Information Management

Army in Europe Telecommunications and Unified Capabilities

For the Commander:

HARTMUT H. RENK
Brigadier General, GS
Chief of Staff

Official:

SCOTT T. CHANCELLOR
Chief, Army in Europe
Document Management

Summary. This regulation provides policy and assigns responsibilities for telecommunications and unified capabilities for the Army in Europe (glossary).

Applicability. This regulation applies to HQ USAREUR staff offices, USAREUR major subordinate commands, commands under USAREUR operational control, all units attached to or supporting USAREUR, and USAREUR tenant commands.

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

Supplementation. Organizations will not supplement this regulation without approval of the Programs and Policy Branch; Programs, Policy, and Projects Division; Office of the Deputy Chief of Staff (ODCS), G6, HQ USAREUR.

Forms. This regulation prescribes AE Form 25-13A and AE Form 25-13B. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at http://www.aepubs.eur.army.mil/.

Suggested Improvements. The proponent of this regulation is the Programs and Policy Branch; Programs, Policy, and Projects Division; ODCS, G6, HQ USAREUR (mil (sensitive but unclassified) 537-6223). Users may send suggested improvements to this regulation by email to the Programs and Policy Branch at usarmy.wiesbaden.usareur.list.g6-policy@mail.mil.
1. Purpose

This regulation establishes Army in Europe policy and assigns responsibilities for managing telecommunications and unified capabilities (UC). For Army tenant units residing on non-Army-hosted installations, some local processes may vary from this regulation. The guidance and direction in this regulation will be used as the basis for providing input for local memorandums of agreement.

2. References

Appendix A lists references.

3. Explanation of Abbreviations and Terms

The glossary defines abbreviations and terms.

4. Responsibilities

a. The Chief of Staff (CoS), HQ USAREUR, is the approval authority for—

   (1) Defense Red Switch Network (DRSN) telephones.

   (2) Commercial high-speed Internet services in the quarters of preferred-subscriber-service customers (AE Pam 25-13, para 4a(2)).

   (3) Exceptions to policy in this regulation for which the USAREUR G6 has not been delegated approval authority.
b. The USAREUR G3/5/7 will—

(1) Validate commercial mobile device (CMD) requirements and CMD contingency-support missions and serve as the approval authority for CMDs and exercise CMDs for HQ USAREUR staff offices and USAREUR major subordinate commands (MSCs). Validation and approval of CMD requirements will be in accordance with the USAREUR CMD Authorization Document developed by the USAREUR G6 (AE Pam 25-13).

(2) Control the issue, turn-in, and reuse of exercise CMDs used by HQ USAREUR staff offices and USAREUR MSCs.

(3) Validate and serve as the approval authority for video-teleconferencing (VTC) requirements of HQ USAREUR staff offices and USAREUR MSCs in accordance with the USAREUR CMD Authorization Document.

(4) Develop the operational requirements for network architecture in conjunction with the Enterprise Architecture Branch; Programs, Policy, and Projects Division; Office of the Deputy Chief of Staff (ODCS), G6, HQ USAREUR.

(5) Review and coordinate operational needs statements that are submitted for tactical information technology (IT) equipment and services and coordinate with the USAREUR G6 on actions to ensure interoperability between IT systems required by the United States Army Reserve and deployed IT systems (AR 71-9).

(6) Ensure that all theater command, control, communications, computers, and information technology priorities support USAREUR strategic plans.

(7) Review and approve or disapprove requests for authorized service interruptions.

c. As the Chief Information Officer (CIO) for the Army in Europe, the USAREUR G6 will—

(1) Report to the CG, USAREUR. The CIO is the primary IT representative for HQ USAREUR, the 2d Calvary Regiment, the 7th Army Training Command, the 10th Army Air and Missile Defense Command, the 12th Combat Aviation Brigade, the 19th Battlefield Coordination Detachment, the 21st Sustainment Command, and the 173d Airborne Brigade Combat Team.

(2) Participate in the USAREUR Acquisition Review Board for procurements related to telecommunications and IT.

(3) Validate all USAREUR IT requirements that cost $25,000 or more. Requirements that need to be approved by a member of the USAREUR Command Group will be reviewed and approved first by the USAREUR G6. IT resources include hardware, software, telecommunications, IT contracting services, and IT civilian personnel.

(4) Provide policy and oversight for USAREUR-level programs, such as, but not limited to, the CMD Program and the VTC Program (AE Pam 25-13, secs V and VI).

