a) Verify the official nature of requested calls.

(b) Provide requesters a call-control number for each justified call.

1. A call-control number for a CONUS call is valid for 7 calendar days after the date of issue.

2. A call-control number for an international call is valid until midnight of the day the call was booked with the operator.

(c) Record the required information as a line entry on AE Form 25-13D (formerly AE Form 25-1G). The remarks column will validate the official purpose of the call.

(d) Validate that the control numbers on the AE Form 25-13D were issued for official calls by signing the bottom of the form.

(e) Provide validated copies of AE Form 25-13D (call-control-number logs) to the Dial-Service Assistance attendant.

(3) Operators. Dial-Service Assistance operators will—

(a) Request an updated Authorized TCO list from the Theater TCO, HQ 2d Sig Bde if their TCO list is more than 90 calendar days old. Operators should also reverify their own contact information with the Theater TCO to ensure they receive periodic updates of the authorized TCO list.

(b) Provide call-control numbers to only those individuals who are identified on the Theater TCO's authorized TCO list.

(c) Before completing each call, verify the call-control number by comparing the number to those listed on the TCO-validated AE Form 25-13D.

(d) Log calls to ensure call-control numbers cannot be reused.

c. Other Procedures for Management of 99-Access and Commercial Telephone Service. To help control the cost of official commercial telephone service, the 2d Sig Bde, unit commanders, unit TCOs, and users will manage and monitor the use of military and commercial telephone service.

(1) 2d Sig Bde. 2d Sig Bde will routinely review (at least annually) the use of SBU and SBU 99-access lines at nonappropriated fund (NAF) facilities to improve effectiveness and efficiency.

(a) NAF activities with a large number of incoming calls from the military area will be provided one or more restricted-use SBU lines (that is, lines that will not accept 99-access calls). This will systemically minimize the use of 99-access by individuals who are calling from SBU telephones.

(b) NAF activities are encouraged to contact the local telecommunications company directly for commercial services. 2d Sig Bde will provide SBU 99-access to NAF activities on a reimbursable basis when in the best interest of the U.S. Army.

(2) Unit Commanders and TCOs. Commanders of Army in Europe units, usually through their appointed TCOs, will—

(a) Review the need for SBU 99-access periodically (at least annually) to add or delete lines as necessary and with the intent to reduce the number of subscribers who are authorized SBU Voice (SBU or DSN) 99-access when possible. SBU Voice 99-access is for use only for official purposes and by authorized personnel. Offices with limited, official 99-access requirements will consolidate and share SBU 99-access on a single monitored group line. Commanders will tightly control HN, European, and worldwide commercial access and limit the 99-access to the mission-required access level.

(b) Review CAIRS reports monthly to detect, identify, and discipline telephone abusers. USAG commanders will make tenant unit personnel aware that SBU 99-access (and SBU) telephone usage will be reviewed and abusers may be subject to counseling, requests for reimbursement, or disciplinary actions (for example, warning letters, other punitive actions). Users should not use 99-access lines to call locations that also have SBU lines, except during switch emergencies.

(c) Review the individual needs for official commercial telephone services periodically (at least annually) and—

1. Identify underused official commercial telephone service lines that may no longer be required. To eliminate the possibility of abuse, these owners should be requested to discontinue the service and turn in the telephone.

2. Identify overused official commercial telephone service lines that may indicate unnecessary faxing, large-scale telephone abuse, or extensive use of dial-up modems with personal computers.

3. For monitoring purposes, assign each official-commercial-telephone-service line designated for group use to an individual who is designated in writing.

4. If required, use AE Form 25-13C for each official commercial telephone service line. Any reviews of such official commercial telephone service lines should include reviewing the copies of AE Form 25-13C to identify under use, over use, incorrect billing, or abuse. Reviewers should—

a. Investigate meter units and local bills that do not match the recorded logs. The local telephone-company billing system may sometimes generate incorrect bills.

b. More carefully review records and usage of lines with indications of abuse or identify such indicators to the commander for a possible official investigation (para 15).

c. Consider seeking reimbursement from tenant units who have SBU lines and also lease commercial telephones.

(3) Users. Individual users who are responsible for official commercial telephone service lines will control access to and use of the telephone by authorized personnel for official purposes.

15. TELEPHONE ABUSE

While the ready availability of SBU services and access to commercial networks provide Army activities in Europe with the rapid communications required to accomplish their mission, this availability can lead to abuse. In addition to following the procedures in AR 25-1, AR 25-13, and DA Pamphlet 25-1-1, TCOs at all levels, on behalf of their commanders, will monitor SBU, 99-access, official commercial telephone service, and cell-phone service for abuse.

a. Telephone Abuse. In the Army in Europe—

(1) SBU and commercial calls, including those placed using CMD, 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) Unit TCOs will identify suspected unofficial telephone calls and inform the chain of command, which can conduct an investigation and take appropriate actions. Reports will be maintained locally and be made available on request.

(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.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

b. Types of Calls to Be Researched or Investigated. The following are examples of calls that management officials should research to verify if the call was made for official business and to identify potential telephone abuse that should be investigated:

(1) SBU "99+0" Calls. Officials should review calls made to commercial numbers in Europe outside the local-area dialing prefix to identify numbers that are called regularly, late at night, or both. Some calls for unofficial business or to commercial establishments that have no connection with the military may be justified. Commanders should decide which calls were not authorized.

(2) SBU "99+00" Calls. Officials should review calls made to areas outside the country of assignment that require a specific "class mark" on the telephone to identify numbers that are called regularly, late at night, or both. These types of calls are often made to areas that have SBU service. Usually such calls should be made using SBU "off-netting" or use of a control number, unless the call is a valid emergency, in which case the commander should have first approved.

(a) 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.

(b) 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, users will usually conduct routine business that does not constitute a valid emergency through the mail, e-mail, or over a military-owned system.

(3) Calls Lasting Longer Than 1 Hour. Official business usually takes less than 1 hour to conduct over the telephone.

(4) Calls Costing More Than $25. Calls for official business usually will cost less than $25.

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

(5) Other Calls. Other types of calls that are potentially abuse that should be researched 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 and SMS send-offs to the same number.

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

c. Investigation Procedures.

(1) If telephone abuse is suspected based on the research or review, the reviewer must notify the commander of the unit involved in the possible abuse.

(a) The commander will investigate, identify the abuses and abusers (whenever possible), and initiate action to collect reimbursement from the abusers (d below).

(b) The NEC, TCO, and commercial telephone management personnel at 2d Sig Bde will help commanders identify and collect reimbursements. The NEC and the TCO should help the commander by documenting the abuse, identifying the caller (when possible) and the places called, and determining the cost. They may also assist the commander in processing the reimbursement action.

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

2. If the individual refuses to sign either form required to initiate the reimbursement process (d below), the Army recommend the unit commander initiate a Financial Liability of Property Loss Investigation in accordance with AR 735-5.

(2) For SBU telephones, CAIRS reports show the duration of SBU and commercial (99-access) calls made, as well as the estimated cost of the commercial calls.

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

d. Reimbursement Procedures. Based on the results of the investigation and the individual’s willingness to reimburse the Government, the unit’s RM personnel will prepare either a DD Form 1131 to collect funds in cash (the preferred method) or a DD Form 139 to collect funds by payroll deduction from the individual responsible for the 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 the applicable DD form.

(1) To initiate deductions from the individual’s pay, RM personnel will prepare a DD Form 139 and send the form to the local finance customer support team (FCST) for processing by the 266th Financial Management Support Center (266th FMSC).

(2) To collect reimbursement funds in cash, the following procedures apply:

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

(b) The individual responsible for the telephone abuse must sign the DD Form 1131 and take the form to the local FCST for processing.

