Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command Europe
Sembach, Germany

Army in Europe Regulation 25-1*

10 October 2019

Information Management

Army in Europe Information Technology

***This regulation supersedes AE Supplement 1 to AR 25-1, 21 November 2016, and rescinds AE Form 25-1H.**

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 establishes policy and assigns responsibilities for information management and information technology in the Army in Europe.

Applicability. This regulation applies to all U.S. Army organizations in Europe and to DOD and non-DOD organizations that use Army in Europe networks.

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 25-1J, AE Form 25-1K, AE Form 25-1N, and AE Label 25-1A. AE and higher level forms are available through the Army in Europe Library & Publishing System (AEPUBS) at *https://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*.

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

CONTENTS

---

1. PURPOSE

This regulation establishes policy and assigns responsibilities for information management (IM) and information technology (IT) in the Army in Europe.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. RESPONSIBILITIES

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

(1) Defense Red Switch Network telephones.

(2) Commercial high-speed Internet services in the quarters of preferred-subscriber-service customers.

(3) Exceptions to policy in this regulation for which approval authority has not been delegated to the USAREUR G6.

(4) IT service requirements with a known or estimated value of $100,000 or more and for IT nonservice requirements with a known or estimated value of $250,000 or more (AE Pam 70-13-45).

b. USAREUR G3/5/7. The USAREUR G3/5/7 will—

(1) Validate and be the approval authority for Automation Table of Equipment requirements of HQ USAREUR staff offices and USAREUR major subordinate commands (MSCs).

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

(3) Review and coordinate operational needs statement (ONS) submissions for tactical IT equipment and services, and coordinate with the USAREUR G6 on interoperability actions between United States Army Reserve and deployed IT system requirements (AR 71-9).

(4) Ensure all theater command, control, communications, computers, and information management (C4IM) priorities support USAREUR strategic plans.

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

(6) Participate in the Theater Acquisition Review Board and function as the designated IT approval authority for—

(a) Service requirements with a known or estimated value of less than $100,000.

(b) Nonservice requirements (hardware and software) with a known or estimated value of less than $250,000.

c. USAREUR G6. The USAREUR G6 or his or her designee will—

(1) Participate in the Theater Acquisition Review Board and provide concurrence and technical approval for all service and nonservice IT requirements to ensure policy compliance (AE Pam 70-13-45).

(2) Validate all IT requirements for HQ USAREUR staff offices and USAREUR MSCs. Requirements that must be approved by a member of the USAREUR Command Group will first be reviewed and approved by the USAREUR G6. IT resources include IT civilian personnel, IT contracting services, IT utilities (base communications (BASECOM)), hardware, software, and telecommunications.

(3) Provide policy and oversight for USAREUR theater-level programs, such as, but not limited to, the following:

(a) Life-Cycle Replacement (LCR) Program.

(b) Copier-Management Program.

(c) Video-Teleconference (VTC) Program.

(4) Be the approval authority for the procurement, implementation, and maintenance of all Voice over Internet Protocol (VoIP) networks for HQ USAREUR staff offices and USAREUR MSCs (AE Pam 25-13).

d. Assistant USAREUR G6. The Assistant USAREUR G6 is the proponent for career program (CP) 34 for Army in Europe IM and information technology IT professionals.

(1) HQ USAREUR staff offices and USAREUR MSCs will—

(a) Appoint a CP-34 activity manager and send the appointment orders to the USAREUR CP-34 Program Management Office (PMO), ODCS, G6, HQ USAREUR.

(b) Coordinate all CP-34 training requirements through their appointed CP-34 activity manager who, in turn, will coordinate the requirements with the USAREUR CP-34 PMO. Each year, organizational CP-34 activity managers will review the individual development plans of Army in Europe IM and IT professionals in their organizations to ensure the plans meet the professional-development guidelines issued by the USAREUR CP-34 PMO.

(2) Commands under USAREUR operational control (OPCON) and USAREUR attached, supporting, and tenant commands will follow their local policies and procedures for CP-34 activities.

e. USAREUR Judge Advocate (USAREUR JA). The USAREUR JA will evaluate the legal aspects of requests for commercial high-speed Internet service in the quarters of key Army personnel in Europe. The USAREUR JA will also review IT-related requests and provide a legal opinion as needed.

f. HQ USAREUR Staff Offices, USAREUR MSCs, USAREUR OPCON commands, and USAREUR Attached, Supporting, and Tenant Commands.

(1) HQ USAREUR staff principals and commanders of USAREUR MSCs, USAREUR OPCON commands, and USAREUR attached, supporting, and tenant commands will—

(a) Designate a primary and an alternate information management officer (IMO).

1. The appointment order (in memorandum format) must be signed by the commander or director and sent to the local network enterprise center (NEC). Appendix B shows the format of an appointment order. If the commander is not present because of an exercise or deployment, a representative authorized to sign for the commander may sign the order.

2. Appointment orders remain in effect for 1 year or until the IMO is officially relieved or released from the appointment, whichever occurs first.

(b) Designate an organizational information systems security manager (ISSM) to perform the responsibilities in AR 25-2.

(c) Coordinate the investigation of new information systems (ISs) that are not addressed in AR 25-1 and are driven by program managers (PMs) at the ODCS, G6, HQ USAREUR; the MSC, OPCON command, or attached, supporting, or tenant command G6; the USAREUR Cybersecurity Program Manager (CSPM), and the servicing NEC before using the proposed systems. This applies to fieldings initiated in the Army in Europe and those directed by higher HQ. Functional proponents are responsible for—

1. Providing early and continuing notification of proposals to field systems to the USAREUR G6; the MSC, OPCON command, or attached, supporting, or tenant command G6; and the USAREUR CSPM.

2. Coordinating with the USAREUR CSPM to ensure risk-management framework (RMF) accreditation in accordance with DOD Instruction (DODI) 8510.01.

3. Complying with the Network Enterprise Technology Command (NETCOM) Certificate of Networthiness (CON) Program.

(d) Participate in the HQ USAREUR Council of Colonels.

(e) Analyze and revise mission-related and administrative work processes, as appropriate, before making significant IT investments to support these processes.

(f) Ensure organizational compliance with USAREUR G6 or MSC, OPCON command, or attached, supporting, or tenant command G6 reporting requirements as mandated in IT capital planning and investment strategies (AR 25-1).