(5) Approve all Voice over Internet Protocol (VoIP) networks (AE Pam 25-13, para 10).
d. The USAREUR Judge Advocate (JA) will evaluate the legal aspects of requests for commercial high-speed Internet services (a(2) above) in the quarters of key general officers (GOs) and Senior Executive Service (SES) personnel in Europe. The USAREUR JA will also review IT-related requests and provide a legal opinion as needed.

e. HQ USAREUR staff principals, commanders of USAREUR MSCs and commands under USAREUR operational control (OPCON), commanders of units attached to or supporting USAREUR, and commanders of USAREUR tenant commands will—

(1) Coordinate with the USAREUR G6 on IT issues to determine smartphone requirements according to AR 25-13 and AE Pamphlet 25-13.

(2) Designate a telephone control officer (TCO) to validate the use of telecommunications within their organizations and monitor command programs for base communications (BASECOM) services. Newly assigned TCOs must complete TCO certification training within 90 days after being appointed, provided the Army in Europe Information Technology Training (AE-ITT) TCO course is available. TCOs must contact the AE-ITT office for training provided in their area. AE Pamphlet 25-13, paragraph 7, provides information about the Army in Europe TCO Program.

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

(1) Is under the operational control of USAREUR.

(2) Exercises Network Enterprise Technology Command/9th Signal Center (Army) technical-direction and configuration-management authority for Army in Europe voice networks, data networks, and enterprise application systems that support HQ USAREUR, USAREUR MSCs, commands under USAREUR OPCON, and USAREUR attached, supporting, and tenant commands.

(3) Provides command, control, communications, computers, and information management (C4IM) services to Army in Europe organizations. Commanders of 2d Sig Bde subordinate units are responsible for installation network enterprise centers (NECs) providing support to United States Army garrisons in their area of responsibility.

(4) Has a vital role in providing key C4IM services for the Army in Europe. This includes, but is not limited to, maintaining area processing centers, staffing the Enterprise Service Desk, and overseeing the Regional Cyber Center–Europe. These facilities are part of the overall scheme of IT service providers for the Army in Europe.

(5) Provides data connectivity between local area networks (LANs), Army in Europe NIPRNET and SIPRNET, on installations and connectivity to outside networks. Engineering, installing, operating, and maintaining installation LANs is part of the 2d Sig Bde mission. These duties will not be handled by any other unit without a waiver from the ODCS, S3, 2d Sig Bde. Regional operation-center personnel will operate and maintain installation LANs, design internal cable-distribution systems to meet commercial standards, and install these systems.

(6) Through its Tactical Action Center–Europe (TAC-E), serves as the TCO and telecommunications ordering office (TOO) for the European theater, providing policy and oversight to TCO and TOO theater-level programs.

(7) Provides policy input for Army in Europe publications.
5. BILLING AND PAYMENT

a. TCOs will—

(1) Validate that they have reviewed the monthly BASECOM/Central Base File reports for their assigned organizations. TCOs receive these reports through the Configuration Accounting Information Retrieval System or from the 2d Sig Bde S8. In addition, commanders and activity heads will ensure that TCOs review and validate cell phone, smartphone, and other CMD usage in accordance with AE Pamphlet 25-13.

(2) Ensure that all BASECOM requirements for above-baseline services are validated in the service-level agreement between their organization and the servicing NEC.

(3) Ensure that all CMD users sign AE Form 25-13A annually.

b. Operators will use the most cost-effective service available when placing calls to CONUS. When calling a telephone number in CONUS from Europe, operators handling sensitive but unclassified (SBU) calls may use commercial long-distance services for official calls that are not being made for command and control purposes. SBU call operators will not transfer nonemergency morale calls to other operators for “off-netting” (that is, transferring the call to a commercial line) if those calls result in fees being charged to the U.S. Government.

6. VIDEO-TELECONFERENCING

a. VTC activities and capabilities include room-based, roll-about, stand-alone, and soft client devices that are above baseline services. VTC items must meet DOD cybersecurity standards.

b. The USAREUR G3/5/7 is the approving authority for VTC systems for HQ USAREUR staff offices and USAREUR MSCs. Commands under USAREUR OPCON and USAREUR attached, supporting, and tenant commands will follow their Army command, Army service component command, or direct-reporting unit policy and guidance on approval authority.

c. All intelligence activities that require sensitive compartmented information (SCI) secure VTC capability will use the Joint Worldwide Intelligence Communications System (JWICS) or an equivalent SCI VTC medium and will be managed by the Army intelligence organization where the JWICS is installed.

