Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command
Directorate-Europe
Sembach, Germany

Army in Europe
Supplement 1 to AR 25-1*

21 November 2016

Information Management

Army Information Technology

***This supplement supersedes AE Supplement 1 to AR 25-1, 30 July 2014.**

For the Commander:

MARKUS T. LAUBENTHAL
Brigadier General, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This supplement prescribes policy and assigns responsibilities for information management (IM) and information technology (IT) management for the Army in Europe.

Summary of Change. This revision—

● Updates organization names, office symbols, telephone numbers, and other administrative information throughout.

● Clarifies IT responsibilities for the Army in Europe (para 2-32) and provides a sample format for the information management officer appointment memorandum (fig 1).

● Updates IT acquisition and lifecycle-management processes (paras 3-2, 3-3, and 3-4b, d, l, and s).

● Provides guidelines for formatting signature blocks in e-mail messages (subparas 4-1f(7)(e) and (f) and figs 2 and 3).

● Updates visual information (VI) services policy and procedures (subparas 5-3b(13) thru (21)).

● Prescribes a new label, AE Label 25-1A, and procedures for coordinating support services for leased copiers (para 5-5e).

● Rescinds AE Form 25-1A and AE Form 25-1L.

● Removes the prescribing authority for AE Form 25-1M and transfers that authority to AE Supplement 1 to AR 25-13, which prescribes AE Form 25-13A and supersedes AE Form 25-1M.

● Removes the prescribing authority for AE Form 25-1D, AE Form 25-1F, and AE Form 25-1G and transfers that authority to AE Pamphlet 25-13, which prescribes AE Form 25-13B, AE Form 25-13C, and AE Form 25-13D and supersedes AE Form 25-1D, AE Form 25-1F, and AE Form 25-1G, respectively.

Applicability. This supplement applies to all DOD and non-DOD organizations that use Army in Europe networks (including all Army in Europe organizations).

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 and AE Regulation 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 supplement 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 supplement prescribes AE Form 25-1H, 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://aepubs.army.mil/*.

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

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

AR 25-1, 25 June 2013, is supplemented as follows:

Contents

Add the following to the chapter 2 list:

Add the following after the list of appendixes:

Figures

Paragraph 2-1, The Army Chief Information Officer/Deputy Chief of Staff, G-6. Add the following to subparagraph c(16):

The Assistant Deputy Chief of Staff, G6, USAREUR, is the proponent for Career Program-34 (CP-34) for USAREUR information management (IM) and information technology (IT) professionals.

(a) HQ USAREUR staff principals and commanders of USAREUR major subordinate commands (MSCs) with IM or IT professionals authorized or assigned to their staffs or subordinate organizations will—

1. Appoint a CP-34 activity manager and send a copy of the appointment memorandum to the USAREUR CP-34 Program Management Office (PMO), Office of the Deputy Chief of Staff (ODCS), G6, HQ USAREUR.

2. 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.

3. Ensure organizational CP-34 activity managers review the individual development plans of IM and IT professionals in their organizations each year to ensure the plans meet the professional-development guidelines issued by the USAREUR CP-34 PMO.

(b) USAREUR specialized commands and other USAREUR-affiliated organizations will comply with the policy and procedures of their parent higher headquarters for the management of CP-34 professionals, but should also inform the USAREUR CP 34 PMO about their organization's training requirements to gain theater efficiencies when possible.

Paragraph 2-3, The U.S. Army Network Enterprise Technology Command. Add the following to subparagraph n:

The combat camera (COMCAM) mission provides the commander a direct imagery capability that supports operational and planning requirements during worldwide crises, contingencies, exercises, and wartime operations. In Europe, military and civilian visual information (VI) personnel assigned to the Seventh Army Joint Multinational Training Command (JMTC) who have the necessary level of security clearance will also provide immediate supplementary COMCAM support locally during emergencies. In support of this requirement, the JMTC will—

(1) Maintain a cadre of deployable COMCAM documentation specialists (military occupational specialty 25V) among its assigned personnel who are ready to deploy and provide support for remote or austere missions. The cadre personnel may be among those assigned to the United States Army Joint Multinational Readiness Center or one of the theater-wide Training Support Activity Europe (TSAE) training support centers (TSCs).