(c) The local FCST will prepare a deposit ticket for the responsible individual.

(d) The responsible individual will take the deposit ticket to the community bank, deposit the reimbursement funds in the 266th FMSC account, and return to the local FCST with the resulting deposit voucher.

(e) The local FCST will provide the responsible individual with a copy of the DD Form 1131 with the number of the deposit ticket-voucher annotated on the form.

(f) The local FCST will scan the DD Form 1131 and send a digital copy to the 266th FMSC for processing.

SECTION IV
NETWORK SERVICES IN GOVERNMENT QUARTERS

16. PREFERRED SUBSCRIBER SERVICE

a. Positions Authorized PSS. Individuals serving in the unit positions listed in table 4 and the HQ USAREUR positions listed in table 5 are authorized to request and receive PSS (official telephone service in quarters).

Table 4
Army in Europe Unit Positions Authorized Preferred Subscriber Service

Position	USAREUR MSCs and OPCON Commands	Division HQ (and their equivalents)	Bdes, Bde-equivalents, Specified Commands	USAGs	Tactical Bns (MTOE units)
Commander	X	X	X	X	X
Deputy Commander	X	X			
Chief of Staff	X	X		X	
Command Sergeant Major	X	X			
Deputy Chief of Staff, Operations (G3/S3);	X	X	X	X	
Support Operations Officer	X	X	X	X	
General Officers	X	X	X	X	
Distinguished-visitor guestroom occupants				X	

b. PSS Restrictions. PSS is subject to the following restrictions:

(1) PSS is considered an above-baseline service and the user’s organization is responsible for the associated costs. If the quarters do not already have a military (SBU Voice) telephone line, a line may be leased, which is an additional unit-funded cost.

(2) Under no circumstances will PSS include direct-commercial access (that is, SBU 99-access).

c. Exceptions to Policy. Organizations may send requests for exception to policy (that is, the authorized-positions policy) to the USAREUR G6 (AEIM-A) for approval.

(1) Exceptions should be requested only for the mission-required duration. Permanent exceptions should be requested as a recommended change to this publication.

(2) An example of a valid exception would be a rear detachment commander who must coordinate casualty or health, morale, and welfare issues while the unit is deployed to a war zone. This PSS line would usually end shortly (usually no longer than 30 days) after the unit returns to home station or the end of any block-leave period.

Table 5
HQ USAREUR Positions Authorized Preferred Subscriber Service

Positions
CG, USAREUR
CG Executive Officer
CG Aide-de-Camp
DCG, USAREUR
DCG-ARNG, USAREUR
DCG-M&RA, USAREUR (dual-hatted: Dir, AREC, Office of the CoS, HQ USAREUR)
Chief of Staff, HQ USAREUR
Deputy Chief of Staff, HQ USAREUR
Command Sergeant Major, USAREUR
Secretary of the General Staff, HQ USAREUR
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, G3/5/7
Assistant Deputy Chief of Staff, G3/5/7
Chief, G3/3 Operations Division, ODCS, G3/5/7
Deputy Chief of Staff, G4
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 Office
Command Surgeon
Deputy Command Surgeon
Inspector General
Judge Advocate
Provost Marshal
Deputy Provost Marshal
Any other HQ USAREUR GO position

17. INTERNET SERVICE PROVIDER AND DIGITAL SUBSCRIBER LINE SERVICE IN QUARTERS

DOD agencies are generally prohibited from paying with appropriated funds for commercial ISP and DSL services in Government quarters (known as ISP-in-Quarters service).

a. Exception and Approval Authority for ISP-in-Quarters Service. HQDA has coordinated for and issued a limited exception to policy for Army commanders at division level or higher who are special C2 users as defined by Chairman of the Joint Chiefs of Staff Instruction 6211.02D. For authorization according to this exception, the Office of the Judge Advocate, HQ USAREUR, must review each ISP-in-Quarters request before it will be considered for approval by the USAREUR approval authority (that is, the CoS, HQ USAREUR).

b. Request for ISP-in-Quarters Service. To request ISP-in-Quarters service—

(1) Requesters from within HQ USAREUR staff offices will prepare a request memorandum for signature by the staff principal.

(2) Units will prepare a request memorandum for signature by the commander or chief of staff (for GO or civilian-equivalent commands) of the applicable USAREUR MSC, USAREUR OPCON command, IMCOM-Europe, or USAG. If the request is for someone assigned to any IMCOM-Europe element, c(1) below also applies.

(3) Requesters will prepare the memorandum to provide all of the following information:

(a) Name of the individual for whom ISP-in-Quarters service is requested.

(b) Individual's duty position.

(c) Individual's rank or grade.

(d) The individual's primary duty location (room number, building number, and installation name).

(e) The primary network and e-mail server the individual will access through the ISP service.

(f) The type (for example, analog, DSL) and telephone number of dial-in telephone service currently installed to the server.

(g) The name and telephone number of the system administrator responsible for the server.

(h) The location of both the individual's quarters and of the requested ISP or DSL connection in those quarters.

(i) A list of data services that the individual is currently using or will need in the quarters (request must include the current and projected average daily use for each type of service listed).

(j) The type of telecommunication service currently being used by the individual to access data services in quarters.

(k) The typical, maximum data-transmission rates or bandwidth provided by the telecommunication services being used by the requester.

(l) A justification for the request. The justification must explain why existing telecommunication services in the quarters do not adequately support the individual's requirements for data services.

(m) The type of computer and operating system that will be connected to the ISP in the individual's quarters.

c. Processing Requests. The requesting organization will send the signed request—

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

NOTE: For requests for personnel assigned to any IMCOM-Europe organization (that is, all USAGs in Europe or the IMCOM-Europe headquarters), the requester will send the request through the IMCOM-Europe headquarters for line-thru recommendation for approval by the appropriate official (that is, at least the CoS, HQ IMCOM-Europe) before sending through the USAREUR G6 ((1) above).

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

(3) To the CoS, HQ USAREUR, Unit 29351, APO AE 09014-9351, for review and approval or disapproval and then return routing to the requesting organization (CF: to the USAREUR G6) for coordinating implementation or notification of disapproval.

d. Restrictions to Approved Requests. All ISP-in-Quarters service requests approved by the CoS, HQ USAREUR, will be subject to the following conditions:

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

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

(3) Commercial ISP service may be used to send e-mail and other data through Army hosts, but only when the e-mail or data is for official business and directly related to the C2 of military Forces.

(4) Commercial ISP service will not be used for routine voice communications, VTC, or mere convenience.

(5) Monthly billing statements will list the types of connections and include a record of each call (for example, time, number called, duration, resulting cost). IT managers, resource managers, and leaders will use these billing statements to review the ISP-in-Quarters service for compliance with published policy and standards (e below).

e. Monitoring of ISP-in-Quarters Service.

(1) IT and telecommunications managers and unit leaders will routinely review billing statements for policy compliance and potential abuse as the funding organization deems appropriate (that is, frequency and level of detail of the review).

(2) The RM offices of ISP-in-Quarters service users will—

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

(b) Certify monthly billing statements after reviewing them.

(c) Keep monthly billing statements on file for annual revalidations and as a record copy for at least 2 fiscal years.

(d) Notify the USAREUR G6 (AEIM-A) immediately after finding any evidence of potential abuse of an ISP connection.

(3) If notified of potential abuse, the USAREUR G6 will coordinate with the Office of the Judge Advocate, HQ USAREUR, to determine whether or not the evidence indicates that abuse has actually occurred and if any action (to include an official investigation, if necessary) is required.

SECTION V
MOBILE SERVICES

18. CELL PHONES

A cell phone is defined as an active subscriber identity module (SIM) chip in combination with either a handset or other CMD equipment that has only basic Global System Mobile (GSM) capability to send and receive voice and text messages. Basic GSM capability does not include data capability. Because of the high cost of using cell phones, management control over active Government SIM chips is required.

a. Approval Authorities.