d. Commanders and division chiefs will appoint, in writing, a primary and an alternate VTC systems administrator (SA) as POCs for VTC operations. The functions of an SA include routine maintenance, testing, and other requirements as needed. VTC SAs must know VTC standards and be trained on using unit VTC equipment (AE Pam 25-13, sec VI).

e. The USAREUR G6 will—

(1) Appoint a VTC program manager (PM) to provide for the annual identification, funding, and acquisition of required commercial off-the-shelf (COTS), USAREUR-controlled VTC equipment including the following coder/decoders (CODECs): room-based, roll-about, stand-alone, and soft client devices that are above baseline services. The VTC PM will—
(a) Determine annual VTC equipment life-cycle replacement (LCR) allocations for HQ USAREUR staff offices, USAREUR MSCs, commands under USAREUR OPCON, and USAREUR attached, supporting, and tenant commands.

(b) Establish user VTC policy, procedures, and guidelines (AE Pam 25-13, sec VI).

(c) Establish and maintain a list of VIP positions for HQ USAREUR staff offices, USAREUR MSCs, commands under USAREUR OPCON, and USAREUR attached, supporting, and tenant commands.

(2) Appoint the Chief, VTC Operations Branch. The Chief, VTC Operations Branch, will—

(a) Be responsible for maintaining the above-baseline VTC architecture in Europe.

(b) Operate and maintain VTC hub equipment. The hub infrastructure will provide point-to-point and multipoint VTC capabilities up to the US SECRET classification in support of command and control and user requirements.

(c) Determine annual audio and video equipment for new installations and LCR allocations for HQ USAREUR staff offices for shared conference rooms in the USAREUR Mission Command Center.

(d) Create and maintain a list of registered USAREUR VTC systems.

(3) Obtain, load, and initiate appropriate communications-security keys for VTC missions that are classified as SECRET to support USAREUR exercises.

f. HQ USAREUR staff offices, USAREUR MSCs, commands under USAREUR OPCON, and USAREUR attached, supporting, and tenant commands will—

(1) Obtain and maintain approval to operate assigned VTC systems using the risk-management framework (RMF).

(2) Operate and maintain internal VTC systems.

(3) Register above-baseline VTC systems with the ODCS, G6, HQ USAREUR (AE Form 25-13B).

(4) Comply with the following collaborative desktop VTC risk-mitigating factors:

(a) Collaborative desktop VTC equipment used in a single-person Government office must be approved to process data up to the classification of the space in which the equipment is used. The single-person office must have all walls extended to completely touch the ceiling and floor. Openings such as doors and windows must be completely closed.

(b) Collaborative desktop VTC devices (for example, networked whiteboards, cameras, microphones) must provide an explicit indication of use to users physically present at the devices and in close proximity to the devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated such as VTC-in-progress signage in the office and on the outside of the office door.
(c) Remote activation of collaborative computing devices must be prohibited except in situations for which the organization has defined exceptions under which remote activation is to be allowed and when those exceptions have been approved in the organization’s RMF.

(d) The information system (IS) must provide physical disconnect of collaborative computing devices in a manner that supports ease of use.

(e) The organization will disable or remove collaborative computing devices from organization-defined ISs or IS components in organization-defined secure workareas when users are not explicitly using the devices (for example, manually cover all cameras, disconnect all microphones from desktop computers and laptops, disable collaborative computing applications). This will prevent the transmission of in-room camera video, in-room audio, and desktop computer and laptop audio and video sources.

(f) The IS must provide an explicit indication of current participants in organization-defined online meetings and VTCs.

(g) The organization will ensure that all personnel participating in the VTC have the appropriate security clearance, access, and need-to-know for the specific information to be presented.

(h) The organization will ensure that all classified papers to be used and all classified presentations have been approved, in writing, by the originators of the information for release to the cleared VTC participants.

(i) IMCOM-Europe will conduct physical security inspections every 2 years for highly sensitive, sensitive, or nonsensitive IS service center activities or facilities servicing multiple customers. Inspections of all other IS activities or facilities not classified as critically sensitive will be incorporated into scheduled physical security inspections of the individual activity or facility.

(j) The use of collaborative desktop VTC systems in open-area office workspaces such as pods or common areas must be prohibited.

(k) All exceptions for using collaborative desktop VTC systems must be approved through the RMF.

  g. USAREUR MSCs, commands under USAREUR OPCON, and USAREUR attached, supporting, and tenant commands will—

  (1) Determine their audio- and video-equipment requirements for new installations and LCR and fund these requirements.