(2) Provide COMCAM documentation support when required using JMTC cadre (VI specialists, VI Soldiers, or both) until relieved by an official DOD Joint Chiefs of Staff COMCAM team.

Paragraph 2-3, The U.S. Army Network Enterprise Technology Command. Add subparagraph s as follows:

s. The 5th Signal Command (5th Sig Cmd), under the operational control of USAREUR, exercises authoritative network operations, technical direction, and configuration-management authority for voice and data networks in the Army in Europe. In addition, 5th Sig Cmd provides installation-level command, control, communications, computers, and information management (C4IM) baseline services to Army organizations in the European theater in accordance with Army guidance.

Paragraph 2-27, Commanders or directors of major subordinate commands; field-operating agencies; and separately authorized activities, tenant, and satellite organizations. Add subparagraphs c through e as follows:

c. HQ USAREUR staff offices and USAREUR MSCs will—

(1) Develop an operational needs statement for tactical IT requirements and coordinate with the USAREUR G3/5/7, which will coordinate with the USAREUR G6 before any acquisition is finalized.

(2) Ensure all IT investments are properly accounted for in the Army Portfolio Management Solution (APMS) in accordance with the basic AR, paragraph 3-4d(1) and (5), and this supplement paragraph 3-4d(7), by registering IT investments in the APMS according to the procedures in the basic AR, appendix B, and the current USAREUR procedures (available at *https://intranet.eur.army.mil/hq/portfoliomgnt*).

(3) Coordinate with their servicing network enterprise center (NEC) and the USAREUR G6 about IT issues to ensure potential effects on information systems (ISs) are considered. Subjects that require this coordination include, but are not limited to approval and acquisition of IT hardware, software, and services as well as the specific types of actions identified in (4) and (5) below.

(4) Coordinate IT actions that affect the interoperability and information-sharing between deployed unit and garrison IT platforms. These type of actions should be coordinated through the S6 or G6 of the USAREUR MSC or specialized command, if applicable, and with either the USAREUR G6 or the Office of the Assistant Chief of Staff, G6, ID-E, as well as the servicing NEC and the USAREUR G3/5/7.

(5) Coordinate all authorized service interruptions (ASI), security patches, information assurance vulnerability alert (IAVA) actions, and remote-services support actions before executing them. These types of actions should be coordinated with the servicing NEC, which will coordinate with the affected installation tenants. Requesters may initiate this coordination by sending a completed AE Form 25-1N directly to the NEC or to the NEC through the 119 ticket system or through the 5th Sig Cmd representative at the USAREUR Combined Operations and Intelligence Center.

(a) Routine ASIs must be approved on AE Form 25-1N by a major or higher-graded officer or civilian equivalent in the chain of command.

(b) Other than routine ASIs must be approved on AE Form 25-1N by a colonel or higher-graded officer or civilian equivalent in the chain of command.

d. USAREUR specialized commands and all other DOD or non-DOD organizations that use Army in Europe networks will—

(1) Comply with the policy and procedures in AR 25-1, paragraph 3-4d, and their parent higher headquarters for tactical IT requirements and accounting for IT investments (for Army organizations this includes accounting for IT requirements and IT investments in APMS).

(2) For IT actions or issues that could affect the Army in Europe network, as described in c(4) and (5) above, coordinate with the USAREUR G6 and other applicable agencies as stated above.

(3) Coordinate with the S6 or G6 of their parent higher headquarters and their servicing NEC for any other IT issues to ensure potential effects on the Army in Europe network and ISs are evaluated.

e. The 5th Sig Cmd—

(1) Is under the operational control of USAREUR and assigned to the United States Army Network Enterprise Technology Command (NETCOM).