(1) The USAREUR G3/5/7 is the authorization approver for HQ USAREUR staff offices and USAREUR MSCs. USAREUR-approved cell-phone authorizations are listed on the USAREUR CMD Authorization Document. Paragraph 19e(1) provides the procedures for requesting modifications to unit authorizations (waiver requests) that are applicable to all types of CMDs.

(2) Commanders or directors of other Army in Europe organizations and units (for example, IMCOM-Europe, the Civilian Human Resources Agency, Northeast/Europe Region (CHRA-NE/EU)), USAREUR OPCON commands, the United States Army North Atlantic Treaty Organization (USANATO) Brigade, the Multinational Battle Group East (MNBG-E), or other DOD tenant organizations may be the approving authority for their organizations according to their administrative higher headquarters policy.

b. Responsibilities.

(1) HQ USAREUR Staff Offices and USAREUR MSCs. Each HQ USAREUR staff office and USAREUR MSC that is authorized to approve requests for new (replacement) cell phones for existing approved authorizations and issues of existing cell phones to new users will do the following:

(a) Manage and ensure proper use of cell phones issued under this authority. Specifically, issuing authorities—

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

2. Must manage the use of cell phones in their staff offices or units and ensure payment is made for all associated costs.

3. Will not authorize the use of prepaid cell-phone service, as usage cannot be tracked or verified. Exceptions must be requested through the USAREUR G6.

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

1. For convenience.

2. Instead of fixed telecommunication systems.

3. Instead of a tactical communication system in a field environment.

4. To back-up other cell phones.

5. To send classified or sensitive information.

(2) Other Units. USAREUR OPCON commands, other Army in Europe units, and other Army in Europe tenant units should usually apply the same standards as in (1) above to their cell-phone operations, but should consult with their ADCON higher headquarters for its specific cell-phone-usage guidance, which could be more restrictive or, by exception, less restrictive.

(3) Army in Europe Unit TCOs. The unit TCO (or, as applicable, his or her directed representatives or augmentees) or the issuing authority (when no TCO is appointed) will—

(a) Conduct periodic (at least annual) validations of cell-phone service.

(b) Maintain a unit cell-phone database with the data listed in table 6.

Table 6
Army in Europe Government-Issued Cell-Phone Unit Database Requirements

Data
Name of the user assigned the cell phone
Name of the office the individual is assigned
SBU telephone number of the user
Cell-phone SIM chip serial number
Cell-phone handset model, serial number, IMEI number, and cell-phone telephone number
Level of service (contract CLIN)
Date service started/terminated

(c) Train cell-phone users on the proper use of cell phones. Particular attention must be paid to discussing the consequences of roaming charges, texting, use of device in vehicles, use of toll and operator-assisted services.

(d) Require cell-phone users to sign an Army in Europe Mobile Device User Agreement (AE Form 25-13A (formerly, AE Form 25-1M), acknowledging that they have read and understand the rules on the proper use of cell phones.

(e) Notify the issuing authority concerning extremely high-volume cell-phone users or if improper use is suspected.

(f) Routinely review cell-phone use. This review will also be used to revalidate cell phones ((a) above) and may include the following:

1. Number of unit cell phones.

2. Frequency of use for each cell phone.

3. Destination types (to international or national numbers, numbers serviced by other cell-phone providers) of calls placed and text messages sent.

4. Average monthly use costs.

5. Documented cases of improper use of cell phones and reimbursement obtained.

(4) Cell-Phone Users. Personnel who are issued an Army-in-Europe cell phone will sign an Army in Europe Mobile Device User Agreement (AE Form 25-13A (formerly, AE Form 25-1M)) acknowledging that they have read and understand the rules on the proper use of cell phones and comply with those agreement procedures. Users may be held financially responsible for abuse (para 15).

c. Procedures for Requesting Cell Phones.

(1) HQ USAREUR staff offices and USAREUR MSCs will refer to the USAREUR CMD Authorization Document maintained by the USAREUR G6 to determine their cell phone or other CMD authorizations.

(2) USAREUR OPCON commands and other Army in Europe tenant units will request cell-phone authorizations through their applicable ADCON higher headquarters G6 or CoS.

d. Procurement.

(1) Procurement Options. Units that need cell phones for contingency-support missions will send a request according to the specific needs of the mission. Issuing authorities are authorized to approve cell phones using one of two procurement methods for activation and payment of services. If a request cannot be met under the first method ((a) below), which is preferred, the issuer may use the second method ((b) below).

(a) Method 1–Procuring Service Through the 2d Sig Bde Blanket Purchase Agreement (BPA) with the General Services Administration (GSA). International cell-phone services are available under the 2d Sig Bde BPA contract with GSA, which offers worldwide service coverage, according to the following steps:

1. Unit Request. After approval by the issuing authority, the TCO sends a DA Form 3953 (as a service (purchase) request) to the applicable 2d Sig Bde TOO (table 3).

2. Unit Funding. In coordination with the unit TCO and 2d Sig Bde (4b below), the unit RM sends a DD Form 448 to the 2d Sig Bde (NETC-SEC-RM) to provide funds.

3. TOO Processing. The TOO assigns a PVN to each service request and sends the request to the 2d Sig Bde (NETC-SEC-RM) for funding certification. After receipt of an approved DA Form 3953 from the 2d Sig Bde (4c below), the TOO executes the order and notifies the customer.

4. 2d Sig Bde Processing. The 2d Sig Bde will—

a. After receiving the DA Form 3953, assign a corresponding customer or WBS account number, which the unit TCO must annotate on all future orders to be paid from that account, and provide the TCO with that number.

b. Inform the unit POC (budget analyst noted on the DA Form 3953) of the amount of funds required and will not process the request further until it receives a valid DD Form 448.

c. After receiving the DD Form 448 that provides funds, process the service request for approval and return the approved DA Form 3953 to the TOO.

d. Receive monthly itemized billing reports at the ODCS, S8, HQ 2d Sig Bde, and review, distribute, or review and distribute the reports as required.

(b) Method 2: Procuring service through a local vendor. Requesters, issuers, and users will—

1. Ensure cell-phone activation is performed according to the service agreement with the commercial service provider. The requesting organization is responsible for managing the contract.

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

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

(2) Procurement Standards for European Cell-Phone Networks. Approving authorities should approve acquisition of cell phones that use one of the following standards as appropriate for the mission requirements:

(a) GSM Band Standards.

1. The GSM (dual band) standard (900 and 1,800 megahertz (MHz) usually permits cell phones to be used almost anywhere in Europe.

2. Some U.S. digital cell phones also use a GSM (dual-band) standard, but operate on different frequencies (900 and 1,900 MHz) and are usually not recommended for use in Europe.

3. Tri-band (900, 1,800, and 1,900 MHz) handsets are usually required for cell phones that need to interface with all the GSM-based systems used in the United States and Europe.

4. Quad-band handsets also function in the GSM band at 950 MHz, which is used in South America and Asia.

(b) The 3G Standard. The Universal Mobile Telecommunications System (UMTS) (more commonly known as the 3G or third-generation GSM standard*) is the standard that has been implemented in most European countries. Most newer GSM cell phones are UMTS-capable. This additional capability may be used for higher-speed data connections when possible or appropriate.

***NOTE:** Two additional 3G standards exist (referred to as General Packet Radio Service (GPRS) standard and the Enhanced Data Rates for Global System Mobile Evolution (EDGE) standard) that UMTS-capable cell phones can also use in locations where 3G service is limited, but they are substantially slower than true 3G service.