(g) Ensure organizations comply with the NEC information technology technical validation (IT-TV) process for new IT investments before funding execution. This also includes compliance with the USAREUR Requirements Validation System (URVS), the 2d Signal Brigade (2d Sig Bde) Contract Review Board (CRB) process, IMCOM-Europe CRB procedures, 409th Support Brigade (Contracting) (409th SB (Contracting)) procedures, and the Chief Information Officer (CIO) Information Technology Approval System (ITAS) approval process established at the Department of the Army (DA) level. All organizations that procure new IT assets (software or hardware) must collaborate with their local supporting NEC to ensure procurements are submitted through the NEC IT-TV process. New procurements must be originated through the Army Computer Hardware, Enterprise Software, and Solutions (CHESS) system and comply with the CHESS statement-of-nonavailability process, when applicable.

(2) HQ USAREUR staff offices and USAREUR MSCs will—

(a) Manage CP-34 activities in accordance with d(1)(a) and (b) above.

(b) Coordinate with the ODCS, G6, HQ USAREUR, and their servicing NEC on IT issues to ensure potential effects on ISs are considered. Subjects that require this coordination include, but are not limited to, the following:

1. Approval and Acquisition of IT Hardware, Software, and Services. HQ USAREUR staff offices and USAREUR MSCs will coordinate with the ODCS, G6, HQ USAREUR. For tactical IT requirements, HQ USAREUR staff offices and USAREUR MSCs must develop an ONS and coordinate with the USAREUR G3/5/7.

2. IT Investments. HQ USAREUR staff offices and USAREUR MSCs will ensure that all IT investments are properly registered and accounted for in the Army Portfolio Management Solution (APMS) in accordance with the guidance published at *https://intranet.eur.army.mil/hq/portfoliomgnt*. USAREUR MSCs will coordinate with the ODCS, G6, HQ USAREUR.

3. IT Actions to Ensure Interoperability and Information-Sharing Between Deployed and Garrison IT Platforms. These actions should also be coordinated with the ODCS, G3/5/7, HQ USAREUR.

4. ASIs, Security Patches, Information Assurance Vulnerability Alert (IAVA) Actions, and Remote-Services Support Actions. These actions should be coordinated with the servicing NEC and affected installation tenants using AE Form 25-1N.

(3) USAREUR OPCON commands and USAREUR attached, supporting, and tenant commands will coordinate with their respective Army command (ACOM), Army service component command (ASCC), or direct-reporting unit (DRU) G6 and their servicing NEC on IT issues to ensure potential effects on ISs are considered.

g. 7th Army Training Command (7th ATC). The combat camera (COMCAM) mission provides the CG, USAREUR, a direct imagery capability that supports operational and planning requirements during worldwide crises, contingencies, exercises, and wartime operations.

(1) In Europe, military and civilian visual information (VI) personnel assigned to the 7th ATC who have the required security clearance will provide immediate COMCAM support locally during emergencies. In support of this requirement, the 7th ATC will maintain a cadre of deployable COMCAM documentation specialists (military occupational specialty 25V) who are ready to deploy and provide support for remote or austere missions.

(2) 7th ATC VI specialists and Soldiers assigned to the United States Army Joint Multinational Readiness Center and Training Support Activity Europe (TSAE) training support centers (TSCs) theater-wide will provide documentation support until relieved by official DOD Joint Chiefs of Staff COMCAM teams.

h. 2d Sig Bde. The 2d Sig Bde—

(1) Is under USAREUR OPCON.

(2) Exercises technical-direction and configuration-management authority over Army in Europe voice networks, data networks, and enterprise application systems that support HQ USAREUR, USAREUR MSCs, USAREUR OPCON commands, and USAREUR attached, supporting, and tenant commands.

(3) Provides C4IM services to Army in Europe organizations.

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

(a) Programs such as the "Single Director of IM" concept, server consolidation, the Army Data Center Consolidation Plan, service-level management, and IT metrics are part of the strategic IT vision to sustain and run networks and IT operations in Europe more efficiently. The 2d Sig Bde coordinates ASIs, security patches, IAVA actions, and remote-service support actions with theater IT service customers.

(b) The 2d Sig Bde engineers, installs, operates, and maintains Army in Europe networks. Requests for exceptions to this requirement must be sent to the ODCS, S3, 2d Sig Bde.

(c) All projects involving the installation of cable-distribution systems or inside-plant work must meet relevant commercial standards as specified by the 2d Sig Bde.

(d) 2d Sig Bde supporting signal battalions (SSBs) and local NECs will be the local C4IM service-level managers (SLMs).

1. Local C4IM SLMs are service providers who directly interact with customers. They are primarily responsible for managing, overseeing, and delivering required C4IM services in the assigned area of responsibility (AOR).

2. The 2d Sig Bde will prepare, coordinate, negotiate, and maintain agreements for customers in AORs that receive above-baseline (reimbursable) IT services. Above-baseline services may include contracted IT support for exercises, contingency operations, or real-world missions, and IT support required outside of NEC geographical boundaries or where NEC capabilities are unresourced.

a. A Support Agreement (DD Form 1144) will be prepared for recurring and reimbursable IT services costs.

b. A service-level agreement (SLA) will be negotiated and developed to define service-delivery standards for reimbursable IT services that require additional manpower, new technologies, and new operation and maintenance services from the 2d Sig Bde and its subordinate NECs.

c. The Commander, 2d Sig Bde, is the approval authority for SLAs between the 2d Sig Bde, its SSBs and NECs, and the customers they support.

(5) Is responsible for developing and maintaining enterprise system architectures for the Army in Europe.

(a) The USAREUR G6 is responsible for consolidating operational and system-architecture requirements and overseeing the technical architecture of the DOD Information Technology Standards Registry (DISR) as it applies to the Army in Europe.

(b) HQ USAREUR staff offices, USAREUR MSCs, and IMCOM-Europe are responsible for developing and maintaining their internal architecture product sets and informing and participating in USAREUR Enterprise Architecture Working Groups.

(c) The ODCS, G3/5/7, HQ USAREUR, will work with the Programs and Policy Branch; Programs, Policy, and Projects Division; ODCS, G6, HQ USAREUR, to develop operational requirements.

(d) USAREUR MSCs will ensure that their IT projects, standards, policy, and procedures are in compliance with the DOD Architecture Framework.

(e) The Projects Branch; Programs, Policy, and Projects Division; ODCS, G6, HQ USAREUR, will develop enterprise architecture "communities of interest" and use the USAREUR Microsoft (MS) SharePoint portal to publish Army in Europe architectures, views, and standards, and to identify (in coordination with theater IT managers) the strategic vision for the enterprise architecture and how it will evolve.

i. IMOs.

(1) Newly assigned IMOs must complete IMO certification training no later than 90 days after being appointed.

(2) IMO responsibilities encompass automation, cybersecurity (CS), the IM and IT areas of communications systems and system support, and VI. IMO core duties include, but are not limited to, the following:

(a) Overseeing the content, development, and security of organizational automated applications.