(2) Exercises NETCOM technical-direction and configuration-management authority (through its supporting signal battalions (SSBs) and NEC chiefs) over the Army in Europe voice networks, data networks, and enterprise-application systems that support HQ USAREUR, USAREUR MSCs, USAREUR specialized commands, and other USAREUR-affiliated organizations.

NOTE: 5th Sig Cmd's subordinate SSBs will designate the NEC chief for each United States Army garrison (USAG) area of responsibility that they support.

(3) Provides C4IM services to Army in Europe organizations. This includes, but is not limited to, all of the following:

(a) Exercises oversight of key C4IM service-providing facilities for the Army in Europe. This oversight includes maintaining installation processing nodes, staffing the Enterprise Service Desk, and managing the Regional Cyber Center-Europe (RCC-E).

(b) Managing other theater-wide programs that are part of the strategic IT vision to sustain and run networks and IT operations in Europe more efficiently, such as the Single Director of IM Concept, server consolidation, the Army Data Center Consolidation Plan, service-level management, and IT metrics.

(c) Coordinating ASIs, security patches, IAVA actions, and remote-service support actions with theater IT-service customers.

(d) Engineering, installing, operating, and maintaining installation networks.

1. All projects involving the installation of cable-distribution systems or inside-plant work must meet relevant commercial standards as specified by 5th Sig Cmd.

2. Any requests for an exception to this requirement must be sent to the ODCS, G3, HQ 5th Sig Cmd.

(e) Identifying and establishing local C4IM service-level managers. 5th Sig Cmd's subordinate SSBs and local NECs will be the local C4IM service-level managers. Local C4IM service-level managers are primarily responsible for the management, oversight, and delivery of required C4IM services in the assigned area of responsibility and will—

1. Be the service providers who directly interact with customers.

2. Prepare, coordinate, negotiate, and maintain service-level agreements (SLAs) for all customers in their area of responsibility who receive baseline and above-baseline IT support services. For above-baseline IT support services, an interservice support agreement (DD Form 1144) must be negotiated to specify the requirements for recurring and reimbursable support costs. The Commander, 5th Sig Cmd, is the approval authority for all SLAs between 5th Sig Cmd SSBs, local NECs, and the customers they support.

(4) Develops and maintains enterprise system architectures for the Army in Europe in coordination with the USAREUR G6 and other Army in Europe organizations as specified in (a) through (e) below.

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

(b) The USAREUR G6 is responsible for consolidating operational and system-architecture requirements and managing the technical architecture of the Department of Defense Information Technology Standards Registry (DISR) for the Army in Europe.

(c) The Enterprise Architecture Branch; Programs, Policy, and Projects Division; ODCS, G6, HQ USAREUR, will develop enterprise architecture "communities of interest" and use the USAREUR SharePoint portal to publish Army in Europe architectures, views, and standards. The Enterprise Architecture Branch (EAB), in coordination with theater IT managers, will also identify the strategic vision to provide guidance on how the enterprise architecture will evolve.

(d) HQ USAREUR staff offices, USAREUR MSCs, ID-E, and the USAGs in Europe are responsible for developing and maintaining their internal architecture-product sets in coordination with the EAB by informing and taking part in the appropriate USAREUR Enterprise Architecture Working Groups.

(e) USAREUR specialized commands and other organizations that use Army in Europe networks (for example, Army in Europe tenant units, DOD organizations, non-DOD organizations) will ensure their IT projects, standards, policy, and procedures comply with the DOD Architecture Framework and their parent higher headquarters guidance, while informing and coordinating with the appropriate USAREUR Enterprise Architecture Working Groups, as required.

Chapter 2, Responsibilities. Add paragraph 2-32 as follows:

2-32. Army in Europe Responsibilities
In addition to the responsibilities prescribed in the basic AR, the following responsibilities apply to the Army in Europe:

a. Chief of Staff, HQ USAREUR. The Chief of Staff (CoS), HQ USAREUR, or the CoS's designee (authority delegated in writing) 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 supplement if authority for the particular policy has not been delegated to the USAREUR G6.

b. HQ USAREUR Staff Principals and Commanders of USAREUR MSCs and USAREUR Specialized Commands. USAREUR staff principals and commanders of USAREUR MSCs and specialized commands will—

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

(a) The appointment memorandum must be signed by a commander or staff principal who is a colonel or higher or the civilian equivalent and a copy must be sent to the local NEC. Figure 1 provides a sample memorandum format (also available at *https://intranet.eur.army.mil/hq/portfoliomgnt* under the *USAREUR* tab on the right-hand side as an MSWord template).