(c) Long-Term Evolution (LTE) Standard. The LTE (also known as the 4G) standard is the newest standard and offers data connections of up to 300Mb downlink and 75Mb uplink.

e. 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), cell phones will not be used—

(1) On post or at other locations where other less costly means of communication exist (for example, SBU, DSN, official commercial telephone service). Cell phones should not be used if normal fixed telephone devices are available, unless the call is among cell phones that are all on the 2d Sig Bde cell-phone contract. Personnel will always use the least expensive means of communication.

(2) For personal use.

(3) For routine health, morale, and welfare calls.

(4) In medical treatment facilities or other areas with sensitive equipment. In areas where cell-phone use may disrupt medical or other equipment, Army in Europe organizations will post signs to indicate the start of the areas where cell phones must be turned off and not used.

(5) During meetings, in open storage facilities, or in areas where sensitive or classified information is being discussed.

NOTE: Even when a cell phone is turned off, a person with malicious intent can 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 unless the user attempts to place a call.

(6) To subscribe to download services such as ring tones, apps, wall papers, film clips, and news services.

(7) With Bluetooth technology, except when used with approved devices. Bluetooth technology is authorized for use with approved headsets and Smart-Card readers as well as vehicle manufacturer-installed hands-free devices ((8) below).

(8) While operating privately owned vehicles or Government-owned vehicles unless the vehicle is safely parked and the engine turned off (preferred), or the cell phone is used with a hands-free device (less preferred and only while the driving situation permits safe use). Emergency responders (for example, ambulances, explosive ordnance disposal teams, fire emergency services, hazardous material responders, military police) are the only personnel exempt from this prohibition.

f. Special Cell Phone Procedures.

(1) 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 should, however, share cell phones within their units for efficiency and cost reduction.

(2) Lost and stolen cell phones must be reported immediately to unit TCOs, the TOO, the 2d Sig Bde Theater TCO, or the service provider (whichever is first available) to deactivate the SIM chip. This measure will help ensure that the Government is not charged for unauthorized use.

(3) TCOs will issue only SIM chips that include active PIN-verification. PIN-verification will not be deactivated by users. Users should memorize their PIN. If someone tries to activate the cell phone with the wrong PIN, the SIM chip will lock after 3 unsuccessful tries. To obtain the PIN-unblock key, users must provide the TCO with the SIM chip serial number or telephone number.

g. Exceptions to Policy.

(1) HQ USAREUR Staff Offices and USAREUR MSCs. When exceptions to cell-phone policy are needed, the organization will send a memorandum to the USAREUR G6 (AEIM-A) to request the exception. The justification in the memorandum should include the five Ws (who, what, when, where, and why) and funding information.

(2) USAREUR OPCON Commands and Other Army in Europe Tenant Organizations. These organizations will send exception-to-policy-request memorandums for cell phones through the G6 of their applicable administrative higher headquarters.

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

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

h. Cell Phones for Contingency-Support Missions. Contingency operations are often a rapidly changing situation or environment and may require that deploying units or personnel have cell-phone voice-communication capability for C2 on short notice.

(1) When planning for cell-phone use in contingency operations, requesters must first determine whether or not a cell-phone infrastructure exists in the deployed area. If an appropriate infrastructure exists, the requester may contact the Crisis Action Team, Current Operations Branch (CUOPS), G3/3 Operations Division (G3/3/ OPS), ODCS, G3/5/7, HQ USAREUR, to request cell-phone services.

(2) The Crisis Action Team will validate and approve or disapprove the request for cell phones for the particular contingency operation.

(3) Units deploying to operational areas with approved requirements will usually procure cell-phone service from local cell-phone providers through deployed DOD contracting agents or organizations, if available.

(4) Request memorandums for cell phones for contingency-operation missions must identify all of the following:

(a) Why other communication systems cannot meet the contingency-operation requirement.

(b) The estimated period of time the cell phone is needed (start and end dates).

(c) The name of the user or unit to which the cell phone will be assigned.

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

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

i. Cell Phones for Exercise Support.

(1) Requests for cell-phone service for use in exercises directed by the Joint Chiefs of Staff will be sent to the USAREUR G3/5/7 (AEOP-OMT), Unit 29351, APO AE 09014-9351.

(2) The USAREUR G3/5/7 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. Army in Europe exercise requirements must be for 89 days or less. Requests for extensions must be sent to the USAREUR G3/5/7 (AEOP-OMT) at least 30 days before the authorization period ends.

(3) The Crisis Action Team, CUOPS, G3/3 OPS, ODCS, G3/5/7, HQ USAREUR, currently controls the initial receipt, temporary issue, return, re-issue, and turn-in of exercise cell phones used by HQ USAREUR staff offices as well as cell phones for contingency operations. Other Army in Europe commands will identify their agency that will control the initial receipt, temporary issue, return, re-issue, and turn-in of exercise cell phones used by their subordinate units to the USAREUR G3/5/7 (either as a fixed POC office (if routinely required) or per request at the time when service is requested).

(4) In accordance with AR 25-13 requirements and other Army property-accountability and financial-management policy, the USAREUR G3/5/7 and TCOs or other designated agents at other Army in Europe headquarters (USAREUR MSCs, USAREUR OPCON commands, IMCOM-Europe and its USAGs, and CHRA-NE/EU) will—

(a) Procure exercise cell phones using contracts.

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

(c) Maintain the following information about 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.

(d) Ensure cell-phone service contracts are terminated at the end of the exercise and that all cell-phone equipment is accounted for or returned to the service provider.

(5) Requesters and users of exercise cell phones will—

(a) Temporarily hand-receipt for the cell phone and turn-in the cell phone to the controlling office after the exercise.

(b) Not use the cell phone to send sensitive or classified data.

(c) Not use the cell phone when tactical or other communication systems are available.

(d) Not receive, issue, or subissue the cell phone for purposes other than the exercise. Exercise cell phones will not be used merely to supplement permanently assigned cell phones.

(6) Approved exercise cell phones will not be converted to permanent cell phones.

j. Tactical Cell Phones.

(1) For routine tactical cell-phone requirements, requesters will complete DA Form 2028 and a DA Form 4610-R, and send these forms for approval through the Vertical–The Army Authorization Documents System.

(a) Approved requirements for tactical cell phones will be identified in the equipment section of a unit’s MTOE or table of distribution and allowances (TDA).

(b) Whether authorized on the MTOE or TDA or not, on-hand tactical cell phones must be accounted for through standard Army property-accountability procedures according to AR 710-1.

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

(3) Urgent requirements for commercial cell phones to be used in place of authorized, but not on-hand tactical communication equipment must be approved through the operational-needs statement process according to AR 71-9.

19. OTHER COMMERCIAL MOBILE DEVICES

CMDs include cell phones; BlackBerrys; iPhones and Android or Windows smart phones; and iPads and Android or Windows tablets that are approved for DOD use (that is, listed on the DOD Unified Capabilities (UC) APL) and available through the 2d Sig Bde wireless contract or from the Computer Hardware, Enterprise Software, and Solutions (CHESS) website. Other CMDs (those other than basic cell phones (para 18)) can also provide remote (NIPRNET) e-mail access, Internet access, or both to support official business. Because these other CMDs are easy to use and tightly integrated with existing infrastructure, select personnel are authorized to use these Government CMDs to allow encrypted and continuous access to e-mail and continuous access to other required Internet-based services.

a. Requirements for Government Use of CMDs.

(1) All CMD hardware must meet the same technical requirements as identified for cell phones in paragraph 18d(2).

(2) The network infrastructure required to support CMD technology is implemented and maintained by DISA.

(3) Each organization must pay for acquisition of its own devices and costs of services received.

(4) Smart-phone systems used in the Army in Europe must—

(a) Meet Federal Information Processing Standard (FIPS) certification requirements. FIPS certification protects unclassified Government information when the data leaves networks owned and controlled by the DOD.