(b) Developing and maintaining the organization's information resource-management program. This includes life-cycle requirements for automation and required software upgrades to ensure that all software used is in compliance with Army enterprise-licensing and security requirements.

(c) Managing and validating the organization's IM and IT requirements documents.

(d) Ensuring system and user compliance with theater-level enterprise management requirements and procedures.

(e) Coordinating with the USAREUR CSPM to ensure accreditation in accordance with DODI 8510.01.

(3) Only IMOs who have valid appointment orders (app B) on file with the servicing NEC may request IT hardware, software, network equipment, and telecommunications equipment. Telephone control officers will coordinate telecommunications requirements with their IMOs. AE Regulation 25-13 and AE Pamphlet 25-13 provide further guidance. Personnel who try to order IT equipment without the appropriate appointment orders on file will have their request returned without action. Each organization's commander (or equivalent) is responsible for ensuring current orders are on file with the servicing NEC.

(4) IMOs who require elevated privileges to serve as IMO technicians or administrators will be under the technical direction of their local supporting NEC. For these IMOs, appointment orders must also justify the need for elevated privileges.

5. IT CONTRACTS AND ACQUISITIONS

a. Planning Phase.

(1) HQ USAREUR Staff Offices and USAREUR MSCs. All USAREUR IT contract and acquisition (service and nonservice) requirements will be planned, reviewed, validated, and managed in accordance with AE Pamphlet 70-13-45, the USAREUR IT Portfolio Management (PfM) Program, and capital-planning and investment-management governance processes. The Information Technology Resource and Analysis (ITR&A) Division, ODCS, G6, HQ USAREUR, will oversee and manage the investment life cycle of IT hardware, software, and services for the European theater in accordance with the Clinger-Cohen Act of 1996, APMS requirements, and other pertinent policy guidance.

(2) USAREUR OPCON Commands and USAREUR Attached, Supporting, and Tenant Commands. These commands will coordinate with their respective ACOM, ASCC, or DRU G6 for further guidance on the planning phase.

b. Investment Phase.

(1) HQ USAREUR staff offices and USAREUR MSCs will—

(a) Identify all IT contract and acquisition (service and nonservice) requirements during annual budget lay-downs and funding reviews.

(b) Immediately identify emergent requirements.

(c) Coordinate all IT requirements with the ITR&A Division for acquisition assistance.

(2) The ITR&A Division will coordinate all IT contract and acquisition requirements with the requiring activity (RA) and the 409th SB (Contracting) and help develop acquisition strategies, procurement milestones, and required acquisition documents in accordance with AE Pam 70-13-45 for the following:

(a) All IT services, regardless of cost.

(b) All IT moratorium items, regardless of cost.

(c) Nonservice hardware and software that cost $25,000 or more.

(3) All IT procurement actions (for example, Government purchase card (GPC) purchases, military interdepartmental purchase requests, nonservice contracts) for hardware, software, telecommunications equipment, and network equipment require a NEC IT-TV unless the items are on the IT-TV exemption list and procured in accordance with the IT PfM process. The servicing NEC manages the IT-TV process. Organizations must procure IT-TV exemption-list items that cost less than $25,000 through CHESS using a GPC.

NOTE: Further guidance on the IT PfM process is available at *https://intranet.eur.army.mil/hq/portfoliomgnt*.

c. Execution Phase.

(1) Non-IT-Programmed Funds.

(a) HQ USAREUR staff offices and USAREUR MSCs will submit a request for a DA CIO/G-6 ITAS waiver for—

1. IT expenditures using operational tempo (OPTEMPO) funds, regardless of dollar thresholds.

2. All IT moratorium items (for example, servers, data centers, VTC equipment). The USAREUR IT PfM portal (*https://intranet.eur.army.mil/hq/portfoliomgnt*) lists all IT items subject to the IT moratorium.

(b) Commands under USAREUR OPCON and USAREUR attached, supporting, and tenant commands will coordinate with their respective ACOM, ASCC, or DRU G6 or business office on how to procure non-IT-programmed funds.

(2) IT Capital Asset Management.

(a) The ITR&A Division, ODCS, G6, HQ USAREUR, is responsible for ensuring that all IT investments of HQ USAREUR staff offices and USAREUR MSCs are managed through the IT PfM Program. The ITR&A Division will—

1. Serve as the IT PfM PMO for USAREUR.

2. Chair annual USAREUR IT PfM summits.

3. Ensure that portfolio owners (POs) are appointed for each mission area.

4. Ensure that USAREUR IT costs are captured in the APMS.

5. Coordinate directly with all Army in Europe organizations to review all documents that relate to the IT procurement requirement (for example, documents related to budgeting, contracting, manpower, operations, missions, planning).

6. Review and assist in the development of contract acquisition requirements.

7. Serve as the POC to the 409th SB (Contracting) for all IT contract acquisition requirements.

(b) POs will—

1. Be appointed on orders by the DCG, USAREUR.

2. Define the investment posture for their portfolios.

3. Identify domains and domain leads for their portfolios.

(c) Domain leads will—

1. Establish the investment posture for their domains in accordance with PO guidance.

2. Appoint functional PMs for their functional programs.

(d) Functional PMs will—

1. Manage investments under their functional programs.

2. Assess investments submitted for review through the URVS.

3. Publish approved hardware and software lists for their programs.

(e) RAs will—

1. Submit planned or known (recurring or new) IT requirements during annual budget lay-downs and funding reviews through the URVS for the ITR&A Division to coordinate acquisition. Emergent IT requirements must be submitted immediately.

2. Inform their POs of any IT investment changes.

3. Submit valid recurring investment requirements through the URVS for review and pre-acquisition assistance 12 months in advance of the required delivery date.

4. Submit new IT investment contract acquisition (service and nonservice) requirements through the URVS for review and pre-acquisition assistance 18 months (24 months for large or complex IT requirements) in advance of the required delivery date.

NOTE: RAs will not submit IT procurement requirements for hardware, software, or services directly to the 409th SB (Contracting) or any other contracting office.

(f) IMOs and IT technicians of requesting tactical units will closely coordinate all requirements for C4IM equipment, connectivity, and services with the servicing NEC. The NEC provides garrison-to-tactical networking and interface support and related IT services as agreed on using the DA C4IM service list, the Army in Europe Network Service Catalog, and IMCOM-Europe common levels of support. Mission-funded C4IM services will require the tactical unit to reimburse the C4IM service provider, SSB, or NEC through an SLA. Everyone involved in acquiring IT equipment and services (for example, IMOs, TCOs, contracting offices, resource-management offices) will maximize the use of DOD and other Federal contracts.