1. Each organization's commander (or equivalent) is responsible for ensuring current orders are on file with the servicing NEC; otherwise, acquisitions may be returned without action ((c)6 below) and other services may not be available.

2. If the commander is not present because of an exercise or deployment, a representative authorized to sign for the commander may sign the appointment order.

3. Appointment orders will remain in effect for no longer than 1 year (existing appointments may be renewed annually) or until the IMO is officially relieved or released from the appointment in writing, whichever occurs first.

(b) Newly assigned IMOs must complete IMO certification training no later than 90 days after being appointed. IMOs should contact the Army in Europe Information Technology Training office (*https://aeitt.ext.eur.army.mil*) for available training in their area. IMO responsibilities encompass automation, information assurance (IA), the IM and IT areas of communications systems and system support, and VI. IMO core duties include, but are not limited to, the following:

1. Managing the content and overseeing the development and security of the organization's automated applications.

Letterhead

OFFICE SYMBOL Date

MEMORANDUM FOR

Mr. John Doe, Unit 23333, APO AE 09000-3333
Ms. Jane Doe, Unit 23333, APO AE 09000-3333
Commander, 2d Sig Bde (AEIM-IM) Unit 23333, APO AE 09000-3333 *(local director of information management)*
Commander, 44th Sig Bn (NEC), Unit 21111, APO AE 09096-1111 *(servicing Network Enterprise Center)*

SUBJECT: Designation of Information Management Officers for the3d Battalion, 2d Signal Brigade *(unit name)*

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

2. Purpose: To appoint information management officers (IMOs) to perform duties according to the reference.

3. Effective immediately, I appoint the following individuals as the primary and alternate IMOs for *(organization or unit name)* the 3d Battalion, *(higher HQ name)* 2d Signal Brigade, and grant them the additional information technology (IT) authorizations as identified in the table below.

Appointed IMOs								
Duty	**Name** (First MI. Last)	**Grade**	**DEROS**	**OCC Code[1]**	**Contractor** (yes or no)	**Authorizations[2]** (yes or no) **A**	**B**	**C**
Primary:	John M. Doe	CPT	DD MMM YY	13D	No	Yes	Yes	Yes
Telephone (mil):		565-1001		**E-mail:**	john.m.doe.mil@mail.mil			
Alternate:	Jane R. Doe	GS-11	DD MMM YY	1301	No	Yes	No	No
Telephone (mil):		565-1001		**E-mail:**	jane.r.doe.civ@mail.mil			
NOTEs: 1. Occupation (OCC) code: use military occupational specialty (MOS) or civilian occupation code, as applicable. **2.** Authorizations are: A–Submit IT acquisition requests, B–Submit Microsoft enterprise-license requests, and C–Sign agreement products. Answer *Yes* or *No* in each column.								

4. Organization Information. The following table identifies this unit's USAREUR major subordinate command (MSC) or specialized command, Department of Defense activity address code (DODAAC), supporting network enterprise center (NEC), and location (kaserne or post, city, and country)**:**

Organizational Information for 3d Bn, 2d Sig Bde					
MSC	**DODAAC**	**NEC**	**Location:**		
			Post	**City**	**Country**
5th Sig Cmd	WZZZZZ	44th Sig Bn	Clay Kaserne	Wiesbaden	Germany

5. Special Instructions. The appointee must have a good understanding of DOD, Army, and Army in Europe IT policy (to include IT acquisition policy and procedure) and a working knowledge of IT principles, techniques, hardware, and software. Newly assigned IMOs must complete IMO-certification training within 90 calendar days after their appointment. Appointees may contact the local Army Europe Information Technology Training Office (*https://aeitt.ext.eur.army.mil*) for information about available courses and the registration procedures.