(b) Use secure/multipurpose Internet mail extension (S/MIME) software to be public key infrastructure (PKI)-compliant. S/MIME-enhanced smart-phone systems are subject to DOD, DA, and Army in Europe policy governing the security and use of unclassified information systems.

b. Approval Authorities. Personnel authorized to approve the acquisition of CMDs must consider the overall long-term cost to their organizations before approving the acquisition. Smart-phone devices should be acquired only for personnel who require a “24/7” mobile enterprise e-mail capability as a mission-critical tool.

(1) The USAREUR G3/5/7 is the approving authority for HQ USAREUR staff offices and USAREUR MSCs to acquire and use CMDs. Current USAREUR-approved authorizations are listed on the USAREUR CMD Authorization Document.

(2) Commanders or directors of USAREUR OPCON commands, the USANATO Brigade, and the MNBG-E, are the approving authority for CMDs for their organizations, but will coordinate their authorization list with or routinely (at least annually) provide a copy of the list to the USAREUR G6.

(3) Other Army in Europe organizations (for example, IMCOM-Europe, CHRA-NE/EU) and DOD or non-DOD organizations that use the Army in Europe networks will request approval for CMDs through their ADCON higher headquarters or according to that ADCON higher headquarters’ delegated authorities.

c. Responsibilities for Using CMDs.

(1) The USAREUR G6. The USAREUR G6 is responsible for policy on and oversight of the Army in Europe CMD 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 CMD Security Checklist.

(2) The 2d Sig Bde. The 2d Sig Bde will—

(a) Be the interface to provision, delete, and manage devices and user accounts on the DISA 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 CMDs before they are approved for use.

(d) Maintain copies of all required licenses and documentation for the operation of CMD Enterprise services, which includes copies of the server-router-protocol 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 CMD Security Checklist.

(3) Units. Units will—

(a) Purchase, upgrade, license, install, configure, and provide basic troubleshooting for all assigned CMDs. Unit-level IMOs are usually the first line of support for all CMD users within their organization

(b) Pay the BlackBerry regulated service fee for each device. All units supported on the DISA BES (regardless of their unit affiliation) are required to pay this fee for applicable devices.

(c) Establish a program designator code for Android and iPhone devices (not required for BlackBerry) and assign authorized requesting officials (AROs) and authorized funding officials (AFOs) for the DISA Direct Order Entry portal to register all Wi-Fi media access control (MAC) addresses obtained for order entry.

(d) Designate an appropriate number of IT personnel to support CMDs within their organization.

(e) Pay all recurring and nonrecurring costs associated with the purchase of CMDs, use of CMDs, and training for CMD-support personnel.

(f) Perform a security “wipe” on all new or reissued CMDs. After a wipe, the IT-support personnel will load the latest DISA-authorized handheld software and desktop software on the CMD.

(4) CMD Users. Personnel who are issued a CMD will sign an Army in Europe Mobile Device User Agreement (AE Form 25-13A (formerly, AE Form 25-1M)) acknowledging that they have read and understand the rules on the proper use of CMDs and comply with the agreement procedures. Users may be held financially responsible for abuse (para 15).

d. Special CMD Control Procedures. In addition to general network security regulations and policy, the following special control procedures govern the general Government use of CMDs, use of CMDs in the European theater, or both:

(1) CMDs will not be used to process classified information (that is, Confidential and higher). There are no sanitation products that are DOD-approved for use with CMDs. If a CMD is accidently used to process classified information, the device must be treated as a classified item until the CMD is destroyed according to applicable Army regulations.

(a) According to Director of Central Intelligence Directive 6/3 (DCID 6/3) and DCID 6/9, CMDs are not permitted in sensitive compartmented information facilities (SCIFs).

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

(2) CMDs will not be configured to work with or be connected to any device.

(3) 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.

(3) CMDs will use a PIN for the SIM (for example, SIM chip), a password for the device (for example, device password, hand-held password), and a password for the certificate store (for example, key-store password).

(a) Device passwords will be configured with a timeout of 15 minutes, a password history of five, and a maximum of three password attempts. On the third failed attempt, all data on the device will be wiped automatically.

(b) Within the limitations of the device, device passwords must be five alphanumeric characters with at least one alpha and one numeric character.

(c) Device passwords will be changed every 90 days.

(4) When using the voice and telephony capabilities of CMDs, the cell-phone guidance in paragraph 18 (specifically subparas 18b and d) applies to these other CMDs.

(5) All CMDs will be configured on the DISA-managed BES and Department of Defense Mobility Unclassified Capability (DMUC) servers. The USAREUR G6 may also implement additional policy requirements as needed. This additional configuration policy is available from the USAREUR G6 (AEIM-I/mil 537-6223).

(6) If a CMD device is lost or stolen, the owner or organization must report the loss immediately to the Enterprise Service Desk (ESD), 2d Sig Bde. The ESD technician who receives the notice will immediately issue a "kill" command for the device, which will wipe all data on the CMD.

(7) To maintain the efficiency of the Army in Europe CMD infrastructure, the 2d Sig Bde (that is, the ESD) will remove dead accounts from the BES and DMUC immediately. Inactive accounts will also be removed from the BES and DMUC after 30 days of inactivity.

(8) When conducting a wireless activation of a CMD, ESD technicians will ensure that—

(a) CMD users may not activate their CMD device themselves, unless they do so under the direction of an ESD technician.

(b) Only an authorized CMD system administrator performs a wireless (emergency) device-reactivation and only when based on critical mission requirements (for example, if a CMD device of a GO on temporary duty becomes corrupted and requires reactivation).

(c) The activation password is given to the user only by a secure means (for example, encrypted e-mail sent to a trusted individual traveling with the GO).

(9) Any time a user or IT-support personnel suspect a CMD may be compromised, they will immediately notify the USAREUR G2 for further guidance.

(a) All personnel traveling to restricted areas (as determined by the USAREUR G2) will follow USAREUR G2 benchmarking procedures before leaving for the area and again after returning from the area.

(b) Users and IT-support personnel will report to the USAREUR G2 any system changes that are identified by comparison of the before-travel and after-travel benchmarks.

e. Authorization, Procurement, and Distribution of CMDs. CMDs may be provided to personnel based on their assigned duty positions (HQ USAREUR and USAREUR MSC personnel may be provided CMDs if their position is listed in the USAREUR Commercial Mobile Device (CMD) Authorization Document (available at *https://intranet.eur.army.mil/hq/portfoliomgnt* under the "Law & Policy" and "USAREUR" headings)).

(1) Authorization Changes. Requests to modify unit authorizations (waiver requests) must be sent through the Programs, Policy, and Projects Office, ODCS, G6, HQ USAREUR, to the USAREUR G3/5/7.

(a) Units must prepare waiver-request memorandums in the format provided in the USAREUR CMD Authorization Document.

(b) Valid justifications for requesting an increase to CMD authorization levels include a change to a unit's or staff office's MTOE or TDA or a change to a unit's mission requirements.

(c) An approved waiver request will result in modification of the CMD authorization levels to include the new requirement for the HQ USAREUR staff office or USAREUR MSC in the USAREUR CMD Authorization Document.

(2) Procurement, Operation Costs, and Disposal. CMDs will be purchased with the necessary and appropriate level of service from the 2d Sig Bde wireless contract at the requesting unit’s expense. No other contract source is authorized without USAREUR G6 approval of the exception.

(a) Units are responsible for all costs for the device. This includes the cost of hardware, licenses, monthly charges, hosting fees, and usage.

(b) Units must be prepared to purchase new equipment (conduct life-cycle replacement (LCR)) when the current device or CAC reader does not meet current messaging or security requirements.