  (2) Obtain, load, and initiate appropriate communications-security keys for VTC missions that are classified as SECRET to support USAREUR exercises.

7. ARMED FORCES RADIO AND TELEVISION SERVICE
As an adjunct to the Armed Forces Radio and Television Service, the American Forces Network Europe provides cable- and satellite-television transmission support. Television-reception support in Europe involves the Office of the Public Affairs Officer, HQ USAREUR; 2d Sig Bde; and IMCOM-Europe.
8. COMMERCIAL MOBILE DEVICES
The Army in Europe policy on the use of Government-issued CMDs is as follows:

a. Before being issued a smartphone, cell phone, or other CMD, Army in Europe personnel must complete and sign AE Form 25-13A. Units will not issue any device to personnel who refuse to complete and sign the form.

b. CMDs enable users to conduct Government business while away from their regular workplace. When using these devices, users must exercise good judgment to avoid security incidents, accountability issues, and exorbitant costs.

c. Non-enterprise tablet CMDs (that is, tablets without SIM cards that are not administered by Defense Information System Agency (DISA) management servers) can process only publicly releasable information. USAREUR G3/5/7 approval (para 4b(1)) is not required for tablets that are capable of Wi-Fi only.

d. Enterprise tablet CMDs (with SIM card) will meet requirements to allow connectivity to DOD networks and process information up to the For Official Use Only level.

   (1) Smartphone users identified in the USAREUR CMD Authorization Document are not authorized both an enterprise-connected tablet and a smartphone unless the user is a GO, an SES member, or a commensurate-level command sergeant major (CSM).

   (2) Organizations may allow users to turn in their smartphones in order to receive a cell phone and a tablet, but TCOs of USAREUR MSCs must inform the HQ USAREUR TCO before doing so.

   (3) Requests for exceptions to the policy in (1) and (2) above must be submitted to the USAREUR G3/5/7 for approval using the CMD authorization-modification request memorandum (AE Pam 25-13, para 19e(1)).

e. Hybrid laptops are defined as being capable of serving both as a mobile tablet and as a NIPRNET laptop and therefore require special authorization consideration.

   (1) Hybrid laptops to be used with a SIM card must obtain approval of both the COTS IT LCR PM and the CMD PM. An approval of a hybrid laptop with a SIM card will be considered a tablet authorization under the CMD program and a laptop authorization under the COTS IT LCR program.

   (2) Hybrid laptops to be used without a SIM card require only COTS IT LCR PM approval.

   (3) Because of budgetary constraints, an approval of a hybrid laptop will automatically displace the user’s current laptop or desktop system. In other words, a user authorized a hybrid laptop to be used with a SIM card will not be authorized an additional laptop, desktop, or other tablet device.

9. NONTACTICAL LAND MOBILE RADIO SYSTEMS
The operation of equipment that emits radio frequencies requires the approval of the host nation. Requests to operate radio-frequency equipment must be sent to the Operations, Plans, and Exercise Division, ODCS, G6, HQ USAREUR (AE Pam 25-13, para 6).
a. **Iridium Telephones.** Iridium telephones are handheld satellite radio telephones that can also be used for storing and transferring data. Fielded units with Iridium telephones must use the equipment and service at least once every quarter to maintain the equipment and service. Service can be ordered through DISA Direct at [https://inah.pac.disa.mil/home.shtml](https://inah.pac.disa.mil/home.shtml).

b. **International Maritime Satellite (INMARSAT) Telephones.** INMARSAT telephones are portable satellite radio telephones that can also be used for storing and transferring data.

## 10. LONG-HAUL AND DEPLOYABLE TELECOMMUNICATIONS

a. **DRSN.** DRSN is a secure telephone system that is part of the Defense Information Systems Network but independent of SBU communications. Its use is normally reserved for GOs. Users can connect to a DRSN switch using secure telephone equipment. Requests for DRSN service must be sent to the Programs, Policy, and Projects Division, ODCS, G6, HQ USAREUR; recommended for approval by the CoS, HQ USAREUR; and approved by the USEUCOM J6.

b. **Army in Europe NIPRNET.** The Army in Europe NIPRNET is a network that is driven by the Internet Protocol (IP) and can be used to send information marked no higher than “unclassified but sensitive.”

c. **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.

d. **DISA VTC Hub Service.** DISA routes dial-up integrated services digital network (ISDN) VTC traffic and IP VTC traffic through its hub in Stuttgart. The hub is intended mainly for transatlantic VTC traffic. USAREUR maintains its own hubs in Wiesbaden and Kaiserslautern.

e. **Noncommon Service Long Haul (as defined by DISA).**

   (1) **Dedicated Circuits.** Dedicated circuits for voice or data to span distances of more than 20 miles must be provided by DISA. Requests for an exception to policy must be submitted to the Programs, Policy, and Projects Division, ODCS, G6, HQ USAREUR, for approval.