(g) The 409th SB (Contracting) will—

1. Serve as the subject-matter expert (SME) for all contract matters.

2. Help develop acquisition strategies and documents.

3. Help define procurement milestones.

NOTE: USAREUR OPCON commands and USAREUR attached, supporting, and tenant commands will coordinate with their respective ACOM, ASCC, or DRU G6 or their business office, or both, for IT capital asset management.

(3) Required Approvals. Before executing funding, HQ USAREUR staff offices and USAREUR MSCs will obtain the appropriate technical approvals (NEC IT-TV, Army command approval (URVS), or DA-level approval (ITAS waiver)) approvals for all IT investments (hardware, software, and services):

(a) A NEC IT-TV for hardware and software listed on the 2d Sig Bde exemption list.

(b) A URVS approval for—

1. Services, regardless of cost.

2. Software, regardless of cost.

3. IT moratorium items, regardless of cost.

4. Executing OPTEMPO funds, regardless of dollar thresholds.

(c) An ITAS waiver for—

1. IT moratorium items, regardless of cost.

2. Hardware, software, and services purchased with OPTEMPO funds.

3. Commercial off-the-shelf (COTS) hardware and software purchased outside of CHESS, regardless of cost.

4. Hardware, software, and services in support of a data center.

NOTE: Further guidance on the USAREUR IT approval process is available at *https://intranet.eur.army.mil/hq/portfoliomgnt*.

(4) Supporting Documents. One or more of the following supporting documents may be required for validation, depending on the service or nonservice solution:

(a) A 3- to 5-year life-cycle replacement schedule for the solution.

(b) A statement confirming that the solution is in compliance with the DISR.

(c) A statement confirming that the solution is in compliance with CS requirements.

(d) An evaluation of emerging technologies.

(e) An evaluation of new or modified requirements against existing systems.

(f) Outcome-oriented performance measurements for achieving the solution.

(g) A statement of objectives on the IT service performance work statement.

(h) An approved NEC IT-TV approval memorandum, BMC Information Technology Service Management (ITSM) validators tab, and equipment or software list.

(i) An independent Government cost estimate, a cost estimate from CHESS using the RFQ tool, or a CHESS statement of nonavailability.

(j) An analysis or print study of in-house printing requirements before requesting shared printing devices (black-and-white and color printers), multifunction printing devices, or leased copiers. The USAREUR IT PfM portal (*https://intranet.eur.army.mil/hq/portfoliomgnt*) provides more information.

(k) An approved ITAS waiver.

(5) Management of Copiers and Printing Devices. HQ USAREUR staff offices and USAREUR MSCs will appoint a copier/printing device manager and provide the manager's name to the Programs and Policy Branch; Programs, Policy, and Projects Division; ODCS, G6, HQ USAREUR. The copier/printing device manager will—

(a) Identify and manage printers, multifunction printing devices (that is, self-service copiers or printers that can be used for scanning), and other printing devices (stand-alone and those on shared networks) throughout the assigned organization.

(b) Conduct an analysis or print study on shared printing devices (black-and-white and color printers), multifunction printing devices, and leased copiers in accordance with the guidance published at *https://intranet.eur.army.mil/hq/portfoliomgnt*.

(6) The NEC IT-TV Process. The NEC IT-TV process is used to request hardware and software.

(a) IMOs will—

1. Identify hardware and software requirements and use the CHESS website (*https://chess.army.mil*) to conduct market research for requirements.

2. Submit a list of materials for all IT hardware and software requirements to their servicing NEC. In addition, an RMF assess-only process must be initiated for all software requirements.

3. Coordinate with the servicing NEC for help with the IT-TV process and market research.

(b) HQ USAREUR staff office, USAREUR MSC, USAREUR OPCON command, and USAREUR attached, supporting, and tenant command G6s and S6s will—

1. Validate and send IT requirements to the servicing NEC. (USAREUR MSCs that are serviced by multiple NECs will send their requirements to the requesting organization's NEC.)

2. Ensure that all necessary documentation is complete before sending requirements for IT equipment to the servicing NEC.

3. Ensure that IT requirements are part of the organization's modernization plan.

(c) The NEC will—

1. Ensure that all necessary documentation is complete before approving or disapproving requirements.

2. Validate, in coordination with the SME or PM, the technical solution to ensure that the requirement is in compliance with the Army Enterprise Architecture.

6. ENTERPRISE LICENSE AGREEMENT

a. HQ USAREUR staff offices and USAREUR MSCs will—

(1) Follow Enterprise License Agreement (ELA) procedures for the purchase of software and product services.

(2) Obtain authorization, in accordance with this regulation, for all software-license procurement requests, whether generated through the CHESS License Tracking System, a designated ELA vendor, or the RA S6 or IMO.

(3) Follow the procedures in CHESS for items ordered through the CIO/G6 CHESS IT Mart. The RA S6 or IMO will include his or her approved IT-TV identification (ID) number in the IT Mart "Comments" section to allow cross-referencing during the G6/G8 approval-validation process.

(a) All new users must complete a user-profile form on the Program Executive Office Enterprise Information Systems SharePoint homepage to gain access to the new SharePoint IT Mart.

(b) Users can access the IT Mart through the CHESS SharePoint portal at *https://peoeis.kc.army.mil/chess/SitePages/Home.aspx*.

(c) For items ordered through a CHESS-designated ELA vendor, the RA S6 or IMO will follow command-directed policies and procedures as well as the designated ELA vendor's ordering procedures.

(4) Maintain accountability and original product materials for all software licenses received through the ELA. Commanders will ensure that distribution does not exceed the quantities authorized or purchased and will act as auditing authorities for ELA software licenses.

(5) Ensure the reuse of available licenses before requesting and ordering new software through the ELA.

(6) Allow only IMOs who have valid appointment orders (app B) on file with the servicing NEC to request software. The appointment orders must be signed by the appointee's commander.

(7) Use the ELA as their only source for software and service products offered by the ELA.

(8) Report all software-license changes to the USAREUR ELA Manager, including, but not limited to, new licenses procured, unused and unneeded licenses released to the USAREUR inventory pool, available licenses transferred to other units, and obsolete licenses retired from their inventory pool.

b. The USAREUR G6 is the approval authority for exceptions to the policy in subparagraph a above.

c. Commands under USAREUR OPCON and USAREUR attached, supporting, and tenant commands will coordinate with their respective ACOM, ASCC, or DRU G6 for ELA policies and procedures.