1. In some cases, the life cycle of a CMD may be shorter than the actual device warranty (which is usually 2 years). Units must be able to defray the cost of upgrading to new equipment in the event a security issue causes a determination that the current model requires LCR earlier than the expected life-cycle date.

2. Life-cycled equipment may not be recycled to other members in the organization.

(c) Once a CMD is replaced through the LCR process or otherwise deemed no longer supported, the owner will request IT support to wipe the old CMD and provide applicable certifying paperwork. The owner will then dispose of the CMD using standard logistic turn-in procedures.

(3) Smart Cards. CMDs configured for e-mail must use an approved smart-card reader to allow for the use of CAC certificates for PKI-enabled e-mail. CMDs are an extension of the Army in Europe official messaging system; consequently DOD and Army policy on use of digital signatures for all official message traffic applies equally to CMD-transmitted e-mail.

(4) Accountability. CMDs must be maintained on unit property books, will be hand-receipted to users, and will remain with the unit (be returned to the hand-receipt holder) when a user leaves the unit.

f. Special Service Restrictions. Although authorized CMD users in the Army in Europe are automatically given the capability to view e-mail attachments and browse the Internet when a device is issued and activated, Internet restrictions that apply to desktop and laptop computer systems also apply to CMDs (for example, blocked websites). Because of security concerns, Government-issued CMDs are currently not authorized to use the following features usually found on a civilian CMD:

(1) Global Positioning System and maps.

(2) Tethered modems.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

SECTION VI
VIDEO-TELECONFERENCE SERVICES

20. VIDEO-TELECONFERENCE EQUIPMENT AND STANDARDS

Army in Europe VTC systems must be interoperable with other theater systems. The below requirements and procedures for establishing and operating VTC systems in the Army in Europe define the acceptable methods, standards, and requirements for using VTC systems on the Army in Europe network in ways that will ensure interoperability.

a. General.

(1) All multipoint VTCs in the Army in Europe require connectivity (b(1) thru (4) below) through a USAREUR VTC hub (para 5b(7)).

(2) All multipoint VTCs in the Army in Europe that connect with CONUS sites require connectivity through a USAREUR VTC hub and then through DISA to the CONUS VTC point.

(3) Once registered, VTC facilitators can schedule VTC sessions by sending an e-mail message to *usarmy.wiesbaden.usareur.mbx.vtc-schedulers@mail.mil*.

(4) VTC equipment will be procured through the IT technical-validation process (AR 25-13).

(5) The Plans and Engineering Division, ODCS, S3, Headquarters, 2d Sig Bde, provides theater-level engineering support, including VTC-systems engineering, to the Army in Europe.

b. VTC Standards and Protocols. To ensure interoperability, Army in Europe organizations and tenant activities will procure and operate only VTC systems that comply with USAREUR-standards ((1) thru (4) below). Questions on VTC equipment standards and compatibility requirements should be directed to the USAREUR G6 VTC Program Manager (mil 314-537-6263).

(1) All Army in Europe VTC systems must be properly accredited by the USAREUR G6 Information Assurance Program Manager (IAPM) and registered to the Wiesbaden USAREUR VTC Hub before they will be allowed to operate on the Army in Europe (*.eur* domain) network.

(2) All VTC coder/decoders (CODECs) must be registered with the USAREUR VTC Program Manager (mil 314-537-6263) before use. To register a CODEC, units must have a memorandum signed by the unit’s designated approval authority (electronic signatures are acceptable).

(3) All VTC systems will connect by IP address.

(4) H.323 is the DOD standard for VTC and data collaboration over IP data networks.

(a) Because IP networks do not necessarily guarantee high-quality service, the H.323 standard usually works well only on networks with high bandwidths and light traffic loads.

(b) Connections using H.321 or ISDN standards will not be allowed or connected through USAREUR VTC hubs unless the unit has an approved waiver from the DAA.

(c) The H.323 standard is usually associated with personal computer-based desktop VTCs. Large CODEC units may, however, also connect by IP if the system has been accredited through the USAREUR G6 IAPM.

(5) 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 the 2d Sig Bde (NETC-SEC-O/mil 314-565-0614/0221).

(6) All VTC equipment to be purchased must be listed on the DISA (USAREUR) APL (in the USAREUR IT Portfolio-Management SharePoint Library at *https://intranet.eur.army.mil/hq/portfoliomgnt*)).

(7) The CHESS website (*https://chess.army.mil*) is the primary source for establishing commercial IT procurement contracts for hardware, software, and services.

c. Procurement Process.

(1) The USAREUR G6 determines annual VTC-equipment LCR allocations for USAREUR units (HQ USAREUR staff offices and USAREUR MSCs) based on the USAREUR G3/5/7-approved USAREUR Automation Table of Equipment (AE Supp 1 to AR 25-1, para 2-32c). The USAREUR G6 will generate acquisition packets and send them to the CoS, HQ USAREUR, for approval.

(a) In cases where the 409th Support Brigade (Contracting), United States Army Expeditionary Contracting Command (ECC), guidance is more stringent than USAREUR procedures ((b) below), the USAREUR G6 will use ECC procedures when submitting those acquisition packets.

(b) USAREUR acquisition packets will include the following items:

1. An AE Form 1-10A (that is, a staff action summary) from the requesting agency that is endorsed by the USAREUR G8 to validate the funding availability.

2. An IT technical validation approved by the NEC.

3. An independent Government-cost estimate and supporting cost data.

4. A performance work statement if services include hardware purchase.

(2) USAREUR OPCON commands, Army in Europe tenant organizations, and other DOD or non-DOD organizations or units that use Army in Europe networks will follow the procurement-process policy, procedures, and guidance as dictated by their applicable administrative higher headquarters (that is, the applicable Army command, Army service component command, Army direct reporting unit, or DOD headquarters). However, any procured equipment must still meet the required USAREUR technical standards to connect through the Army in Europe network (b above).

d. Methods of Communication.

(1) The prevalent method of communication for VTC systems in the Army in Europe is IP router.

(2) Alternatively, ISDN is a digital telephone service that provides a 128 Kb/s channel. Two or three ISDN lines are usually bundled with a multiplexer (for example, an inverse multiplexer (IMUX)) to provide 256 Kb/s or 384 Kb/s VTC links.

(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 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. To be effective, these network protocols must be implemented across the entire network that the VTC traffic will traverse.

(c) Controls on the number of H.323 terminals simultaneously using the network (the H.323 gatekeeper provides terminal-access control). Subparagraph f below provides procedures for registering with the VTC hub.

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

(a) USAREUR VTC hubs have H.320 and H.323 gateways installed to enable 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 USAREUR VTC hubs using H.323 standards must first obtain a 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.

e. Multipoint Control Units.

(1) A multipoint control unit (MCU) enables two or more users to take part in one VTC. The 2d Sig Bde 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 USAREUR VTC hubs provide common-user service throughout Europe, dedicated connections to a hub are permitted only to meet special circumstances (for example, interface to tactical systems) and critical C2 requirements. The standard means of connecting to the hub is by IP.

(3) DISA provides MCU service to DOD VTC users in Europe through its DISA facility at Patch Barracks in Stuttgart, Germany. The USAREUR VTC Hubs will connect all Army in Europe users to DISA users.

(a) DISA offers two levels of security (Secret and Unclassified) and provides the primary link to VTC users and facilities in CONUS and in other theaters. DISA also provides links to other DOD service components, NATO units, and select Allied or partner-nation systems.

(b) Users must register with DISA before they may use DISA services. Registration and use of DISA 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 communication 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.

f. VTC Hub Registration. Army in Europe organizations will register all VTC equipment with the Wiesbaden USAREUR VTC Hub.