   (2) **Transponders.** For emergencies, exercises, and temporary locations, a unit may rent a satellite transponder with a specified bandwidth. Current costs of portable satellite communications equipment are available at [http://www.disa.mil/Services/Network-Services](http://www.disa.mil/Services/Network-Services).

## 11. VOICE SERVICES

The Army in Europe policy on implementing VoIP is as follows:

a. The PM, Defense Communication Systems–Europe, is responsible for implementing VoIP in the Army in Europe and developing a VoIP migration plan and architecture based on the DISA VoIP rollout. The DISA and Army Migration Plan will result in a theater-wide capability for VoIP that is integrated into the Defense Switched Network. The PM, Defense Communication Systems–Europe, will ensure VoIP systems—

   (1) That traverse Government IP networks (NIPRNET and SIPRNET) have been certified by the Joint Interoperability Test Command (JITC) and are on the JITC Approved Products List in accordance with DOD UC requirements, CJCSI 6211.02C, and CJCSI 6215.01C.
(2) Are IPv6-capable in accordance with the DISA Security Technical Implementation Guide (STIG) on network infrastructure.

(3) Comply with DISA STIGs on VoIP, which also include guidance for Voice over Secure Internet Protocol.

(4) Receive authorization to connect from the DISA Unified Capabilities Certification Office in Arlington, Virginia.

(5) Are accredited in accordance with DOD Instruction 8510.01.

b. Requesting organizations will define their requirements, conduct a cost-benefit analysis, and send the request and analysis results to their servicing NEC.

c. The NEC will validate the request and forward it to the USAREUR G6.

d. The USAREUR G6 will incorporate the solution into the migration plan and forward the plan to the Army CIO/G-6 for final approval.

e. All Army in Europe organizations that require VoIP must follow HQDA guidance before installing any VoIP solution on the Army in Europe domain “EUR.”

f. The policy in a(1) through (5) above does not apply to systems fielded by the Program Executive Officer, Enterprise Information System, HQDA, for which VoIP is a component of the accredited system, and to DOD IP networks not managed by the 2d Sig Bde.

12. COMMERCIAL TELEVISION SERVICES

AR 25-13 requires that all units manage and conserve telecommunications assets. Unit commanders are responsible for conserving unit telecommunications. Commercial TV services are above baseline and must be funded by the requesting unit.

a. Unit Responsibilities. HQ USAREUR staff offices and USAREUR MSCs will—

(1) Review requirements to ensure that the use of appropriated funds for commercial TV services is authorized only for offices of GOs, SES members, and CSMs; offices of commanders, CSMs, and civilian-equivalent personnel at the brigade or battalion level; operations centers at the MSC, division headquarters, or higher level; unit dayrooms; and offices that require a customer waiting-area.

(2) Ensure that authorized TV services are limited to USAREUR Internet Protocol television (IPTV) services, if available, and satellite services (Army and Air Force Exchange Service and American Forces Network). Units that require services to be provided by other entities (for example, TKS, Sky) will obtain USAREUR G3/5/7 approval through the USAREUR Requirements Validation System (AE Pam 70-13-45) for an exception to use these services.

b. Commercial TV Request Process. To request commercial TV services, HQ USAREUR staff offices and USAREUR MSCs will submit a ticket to the Army Enterprise Service Desk (119 ticket). The Headquarters Support Division, ODCS, G6, HQ USAREUR, will determine the best technical solution and cost estimate for units located on Clay Kaserne in Wiesbaden, Germany. The servicing NECs will determine the best technical solution and cost estimate for all other locations.
APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities

CJCSI 6215.01C, Policy for Department of Defense (DOD) Voice Networks With Real Time Services (RTS)

DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT)

Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Office Publication, Department of Defense Unified Capabilities Requirements 2013