7. REDISTRIBUTION AND DISPOSAL OF INFORMATION TECHNOLOGY ASSETS

Outdated, defective, and unusable COTS compact discs (CDs) will be destroyed by cutting, shredding, or breaking them and destroying the license if applicable. Each time an organization destroys CDs, the organization will prepare a statement of destruction that specifies the number of CDs that were destroyed and the date and time of their destruction. At least two persons other than the individual destroying the CDs must witness the destruction and sign the statement. The organization will then send the statement to the servicing NEC.

8. EMAIL SERVICES AND EMAIL PROTOCOL

a. Individual Official Email.

(1) Individual official email addresses (for example, *john.d.doe.mil@mail.mil*) are used by individuals to exchange routine duty-related information. The following are examples of routine information typically sent from and to individual email addresses:

(a) Coordination papers from one action officer to another.

(b) Miscellaneous documents provided for information.

(c) Documents that do not require a release or signature authority.

(2) Users are not authorized to use personal individual email accounts (for example, *doej@yahoo.com*) to send organizational email.

(3) Soldiers and DOD civilians may use official email accounts to correspond with their immediate Family at their home duty station (if they are deployed) or in CONUS. The individual's immediate Family comprises those most closely related to or designated by the Soldier or DOD civilian to receive notification in case of emergency. This includes the spouse, children, parents, a person standing in the place of a parent, persons with legal custody, adoptive and half brothers and sisters, grandparents, and persons listed on DD Form 93. Two-way correspondence between the individual and members of the individual's immediate Family is allowed.

(4) To ensure efficient use of the communications bandwidth when communicating by email, Army in Europe personnel should—

(a) Avoid sending email messages that are larger than 20 megabytes. Large email attachments should be compressed when possible. Units sending email attachments to several addressees should consider posting the attachments on a portal instead.

(b) Eliminate unnecessary and excessive graphics from presentation files before forwarding the files by email. Deleting logos and backgrounds from slides may reduce the bandwidth needed to transmit files by up to 85 percent. Logos and backgrounds should be placed on a master slide and sent separately; recipients may then apply the master slide to individual slides.

(c) Delete unnecessary information (for example, long strings of previous email messages or unrelated comments) before forwarding or replying to email messages.

(d) Not routinely use the "delivery receipt" or "read receipt" feature when sending email messages. The receipt features should be used only when the receipt of a message must be verified.

(e) Limit "To" and "courtesy copy (Cc)" addressees to those who have a need to know.

(5) The following applies to signature blocks used in official email messages in the Army in Europe:

(a) Signature blocks of military and civilian personnel will include only the sender's name, military rank if serving on active duty, title, organization, telephone number (military and civilian), fax number (if applicable), and Government email address. The signature block may include an individual's professional or educational certification (for example, Ph.D.) when dealing with foreign and high-level officials outside the DOD (AR 25-50). The signature block may optionally include the sender's location. The use of recognized unit or organizational mottos and logos (for example, "One Team!") is authorized. The use of the unit's or staff office's website URL is authorized. Personal mottos, slogans, quotes, or other forms of personalization are prohibited. This prohibition also includes the areas above and below the signature block. The following are examples of military and civilian signature blocks:

MAJ John Doe
Chief, XX Division
USAREUR G6
Bldg XX, Rm XX, Installation, USAG XX
Mil 555-1111
Fax 555-1222
NIPR: john.d.doe.mil@mail.mil
SIPR: john.d.doe.mil@mail.smil.mil
Check out our webpage at www.eur.army.mil

Mr. John Doe
Chief, XX Division
USAREUR G6
Bldg XX, Rm XX, Installation, USAG XX
Mil 555-1111
Fax 555-1222
NIPR: john.d.doe.civ@mail.mil
SIPR: john.d.doe.civ@mail.smil.mil
Check out our webpage at www.eur.army.mil

(b) Signature blocks of contractor and local national (LN) personnel must clearly indicate the contractor or LN status and must include the sender's name, the name of the contractor's firm, the name of the organization supported, location (optional), and the sender's telephone number (military and civilian), fax number (if applicable), and email address. The following are examples of contractor and LN signature blocks:

Mr. John Doe
Contractor, ABC Company
USAREUR G6
Bldg XX, Rm XX, Installation, USAG XX
Mil 555-1111
Fax 555-1222
NIPR: john.d.doe.ctr@mail.mil
SIPR: john.d.doe.ctr@mail.smil.mil

Mr. John Doe
Program Manager, XX Division
USAREUR G6
Bldg XX, Rm XX, Installation, USAG XX
Mil 555-1111
Fax 555-1222
NIPR: john.d.doe.ln@mail.mil

b. Receiving and Forwarding Unauthorized Email.

(1) The receipt of email messages is not controllable. Most Army email systems interconnect with other Government and commercial email systems. If unauthorized or illegal email messages are received, the recipient is responsible for deleting, destroying, reporting, or otherwise properly disposing of the messages to ensure they do not remain on the system.

(2) Forwarding unauthorized or illegal email messages violates Army email policy, even if the person forwarding the message is not the originator. The individual who receives the message, whether sent to an individual or organizational email address, is responsible for ensuring that only authorized and approved messages are forwarded. Chain email, horoscopes, jokes, thoughts of the day, and similar unauthorized material must not be sent or forwarded. (This policy does not apply to spiritual material sent by chaplains.)

c. Email Security.

(1) Users must comply with the security and privacy restrictions in AR 25-2 and AR 25-55 when sending email.

(2) Email must be sent and received only on systems and networks that are accredited at the level of confidentiality (or higher) of the information being transmitted.

(3) Under no circumstances will email containing classified information be sent through nonsecure, common-user email systems such as the NIPRNET.

(4) Email that contains sensitive but unclassified (SBU) information or personally identifiable information may be sent through nonsecure, common-user email systems such as the NIPRNET, provided that the message is encrypted in accordance with Public Key Infrastructure policy.

9. RESPONSIBILITY FOR VISUAL INFORMATION ACTIVITIES

a. The 7th ATC TSAE provides installation C4IM 702 baseline and mission services to organizations in the European theater in accordance with Army guidance and standing memorandums of agreement (MOAs) through a network of VI activities embedded in local TSCs and the Training Aid Production Center (TAPC). Customers will send all requests for audiovisual (AV) and VI services through the Visual Information Ordering Site (VIOS) to their local TSC. The TSC determines the most cost-effective, timely, and reliable method of service and delivery for the product or service that the customer requested. When necessary, TSCs will transfer work orders through VIOS within the 7th ATC VI network or to Visual Information Services–Europe, IMCOM-Europe. The USAREUR VI Program Manager at the 7th ATC TSAE—

(1) Analyzes requests and builds and submits management decision evaluation packages (MDEPs) to the budget analyst who handles MDEP MU1M (VI Mission Support) for USAREUR.