(1) Organizations must complete an AE Form 25-13B for each of their VTC facilities and send it to the USAREUR G6 VTC Program Manager for approval as part of the on-line registration. The USAREUR G6 requires this information to provide high-quality service and plan hub upgrades or expansion as required. If required, units may call the Wiesbaden USAREUR VTC Hub (mil 314-537-6127/28/30/31) for help in 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 the unit security manager provides a statement that certifies accreditation is being processed and identifies an estimated accreditation date.

(3) After the USAREUR G6 receives and processes AE Form 25-13B, requesting units will be granted hub service and be posted on the USAREUR G6 VTC webpage as authorized users.

21. VIDEO-TELECONFERENCE OPERATIONS

a. Network Operations Center. The Army in Europe Secure VTC Facility operates a Network Operations Center Help Desk on Clay Kaserne in Wiesbaden, Germany (mil 314-537-6127/28/30/31/32). If a VTC needs to be conducted outside normal operating hours, the user must contact the Army in Europe Facility Control Officer.

b. USAREUR VTC Hubs. Technicians at the USAREUR VTC hubs will—

If the Back button of your browser is not visible, use ALT + Back Arrow
to return to previous location.

(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 and quality assurance (PM/QA) sessions to enable registered users to perform scheduled PM on local equipment while aligning and testing audio and video quality in a VTC environment.

(5) Provide telephonic troubleshooting assistance to help individual operators identify, isolate, and solve problems when connecting through the VTC hubs. If a problem cannot be solved within a reasonable amount of time and the issue disrupts the VTC session for other users, the VTC network operations center will place the user in a waiting room while solving the problem. Once the problem is solved, the user may rejoin the conference with the microphone muted.

c. VTC Suite Operators. Registered VTC suite operators will—

(1) 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 technicians at a USAREUR VTC hub to meet local requirements.

(2) Perform PM on site according to original manufacturer manuals and applicable technical manuals.

(3) Keep records of all PM conducted.

(4) Take part in weekly PM/QA sessions that meet periodic testing requirements. In addition, a test session is required when any of the following events occur:

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

(b) Equipment is relocated or repaired.

(c) VTC hub technicians identify user audio or video problems (a failure to perform tests may result in long delays when establishing the next VTC session).

(d) An encryption key is superseded.

(5) VTC suite operators can report malfunctions attributable to communications circuits to the Army in Europe VTC Network Operations Center, which is located at the Wiesbaden VTC Hub. Operators may call mil 314-537-6127/28/30/32.

d. Scheduling VTCs.

(1) The ODCS, G3/5/7, HQ USAREUR, is responsible for scheduling VTCs bridged by USAREUR VTC hubs. Requesting offices may contact the VTC scheduler at military 314-537-6416/6410/6414 or e-mail: *usarmy.wiesbaden.usareur.mbx.vtc-schedulers@mail.mil*.

(2) The VTC scheduler will—

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

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

(c) Schedule and reserve DISA 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 DISA 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. Additionally, the scheduler will add 30 additional minutes to the scheduled end time of the VTC.

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

(f) Post all Army in Europe scheduled VTCs on the USAREUR SharePoint portal VTC calendar.

(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.

e. Secure VTC Communications Security (COMSEC) Procedures. VTC COMSEC custodians will obtain, load, and initiate appropriate COMSEC keys before COMSEC changeovers, which usually occur monthly at 0001Z on the 1st day of each 3-month period.

(1) The VTC hub COMSEC hand-receipt holder will contact 21st Sustainment Command by e-mail 5 days before the changeover and pick up the monthly COMSEC key. The custodian will then schedule an OTAR with DISA to receive the operational key from the DISN.

(2) The COMSEC Material Direct Support Activity, 21st Sustainment Command (mil 484-7469), distributes COMSEC keys 5 workdays before changeovers.

SECTION VII
GOVERNMENT-PROVIDED COMMERCIAL TELEVISION SERVICES

22. GOVERNMENT USE OF COMMERCIAL TELEVISION SERVICES

AR 25-13 requires all organizations to manage and conserve telecommunication assets and resources, including commercial television services. HQ USAREUR staff offices and USAREUR units are authorized to request authorization for and use of Government-funded commercial television (TV) services at specific types of locations according to the policy in AR 25-13 when that service meets Army telecommunication-conservation principles.

a. Because the Army considers commercial TV an above-baseline service, requesting organizations must fund the service.

b. Before requesting new or renewing existing commercial TV service, USAREUR MSCs will review their requirements, ensure the service is or will be provided only at authorized locations, and ensure that appropriated funds are authorized.

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5116.05, Military Command, Control, Communications, and Computers Executive Board

CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities

AR 25-13, Telecommunications and Unified Capabilities

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

AR 71-9, Warfighting Capabilities Determination

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

AR 735-5, Property Accountability Policies

Memorandum, HQDA, SAIS-CB, 11 September 2013, subject: U.S. Army Guidance on the Use of Commercial Mobile Devices (CMD).

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

USAREUR Commercial Mobile Device (CMD)-Authorization Document (maintained by USAREUR G6 and available at: *https://intranet.eur.army.mil/hq/portfoliomgnt* under the “Law & Policy” and “USAREUR” headings)

USEUCOM Instruction 6901.01A, Spectrum Management and Use of the Electromagnetic Environment

USEUCOM Spectrum Management Manual (SMM)

NOTE: USEUCOM publications are available at *https://portal.eucom.mil/* (registration required, then select *USEUCOM J1*, and *Publications*).

Military Communications-Electronics Board Publication 7, Frequency Resource Record System (FRRS) Standard Frequency Action Format (SFAF) (available from the Joint Interoperability Test Command (JITC) at *http://jitc.fhu.disa.mil/organization/references/publications/index.aspx* or through the Mercury application at *http://mercury.dreamhammer.com/*)

Military Communications-Electronics Board Publication 8, Standard Spectrum Resource Format (SSRF) (available from the Defense Information Systems Agency (DISA) at *http://www.disa.mil/Mission-Support/Spectrum/Enterprise-Services/MCEB-Pub-8*)

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 3953, Purchase Request and Commitment

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

AE Form 25-13A, Army in Europe Mobile Device User Agreement

AE Form 25-13B, Video Teleconferencing (VTC) Hub Registration

AE Form 25-13C, Commercial Telephone Log/Report

AE Form 25-13D, Telephone Control-Number Log

APPENDIX B
TELEPHONE CONTROL OFFICER APPOINTMENT ORDERS

Figure B-1 provides a sample format for a telephone control officer (TCO) appointment order.

Letterhead

XXXX-XXX-XX DD Mmmm YYYY

MEMORANDUM FOR

Title Firstname Lastname (Primary), Unit, APO AE 09XXX
Title Firstname Lastname (Alternate), Unit, APO AE 09XXX
ESO, S3, 2d Signal Brigade (Theater TCO), Unit 29800, APO AE 09096

SUBJECT: Telephone Control Officer Duty Appointment (BASECOM Account: XXXX)

1. **Reference (Authority):** AR 25-1, Army Information Technology.

2. **Appointment.** The additional duty of primary and alternate Telephone Control Officer (TCO) is assigned to the following:

Information Description	Primary TCO	Alternate TCO
Rank Name (First MI. Last):		
Organization:		
Unit Identification Code (UIC):		
Telephone:		
Fax:		
E-mail:		

3. **Period.** This appointment is effective immediately, supersedes all previous appointments to this duty, and will remain in effect for 1 year or until the appointee is officially relieved or released from this appointment, is reassigned from the unit, or separated from the service, whichever comes first.

4. **POC.** The POC is Rank Last, military 314-537-1111, civilian 0611-143-537-1111, or e-mail: *first.mi.last.civ@mail.mil*.