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

AR 25-13, Army Telecommunications and Unified Capabilities

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

AR 71-9, Warfighting Capabilities Determination

AE Regulation 25-400-2, Army in Europe Records Information Management

AE Pamphlet 25-13, Army in Europe Telecommunications and Unified Capabilities

AE Pamphlet 70-13-45, USAREUR Requirements Validation System

SECTION II
FORMS

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

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

SECTION I
ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2d Sig Bde</td>
<td>2d Signal Brigade</td>
</tr>
<tr>
<td>AE</td>
<td>Army in Europe</td>
</tr>
<tr>
<td>AE-ITT</td>
<td>Army in Europe Information Technology Training</td>
</tr>
<tr>
<td>AEPUBS</td>
<td>Army in Europe Library &amp; Publishing System</td>
</tr>
<tr>
<td>AR</td>
<td>Army regulation</td>
</tr>
<tr>
<td>BASECOM</td>
<td>base communications</td>
</tr>
<tr>
<td>C4IM</td>
<td>command, control, communications, computers, and information management</td>
</tr>
<tr>
<td>CG, USAREUR</td>
<td>Commanding General, United States Army Europe</td>
</tr>
<tr>
<td>CIO</td>
<td>chief information officer</td>
</tr>
<tr>
<td>CJCSI</td>
<td>Chairman of the Joint Chiefs of Staff instruction</td>
</tr>
<tr>
<td>CMD</td>
<td>commercial mobile device</td>
</tr>
<tr>
<td>CONUS</td>
<td>continental United States</td>
</tr>
<tr>
<td>CoS, HQ USAREUR</td>
<td>Chief of Staff, Headquarters, United States Army Europe</td>
</tr>
<tr>
<td>COTS</td>
<td>commercial off-the-shelf</td>
</tr>
<tr>
<td>CSM</td>
<td>command sergeant major</td>
</tr>
<tr>
<td>DA</td>
<td>Department of the Army</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DRSN</td>
<td>Defense Red Switch Network</td>
</tr>
<tr>
<td>GO</td>
<td>general officer</td>
</tr>
<tr>
<td>HQDA</td>
<td>Headquarters, Department of the Army</td>
</tr>
<tr>
<td>HQ USAREUR</td>
<td>Headquarters, United States Army Europe</td>
</tr>
<tr>
<td>IMCOM-Europe</td>
<td>United States Army Installation Management Command Europe</td>
</tr>
<tr>
<td>INMARSAT</td>
<td>International Maritime Satellite</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IS</td>
<td>information system</td>
</tr>
<tr>
<td>ISDN</td>
<td>integrated services digital network</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>JITC</td>
<td>Joint Interoperability Test Command</td>
</tr>
<tr>
<td>JWICS</td>
<td>Joint Worldwide Intelligence Communications System</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LCR</td>
<td>life-cycle replacement</td>
</tr>
<tr>
<td>mil</td>
<td>military</td>
</tr>
<tr>
<td>MSC</td>
<td>major subordinate command</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NEC</td>
<td>network enterprise center</td>
</tr>
<tr>
<td>NIPRNET</td>
<td>Unclassified but Sensitive Internet Protocol Router Network</td>
</tr>
<tr>
<td>ODCS</td>
<td>office of the deputy chief of staff</td>
</tr>
<tr>
<td>pam</td>
<td>pamphlet</td>
</tr>
<tr>
<td>PM</td>
<td>program manager</td>
</tr>
<tr>
<td>RMF</td>
<td>risk-management framework</td>
</tr>
<tr>
<td>S8</td>
<td>resource management officer</td>
</tr>
<tr>
<td>SA</td>
<td>systems administrator</td>
</tr>
<tr>
<td>SBU</td>
<td>sensitive but unclassified</td>
</tr>
<tr>
<td>SCI</td>
<td>sensitive compartmented information</td>
</tr>
</tbody>
</table>
SES  Senior Executive Service
SIM  subscriber identity module
SIPRNET  Secret Internet Protocol Router Network
STIG  Security Technical Implementation Guide
TAC-E  Tactical Action Center–Europe, 2d Signal Brigade
TCO  telephone control officer
TOO  telecommunications ordering office
UC  unified capabilities
U.S.  United States
USAREUR  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 JA  Judge Advocate, United States Army Europe
USEUCOM  United States European Command
USEUCOM J6  C4/Cyber, United States European Command
VIP  very important person
VoIP  Voice over Internet Protocol
VTC  video-teleconference
Wi-Fi  wireless fidelity

SECTION II
TERMS

Army in Europe
All U.S. Army units in the USEUCOM area of responsibility