(2) Manages authorized TSAE VI activities within the TSCs and the TAPC. He or she also manages regional training support division VI managers and ensures appropriate staff support for those managers.

(3) Ensures that all baseline and mission services are offered to Army units and activities on Army installations in accordance with the C4IM services list, Service 702.

(4) Ensures that all above-baseline services are provided locally at the TSC or that requests for such services are forwarded to the TAPC for production, and that reimbursements for above-baseline services are obtained and properly managed.

(5) Reviews the operation of authorized USAREUR VI activities annually to determine if products and services are cost-effective and systems are being fully utilized. He or she also standardizes equipment and baseline supplies across all TSCs.

(6) Conducts or arranges for technical training for assigned VI personnel and projects, and validates annual training requirements and funding through the MU1M program objective memorandum (POM) to maintain industry standards.

(7) Implements local policy and procedures for using Army files stored at the Defense Imagery Management Operations Center (DIMOC), in the Defense Visual Information Distribution System, or at the Joint Combat Camera Command. This includes ensuring that VI personnel send all pertinent material (for example, graphics, photos, videos) to the DIMOC for permanent archiving.

(8) Plans, programs, and budgets for Operations and Maintenance, Army, resources to support VI mission requirements (for example, equipment, personnel, products, systems).

(9) Prepares directives for implementing VI policy and procedures in theater and serves as the POC for the staffing of all VI-related documents.

(10) Serves as the global administrator for the VIOS for Europe and ensures that the VIOS is implemented correctly at all authorized VI activities for the collection and reporting of all VI activity.

(11) Develops 5-year plans for acquiring VI investment systems based on HQDA strategy and in accordance with AR 25-1 and C4IM services lists. He or she also projects LCR on the MU1M POM and procures HQDA-validated AV, multimedia, and VI equipment to support the VI mission.

(a) Purchases of equipment, systems, and services must be validated and procurements must be made in compliance with AE Pamphlet 70-13-45 and the USAREUR IT PfM Program at *https://intranet.eur.army.mil/hq/portfoliomgnt*.

(b) Purchases of hardware and software of less than $25,000 (except IT moratorium items, which must be approved by the USAREUR G3/5/7 through the URVS or the established IMCOM-Europe process) must be technically validated by the local NEC. In addition, a DA CIO/G-6 ITAS waiver may be required if IT equipment is procured outside of CHESS as outlined in AR 25-1, chapter 3.

(c) Purchases of hardware and software of $25,000 or more must be technically validated by the local NEC and submitted through the URVS to obtain USAREUR G3/5/7 approval before procurement. In addition, an ITAS waiver may be required as outlined in AR 25-1, chapter 3.

(d) After approval is obtained, equipment of less than $50,000 may be procured locally or referred to the Television-Audio Support Activity (T-ASA), DOD Media Center, in Riverside, California. Equipment that costs $50,000 or more must be procured by the T-ASA in accordance with DA Pam 25-91, chapter 3, paragraph 8-3.

(e) Under host-nation law, ergonomic requirements must be considered when purchasing and installing equipment. Systems will be installed to meet the ergonomic requirements of users.

(12) Validates all theater VI and AV purchases in Europe, regardless of cost, using the technical validation system in Europe through ITSM. This will help enforce USAREUR G6 and DOD guidance on reducing unauthorized VI activities and shadow VI and AV facilities that do not maintain a Defense Visual Information Activity Number.

(13) Screens and validates all USAREUR external requests for VI support through the URVS for regulatory compliance, accuracy, and economy in accordance with the VI service MOA between IMCOM-Europe and USAREUR.

(a) Army multimedia and visual-information (M/VI) activities and tenant units in Europe will use the networking component of the VIOS to acquire and track VI products and services. All VIOS requests must be initiated at the customer's local supporting TSC for approval or routing. When the USAREUR G3/5/7 issues a task order for an event that requires VI support, all VIOS requests for that event, regardless of their sources, will be forwarded to the formally tasked VI supporting unit for coordination, approval or disapproval, and execution if approved.

(b) DODI 8510.01 requires certification and accreditation of all DOD ISs (stand-alone and closed restricted networks) used in VI. Graphic- and video-production systems are categorized as stand-alone ISs that may be used in a closed restricted network. M/VI activities will coordinate certification of their graphic- and video-production systems through their supporting ISSM.

(c) The highest priority for VI documentation is to capture imagery that depicts subjects of known or probable interest to the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, or more than one DOD component. DOD 5040.6-M-1 provides additional information.

1. Examples of top-priority imagery include the following:

a. Current operations.

b. Contingency operations.

c. Major exercises, especially joint and combined exercises.

d. Deployment and redeployment of troops, equipment, and weapons systems.

e. Weapons systems in use (especially new systems).

f. Significant events happening in the USEUCOM AOR that would be of interest to higher HQ.

g. Major accidents.

h. Major construction projects, from start to finish.

i. Good images of daily life in the military, particularly in the lives of deployed Soldiers.

j. Memorials.

k. Change-of-command and assumption-of-command ceremonies for officers in the grade of colonel or higher.

l. Distinguished visitors and dignitaries (for example, heads of state, senior U.S. Government or Army officials).

2. When requested, TSCs will document local events such as promotions and retirement ceremonies on a case-by-case basis if staffing and the TSC mission allow. These types of events are normally considered a self-help service. The imagery will generally not be accessioned to the DIMOC unless there is significant interest to justify accessioning.

3. Time-sensitive imagery will be accessioned to the DIMOC within 72 hours after the event. Non-time-sensitive imagery will be accessioned to the DIMOC within 10 days after the event.

4. All imagery captured and processed by VI activities will contain a proper VI record information number using a vision ID (*https://vipro.defenseimagery.mil/*) with the .jpg file extension and a caption or shot sheet, as appropriate, in accordance with DODI 5040.02. A copy will be stored locally.

5. All captions will be created in accordance with the most current DOD VI Style Guide, which is available at *https://www.dimoc.mil/VI-Training/DoD-VI-Style-Guide/*.

6. Only public affairs officers (PAOs) responsible for the supported unit have release authority for VI imagery, media, and captions. PAOs must screen content for web, print, radio, and video media to be released to the public. VI activities will not publicize imagery that does not include proper releasing instructions.