6. This appointment supersedes all previous appointments, is effective immediately, and remains in effect for 1 year from the date signed or until appointees are officially relieved or released in writing, whichever occurs first.

FIRST MI LAST
RANK, BR *(delete line if civilian)*
Commander or director (colonel, GS-15, or higher)

CF:
USAREUR G6 (AEIM-IAPM)

Figure 1. Sample Format for an IMO Appointment Memorandum

2. Developing and maintaining the organization's IT 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.

3. Managing and validating the organization's IM and IT requirements documents.

4. Ensuring system and user compliance with theater-level enterprise management requirements and procedures.

5. Coordinating with the USAREUR Information Assurance Program Manager (IAPM) in the Cybersecurity Program Management Division, ODCS, G6, HQ USAREUR, to ensure accreditation is completed in accordance with Department of Defense Instruction (DODI) 8510.01.

6. Ensuring organizational policy and procedures allow only IMOs with valid appointment orders on file at the servicing NEC to request IT hardware, software, network equipment, and telecommunications equipment. Personnel without appropriate appointment orders on file at the NEC who try to order IT equipment will have their request returned without action. Telephone control officers must also coordinate telecommunications requirements with the servicing NEC through their IMOs.

(2) Designate an organizational information assurance manager (IAM) to perform the responsibilities listed in AR 25-2.

(3) Coordinate an analysis of proposed fielding of any new ISs (usually, proposed by system program managers (PMs)) with the USAREUR G6, the S6 or G6 at the applicable USAREUR MSC or specialized command, the USAREUR IAPM, and the servicing NEC before using the new IS. This applies to the fielding of ISs that are initiated by Army in Europe (organic or tenant) organizations as well as those directed by a higher headquarters. Functional proponents are responsible for—

(a) Providing early and continuing notification to the USAREUR G6, the S6s or G6s at USAREUR MSCs and specialized commands, and the USAREUR IAPM of proposals to field systems.

(b) Coordinating with the USAREUR IAPM to ensure completion of risk-management-framework (RMF) accreditation.

(c) Complying with the NETCOM Networthiness Certification Program.

(4) Send a representative to take part in HQ USAREUR councils of colonels that are addressing IT or IM issues.

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

(6) Ensure their organization complies with Army IT management planning and investment strategies and reporting requirements (basic AR, paras 3-2 and 3-3). HQ USAREUR staff offices and all USAREUR units will also comply with applicable USAREUR G6 and, if applicable, USAREUR MSC S6 or G6 implementing guidance. USAREUR specialized commands and other USAREUR-affiliated organizations will also comply with the implementing guidance of their parent higher headquarters through their designated processes.

(7) Ensure their organization's IT investment actions are in compliance with applicable standards before committing or obligating funds. Organizations must obtain the appropriate approvals for all IT investments before processing the investment action. Appropriate approvals include all of the following:

(a) Information technology technical validation (IT-TV) (that is, for all Army in Europe network users, a NEC approval or NEC IT-TV).

(b) Army agency or command approval (that is, for USAREUR units: approval in the United States Army Europe Requirements Validation System (URVS); for 5th Sig Cmd: 5th Sig Cmd Contract Review Board approval; for ID-E, the ID-E Contract Review Board approval; and for other commands, approval from their parent higher headquarters).

(c) HQDA approval (that is, an Army Chief Information Officer (CIO) Goal 1 waiver).

c. USAREUR G3/5/7. In addition to the responsibilities identified in subparagraph b above, the USAREUR G3/5/7 will—

(1) Validate and approve IT requirements for HQ USAREUR staff offices and USAREUR MSCs before the required IT equipment will be added to and authorized by the USAREUR Automation Table of Equipment (glossary).

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

(3) Review operational needs statements for tactical IT equipment and services and coordinate reviews of the statements with the USAREUR G6 as well as reviews of interoperability actions between the Active Army and the United States Army Reserve's or the U.S. National Guard's deployed-IT system requirements (AR 71-9).