FIRST MI. LAST
RANK, BR
Duty Title

CF:
NETC-SEC-OP/Theater TCO (for files)
NETC-SEC-OP (for filing in CAIRS)

Figure B-1. Sample Format for a TCO Appointment Order

GLOSSARY

SECTION I
ABBREVIATIONS

2d Sig Bde	2d Signal Brigade
7th ATC	7th Army Training Command
21st SC	21st Sustainment Command
66th MI Bde	66th Military Intelligence Brigade
266th FMSC	266th Financial Management Support Center
ADCON	administrative control
AE	Army in Europe
AEPUBS	Army in Europe Library & Publishing System
AFO	authorized funding official
APL	approved products list
APO	Army post office
AR	Army regulation
AREC	Army Reserve Engagement Cell, Office of the Chief of Staff, Headquarters, United States Army Europe
ARNG	Army National Guard
ARO	authorized requesting official
ASR	Army service request
BASECOM	base communications
BES	BlackBerry enterprise server
BPA	blanket purchase agreement
C2	command and control
CAC	common access card
CAIRS	Configuration Accounting and Information Retrieval System
CBF	central base fund
CCB	configuration control board
CHESS	Computer Hardware, Enterprise Software, and Solutions
CG	commanding general
CG, USAREUR	Commanding General, United States Army Europe
civ	civilian
CMD	commercial mobile device
CODEC	coder/decoder
COMSEC	communications security
CONUS	continental United States
COTS	commercial off-the-shelf
CoS	chief of staff
CTO	certificate to operate
CUI	controlled unclassified information
DA	Department of the Army
DCG, USAREUR	Deputy Commanding General, United States Army Europe
DCG-ARNG, USAREUR	Deputy Commanding General, Army National Guard, United States Army Europe
DCG-M&RA, USAREUR	Deputy Commanding General, Mobilization and Reserve Affairs, United States Army Europe
DCO	dial central office

DCS	deputy chief of staff
dir	director
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITCO	Defense Information Technology Contracting Organization, Defense Information Systems Agency
DOD	Department of Defense
DRM	directorate of resource management
DRSN	Defense Red Switch Network
DSL	digital subscriber line
DSN	Defense Switched Network
ECC	United States Army Expeditionary Contracting Command
EDGE	Enhanced Data Rates for Global System Mobile Evolution
ESD	Enterprise Service Desk
EU	European Union
FCST	finance customer support team
FMO	Frequency Management Office, Operations, Plans, and Exercises 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
GO	general officer
GPRS	General Packet Radio Service
GS	general staff
GSA	General Services Administration
GSM	Global System Mobile
HF	high frequency
HQ	headquarters
HQDA	Headquarters, Department of the Army
HQ USAREUR	Headquarters, United States Army Europe
https	hypertext transfer protocol over a secure-sockets layer
IAPM	information assurance program manager
IM	information management
IMO	information management officer
IMCOM	United States Army Installation Management Command
IMCOM-Europe	United States Army Installation Management Command Europe
IMUX	inverse multiplexer
INMARSAT	International Maritime Satellite
IP	Internet protocol
ISDN	integrated service digital network
ISP	Internet service provider
IT	information technology
ITSM	information technology service management
J2	deputy chief of staff, intelligence (joint staff)
J6	deputy chief of staff, information management (joint staff)

JITC	Joint Interoperability Test Command
JMRC	United States Army Joint Multinational Readiness Center, 7th Army Training Command
JWICS	Joint Worldwide Intelligence Communications System
Kb/s	kilobyte per second
LAN	local area network
LCR	life cycle replacement
LSR	local service request
LTE	Long-Term Evolution (also known as, the 4G (standard))
MAC	media access control
MC4EB	Military Command, Control, Communications, and Computers (C4) Executive Board ((glossary (terms))
MCEB	Military Communications-Electronics Board (obsolete as an organization name (use MC4EB), but not for publication names)
MCU	multipoint control unit
MHz	megahertz
mil	military
MSC	major subordinate command
MTOE	modified table of organization and equipment
NAF	nonappropriated fund
NARFA	National Allied Radio Frequency Agency
NATO	North Atlantic Treaty Organization
NEC	network enterprise center
NETCOM	United States Army Network Enterprise Technology Command
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
ODCS	office of the deputy chief of staff
OPCON	operational control
PKI	public key infrastructure
PM	preventive maintenance
PM/QA	preventive maintenance and quality assurance
POC	point of contact
PSS	Preferred Subscriber Service
PVN	purchase voucher number
RAF	regionally aligned force
RF	radio frequency
RFC	request for change
RGBAN	Regional (Global) Broadband Area Network
RM	resource management
S3	operations and training officer
S6	information management officer
SAR	satellite access request
SATCOM	satellite communications
SBU	Sensitive but Unclassified (service)
SBU Voice	Sensitive but Unclassified Voice (network)
SCIF	sensitive compartmented information facility
SFAF	Standard Frequency Action Format
SIM	subscriber identity module
SIPRNET	Secret Internet Protocol Router Network
S/MIME	secure/multipurpose Internet mail extension

SOI	signal operating instruction
SSL	secure sockets layer
STE	secure telephone equipment
STIG	security technical implementation guide
supp	supplement
TCO	telephone control officer
TDA	table of distribution and allowances
TLS	transport layer security
TOO	telecommunications ordering office
UHF	ultra-high frequency
UMTS	Universal Mobile Telecommunications System
U.S.	United States
USAG	United States Army garrison
USANATO Brigade	United States Army North Atlantic Treaty Organization Brigade
USAR	United States Army Reserve
USAREUR	United States Army Europe
USAREUR G2	Deputy Chief of Staff, G2, United States Army Europe
USAREUR G3/5/7	Deputy Chief of Staff, G3/5/7, 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
VTC	video-teleconference (video-teleconferencing)
WBS	work breakdown structure

SECTION II
TERMS

99-access
Phone service that is enabled to call outside the military voice network to civilian numbers (accessed by dialing “99” before the civilian telephone number) (para 9a)

Army in Europe
USAREUR (which includes HQ USAREUR, USAREUR major subordinate commands, and commands under USAREUR operational control), the United States Army Installation Management Command Europe (IMCOM-Europe) (which includes United States Army garrisons in Europe and IMCOM-Europe managed forward operating sites and other installations in Europe), and the Civilian Human Resources Agency, Northeast/Europe Region

NOTE: AE Regulation 10-5, paragraph 1-1, and the USAREUR Organizational Chart (available at *http://www.eur.army.mil/organization/units.htm*) provide more information about command and support relationships among HQ USAREUR, USAREUR major subordinate commands, and commands under USAREUR operational control or other relationships, as well as about select tenant organizations

base communications
All the telecommunications networks and services that are internal to a single installation or United States Army garrison community location

If the Back button of your browser is not visible, use ALT + Back Arrow to return to previous location.

cell phone
An active subscriber-identity-module chip in combination with either a handset or another commercial mobile device that has only basic Global System Mobile capability (to send and receive voice and text messages), which does not include data capability

long-haul communication services
Telecommunication services that span distances of more than 20 miles or go outside an installation (as defined by the Defense Information Systems Agency)

MC4EB
The Military Command, Control, Communications, and Computers (C4) Executive Board (MC4EB), previously known as the Military Communications-Electronics Board (MCEB), that serves as the DOD senior-level council for C4 and Warfighting-mission-area information-technology matters in execution of Chairman of the Joint Chiefs of Staff responsibilities

official commercial telephone service
Government-funded telephone service, digital-subscriber-line service, or both that are provided directly from a host-nation telecommunications company for installation and use only for Government business

USAREUR OPCON command
An organizations in which the senior headquarters of the Army element assigned in Europe remains under the administrative control of the CONUS higher headquarters, but is under the operational control of the United States Army Europe