7. AR 25-1, paragraph 2-3, provides guidance on COMCAM support.

10. CYBERSECURITY

a. As the USAREUR authorizing official (AO), the USAREUR G6 will appoint a CSPM in writing. The USAREUR CSPM will establish, manage, and assess the effectiveness of all aspects of the Army in Europe Cybersecurity Program (AE CS Program). The CSPM is also the agent for the Security Controls Assessor (SCA) for Army in Europe systems and networks.

b. HQ USAREUR staff offices and USAREUR MSCs will implement CS programs in accordance with AR 25-2; Army in Europe policy; and tactics, techniques, and procedures provided by the USAREUR CSPM.

c. Acquisitions supporting the AE CS Program must comply with DISR standards. Evaluations of acquisitions for DISR compliance will be conducted within the framework of USAREUR IT technical evaluations.

11. INFORMATION TECHNOLOGY SUPPORT SERVICES FOR ARMY ORGANIZATIONS ON ARMY INSTALLATIONS

a. Responsibility. In the European theater, the RCC-E is responsible for the regional oversight of local data networks that are connected to Defense Information Systems Agency networks. NECs are responsible for administrating and managing the Installation Campus Area Network (ICAN).

b. Remote Access. A "remote user" is a person who enters the Army in Europe NIPRNET from outside the physical or logical boundary of the internal local area network (for example, for telework purposes). The remote-access system creates a protected extension of the Army in Europe NIPRNET for authorized remote users. Non-Government-furnished equipment is not authorized to be remotely connected to the Army in Europe NIPRNET.

(1) The 2d Sig Bde will—

(a) Facilitate virtual private network (VPN) services for Army in Europe networks (AE Form 25-1J).

(b) Manage all remote-access points.

(c) Configure all remote-access equipment to require authentication using common access cards and encryption.

(2) If the approving authority determines that an individual needs remote access, the authority must provide a Government-owned IS or solution. The remote-access user and the responsible IMO, IAM, or IASO will complete AE Form 25-1K to ensure that the Government-owned IS to be used for remote access is correctly configured. Also, home-station remote-access users (teleworkers) will not be reimbursed any phone costs or issued Government-purchased or -owned commercial mobile devices, since users are normally able to go to their offices to use telephone support.

c. Compatibility and Compliance of Automation Equipment. Army organizations in Europe will—

(1) Ensure automation equipment and software that is developed, procured, or acquired is compatible and compliant with Internet Protocol version 6 (IPv6).

(2) Request an exception to policy (ETP) from the USAREUR G6 if they have an operational requirement to retain non-IPv6-compatible equipment. The request must justify the operational need for the non-IPv6-compatible equipment and provide details about the organization's plan to transition to an IPv6-compatible system. Requests for an ETP must be routed through the user's servicing NEC to the Programs, Policy, and Projects Division, ODCS, G6, HQ USAREUR.

(3) Not transition to IPv6 without approval from the USAREUR G6. The servicing NEC will send all customer requests for transition to IPv6 to the USAREUR G6. Once approved, the 2d Sig Bde will provide an implementation plan in coordination with NETCOM.

d. IT Service Request Process.

(1) All requests for new IT services must be submitted as change requests (CRQs) using BMC ITSM, which is NETCOM's enterprise service management tool that is used globally for submitting, processing, and tracking requirements for new IT services.

(2) IMOs or authorized personnel who submit CRQs for their command or activity must have a BMC ITSM user account. To obtain an account, IMOs and authorized personnel must submit a request to the ESD at *http://www.119.army.mil/* with a completed DD Form 2875 attached. The ESD can also be reached by telephone dialing 119.

(3) NEC change managers receive and process CRQs submitted by customers in the NEC's area of operation. NECs will conduct a local business assessment to determine if the requested services can be provided locally or at the theater level. NECs will forward IT service requests that require theater-level action or resources to the 2d Sig Bde IT Service Management Office. The Theater IT Service Request Policy on the 2d Sig Bde portal provides detailed information regarding the IT service request process.

e. Requirements for Floor Space Intended for IT Systems.

(1) Army organizations in Europe will not purchase servers without an approved ITAS waiver or an ITAS approval.

(2) Before an organization may connect any device to the Army in Europe network, the device must be scanned and be part of a system with an authorization to operate or an authorization to connect. Organizational ISSMs must conduct certification testing and prepare RMF certification documentation. Certification testing is required to ensure that the Army in Europe computer-security baseline, service packs, critical updates, standard technical implementation guidelines, and all corrective actions identified in information assurance vulnerability bulletins (IAVBs) have been applied to the server. Test results must be included in the organization's RMF documentation and provided to the Assessment and Accreditation Branch, Cybersecurity Division (CSD), ODCS, G6, HQ USAREUR, for review and acceptance by the Security Control Assessor-Validator (SCA-V) Lead.

(a) The SCA-V Lead will submit the documentation to the AO for acceptance of residual risks and formal approval to connect to the network. The Army in Europe CSPM and the servicing NEC can provide technical assistance on certification testing and the accreditation process. Units must plan on up to 10 weeks for the CSPM to complete certification testing and for processing and forwarding RMF documentation to the AO. Units must create a plan of action and milestones that identifies their way forward for all noncompliances and submit the plan to the program ISSM within 6 weeks, allowing up to 10 weeks to obtain the AO's signature.

(b) If a server must be connected to meet urgent operational warfighting requirements, the requesting unit must submit justification and supporting documentation to the USAREUR CSPM for CSD and AO review and determination of connection. Units will not connect a server without AO approval.

(c) No Army in Europe organization may activate a server without approval from the 2d Sig Bde Enterprise Change Management Board.

(d) Organizations that have hardware systems that are not capable of operating under the latest operating system (OS) as established by the United States Army Cyber Command and the 2d Sig Bde must submit a request for an ETP to the CSD. The request must fully justify why the old OS must remain in use and provide the timeline expected to upgrade the OS to the current baseline.

(3) After a server has been connected to the Army in Europe network, the CSPM Information Infrastructure Assessment Team will make periodic inspections to ensure that regulatory guidelines are followed. In addition, the RCC-E will periodically conduct random network scans to verify server compliance and quarantine any servers that are not in compliance. Organizations that own servers are responsible for taking the necessary steps to reestablish compliance for any quarantined systems.

f. Army in Europe Knowledge Management (KM) NIPRNET and SIPRNET Portals.

(1) The ODCS, G6, HQ USAREUR, has established Army in Europe KM NIPRNET and SIPRNET portals as adjuncts to AKO and DKO. The URL for the NIPRNET portal is *https://intranet.eur.army.mil/Pages/Welcome-Page.aspx*, and the URL for the SIPRNET portal is *http://portal.eur.army.smil.mil*. The portals are used primarily as business tools that allow individuals to share information and collaborate. Additionally, they are used as tools to help evaluate and refine business processes in order to maximize customer support while minimizing the consumption of resources required for delivering products or services. The KM portals also allow for a more efficient use of bandwidth by storing large files on the portals instead of sending them as attachments through email. Senders need to include only the URL for the required file in their email message, and the recipient will be able to go straight to the document stored on the portal. KM improves the ability of all Army in Europe organizations to collaborate with one another, share information in a timely manner, and maintain an orderly structure.