(4) Ensure all theater C4IM priorities support USAREUR strategic plans.

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

(6) Take part in the URVS process in accordance with AE Pamphlet 70-13-45 procedures and serve as the designated execution approval authority for IT-services requirements and IT-nonservice-acquisition (that is, hardware and software) requirements that have the known or estimated values identified in AE Pamphlet 70-13-45 (para 6a(4)(a) for IT services and para 6c(4) for IT nonservice acquisitions).

d. USAREUR CIO/G6. In addition to carrying out the responsibilities in subparagraph b above, the USAREUR CIO/G6 or his or her designee will—

(1) Take part in the URVS process to provide concurrence or nonconcurrence (that is, technical approval or disapproval) regarding all requirements for IT services and IT nonservice acquisitions and ensure USAREUR complies with AR 25-1 (AE Pam 70-13-45, para 5d).

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

(3) Provide policy and oversight for USAREUR IT and IM programs. These programs currently include, but are not limited to, the following:

(a) The USAREUR Life Cycle Replacement Program.

(b) The USAREUR Copier Management 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 according to the current USAREUR procedures (available at *https://intranet.eur.army.mil/hq/portfoliomgnt*), which will be incorporated in AE Pamphlet 25-13 (when published).

e. USAREUR Judge Advocate (JA). In addition to carrying out the responsibilities in subparagraph b above, the USAREUR JA will provide legal support and advice as required (including to evaluate the legal aspects of requests for commercial high-speed Internet service in the quarters of key personnel and other IT-related requests as needed).

Paragraph 3-2, Planning phase. Add subparagraph d as follows:

d. Army in Europe Responsibilities for the Planning Phase. Army in Europe organizations have the following responsibilities in support of the Planning Phase of IT acquisitions:

(1) The Information Technology-Theater Business Office (IT-TBO), ODCS, G6, HQ USAREUR (AEIM-TBO). The IT-TBO is responsible for managing the investment life cycle of IT acquisitions (hardware and software) and IT services for USAREUR and ensuring USAREUR IT life-cycle actions are in compliance with the Clinger-Cohen Act of 1996 (40 USC, Subtitle III), APMS requirements, and other pertinent policy.

(2) HQ USAREUR Staff Offices and USAREUR MSCs. All HQ USAREUR staff offices and USAREUR MSCs are responsible for ensuring that IT (services and nonservice) acquisitions and IT (services and nonservice) contracts are planned, reviewed, validated, and managed according to AE Pamphlet 70-13-45, the USAREUR Information Technology Portfolio Management (IT PfM) Program, and the capital-planning and investment-management governance processes.

NOTE: More information about the USAREUR IT PfM Program is available at *https://intranet.eur.army.mil/hq/portfoliomgnt/SitePages/Home.aspx*.

(3) USAREUR Specialized Commands. USAREUR specialized commands and other USAREUR-affiliated organizations will coordinate with the G6 of their parent higher headquarters for command-specific guidance for the planning phase of Army IT management.

Paragraph 3-3. Investment phase. Add subparagraphs f through h as follows:

f. Army in Europe Applicability. The policy (g below) and responsibilities (h below) for the Investment Phase of Army IT management applies to USAREUR IT requirements meeting any of the following criteria:

(1) All IT services, regardless of cost.

(2) All IT "moratorium items" (glossary; basic AR, paras 3-3c and d) (for example, servers, data centers video-teleconference equipment, commercial mobile devices, software), regardless of cost.

(3) Nonservice IT requirements (that is, hardware or software) costing $25,000 or more.

g. Army in Europe Investment Phase Policy. ID-E, USAREUR specialized commands, and other USAREUR-affiliated organizations will coordinate with the G6 of their parent higher headquarters for command-specific guidance for the investment phase of Army IT management, but should coordinate with the IT-TBO to provide situational awareness of their requirements and the servicing NEC for IT-TVs, as applicable and required to operate equipment on AE networks. HQ USAREUR staff offices and USAREUR MSCs will comply with the following policy:

(1) All IT nonservice procurement actions (for example, Government purchase card purchases, military interdepartmental purchase requests, nonservice contracts) for hardware, software, telecommunication equipment, and network equipment require an IT-TV from the servicing NEC unless the items are on the IT-TV Exemption List and procured according to the IT PfM process.