(2) The Headquarters Support Division (HSD), ODCS, G6, HQ USAREUR, manages the KM NIPRNET and SIPRNET portals. The HSD performs daily operations, maintenance, and patching of the portals, assists customers with new requirements, and coordinates outage response actions.

(3) The Office of Knowledge Management (OKM), Office of the Chief of Staff, HQ USAREUR, is the owner of the system that supports the KM NIPRNET and SIPRNET portals and manages front-end services. All new requirements must be submitted to the OKM.

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

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

Chairman of the Joint Chiefs of Staff Instruction 6211.02D, Defense Information Systems Network (DISN) Responsibilities

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

AR 25-1, Army Information Technology

AR 25-2, Information Assurance

AR 25-50, Preparing and Managing Correspondence

AR 25-55, The Department of the Army Freedom of Information Act Program

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

AR 71-9, Warfighting Capabilities Determination

DA Pamphlet 25-91, Visual Information Procedures

AE Regulation 1-10, Staff Procedures

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

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

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

SECTION II
FORMS

DD Form 93, Record of Emergency Data

DD Form 1144, Support Agreement

DD Form 2875, System Authorization Access Request

AE Form 1-10A, Staff Action Summary

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

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

AE Form 25-1N, Authorized Service Interruption Request Form

AE Label 25-1A, Leased Copier Service Instructions

APPENDIX B
FORMAT FOR AN FOR INFORMATION MANAGEMENT OFFICER APPOINTMENT MEMORANDUM

Letterhead

Office Symbol *Date*

MEMORANDUM FOR *Local Director of Information Management*

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

1. Effective *date*, I appoint the below-named individual as an information management officer (IMO) for the *organization/unit*.

a. IMO Name:
Grade:
DEROS:
Military occupational specialty:
Civilian job specialty code:
Contractor (yes/no):

b. Organization:
Unit's parent command (USAREUR major subordinate command):
Unit's Department of Defense activity address code (DODAAC):
Supporting network enterprise center:
City/Country:
Kaserne:
SBU telephone number:
DISA enterprise email address (unclassified):

c. Additional Information:
Authorized to submit IT acquisition requests (yes/no):
Authorized to submit requests for Microsoft enterprise licenses (yes/no):
Agreement products (yes/no):

2. Authority: AR 25-1 and AE Regulation 25-1, Army in Europe Information Technology.

3. Purpose: To perform IMO duties according to AE Regulation 25-1.

4. Special Instructions:

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

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

c. Newly assigned IMOs must complete IMO certification training within 90 days after being appointed.

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

CF:
USAREUR CSPM
Appointee

GLOSSARY

SECTION I
ABBREVIATIONS

2d Sig Bde	2d Signal Brigade
7th ATC	7th Army Training Command
409th SB (Contracting)	409th Support Brigade (Contracting)
ACOM	Army command
AE	Army in Europe
AE-ITT	Army in Europe Information Technology Training
AEPUBS	Army in Europe Library & Publishing System
AKO	Army Knowledge Online
AO	authorizing official
AOR	area of responsibility
APMS	Army Portfolio Management Solution
AR	Army regulation
ASCC	Army service component command
ASI	authorized service interruption
AV	audiovisual
C4IM	command, control, communications, computers, and information management
CD	compact disk
CHESS	Computer Hardware, Enterprise Software, and Solutions
CIO	chief information officer
COMCAM	combat camera
CONUS	continental United States
CoS, HQ USAREUR	Chief of Staff, Headquarters, United States Army Europe
COTS	commercial off-the-shelf
CP	career program
CRB	Contract Review Board
CRQ	change request
CS	cybersecurity
CSD	Cybersecurity Division, Office of the Deputy Chief of Staff, G6, Headquarters, United States Army Europe
CSPM	Cybersecurity Program Manager
DA	Department of the Army
DD	Department of Defense [form]
DCG, USAREUR	Deputy Commanding General, United States Army Europe
DIMOC	Defense Imagery Management Operations Center
DISR	Department of Defense Information Technology Standards Registry
DKO	Defense Knowledge Online
DOD	Department of Defense
DODI	Department of Defense instruction
DRU	direct-reporting unit
ELA	Enterprise License Agreement
ESD	Enterprise Service Desk
ETP	exception to policy
GPC	Government purchase card

HQ	headquarters
HQDA	Headquarters, Department of the Army
HQ USAREUR	Headquarters, United States Army Europe
HSD	Headquarters Support Division, Office of the Deputy Chief of Staff, G6, Headquarters, United States Army Europe
IAVA	information assurance vulnerability alert
ID	identification
IM	information management
IMCOM-Europe	United States Army Installation Management Command Europe
IMO	information management officer
IPv6	Internet Protocol version 6
IS	information system
ISSM	information systems security manager
IT	information technology
ITAS	Information Technology Approval System
ITSM	[BMC] Information Technology Service Management
IT-TV	information technology-technical validation
KM	knowledge management
LCR	life-cycle replacement
LN	local national
M/VI	multimedia and visual information
MDEP	management decision evaluation package
mil	military
MOA	memorandum of agreement
MS	Microsoft
MSC	major subordinate command
NEC	network enterprise center
NETCOM	Network Enterprise Technology Command
NIPRNET	Nonsecure Internet Protocol Router Network
ODCS	office of the deputy chief of staff
OKM	Office of Knowledge Management, Office of the Chief of Staff, Headquarters, United States Army Europe
ONS	operational needs statement
OPTEMPO	operational tempo
OS	operating system
PAO	public affairs officer
PfM	portfolio management
PM	program manager
PMO	program management office
PO	portfolio owner
POC	point of contact
POM	program objective memorandum
RA	requiring activity
RCC-E	Regional Cyber Center–Europe
RMF	risk-management framework
SBU	sensitive but unclassified
SCA-V	Security Control Assessor-Validator
SIPRNET	Secure Internet Protocol Router Network
SLA	service-level agreement

SLM	service-level manager
SME	subject-matter expert
SSB	supporting signal battalion
T-ASA	Television-Audio Support Activity
TAPC	Training Aid Production Center
TSAE	Training Support Activity Europe
TSC	training support center
URL	Uniform Resource Locator
URVS	United States Army Europe Requirements Validation System
U.S.	United States
USAG	United States Army garrison
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
VI	visual information
VIOS	Visual Information Ordering Site
VTC	video-teleconference

SECTION II
TERMS

Army in Europe
All United States Army units in the United States European Command area of responsibility