NOTE: More information about the USAREUR IT PfM program process is available at *https://intranet.eur.army.mil/hq/portfoliomgnt/sitepages/home.aspx*.

(2) IT items that are on the IT-TV exemption list and valued at less than $25,000, must be procured by using a Government purchase card to purchase the items through the Computer Hardware, Enterprise Software, and Solutions, Program Executive Officer for Enterprise Information Systems (CHESS), IT E-mart website (*https://chess.army.mil/*).

h. Responsibilities.

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

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

(b) Immediately inform the IT-TBO of all emergent USAREUR IT requirements (that is, IT (service and nonservice) acquisitions and IT (service and nonservice) contracts in support of "emergent operations" (glossary)).

(c) Coordinate all USAREUR IT requirements with the IT-TBO for acquisition assistance.

(2) The IT-TBO will coordinate among the requiring activity (RA), the USAREUR G3/5/7, the USAREUR G8, and the 409th Support Brigade (Contracting) (409th SB (Contracting)) to assist the RA in developing acquisition strategies, procurement milestones, and necessary acquisition documents in accordance with procedures in paragraph 3-4d of the supplement and AE Pamphlet 70-13-45.

(3) The servicing NEC will manage the IT-TV process (g(1) above and para 3-4d(8)).

NOTE: More information about the IT-TV process is available at *https://army.deps.mil/netcom/sites/5thsignal/g3/eso/initiatives/itval/sitepages/home.aspx*.

Paragraph 3-4b, Non-information technology programmed funds. Add subparagraphs (1) and (2) as follows:

(1) HQ USAREUR staff offices and USAREUR MSCs will send the IT-TBO a request for an Army CIO Goal 1 waiver for—

(a) All IT expenditures that use Operations and Maintenance, Army (OMA), funds regardless of dollar thresholds (para 3-4d).

(b) Any request for an HQDA IT moratorium list item (for example, commercial mobile device, data center, data center software, server, video-teleconference equipment) (basic AR, para 3-3c and d).

NOTE: The USAREUR IT PfM Portal (*https://intranet.eur.army.mil/hq/portfoliomgnt*) provides a list (*https://intranet.eur.army.mil/hq/portfoliomgnt/shared%20documents/moratorium_hw_sw.pdf*) of the types of IT items subject to the HQDA IT moratorium.

(2) USAREUR specialized commands and other USAREUR-affiliated organizations will coordinate with the G6 or business office of their parent higher headquarters, the Army Business Office for IT Capital Asset Management, or both on how best to procure IT requirements using OMA funds that were not programmed in an IT management decision evaluation package (MDEP).

Paragraph 3-4d, Information technology capital asset management. Add subparagraphs (7) through (9) as follows:

(7) Army in Europe IT Capital Asset Management. USAREUR specialized commands and other USAREUR-affiliated organizations will coordinate with the G6 or business office of their parent higher headquarters or the Army Business Office for IT Capital Asset Management to determine if they should use USAREUR procedures or other appropriate procedures. The following policy, procedures, and responsibilities for IT capital asset management apply to HQ USAREUR staff offices and USAREUR MSCs:

(a) The USAREUR IT-TBO is responsible for ensuring all IT investments of HQ USAREUR staff offices and USAREUR MSCs are managed through the IT PfM Program. The IT-TBO will—

1. Serve as the IT PfM PMO for USAREUR.

2. Provide the chairperson for semiannual USAREUR IT PfM summits.

3. Ensure portfolio owners (POs) are appointed on orders by the USAREUR DCG (that is, nominate PO candidates, draft appointment memorandums, track appointments, and manage PO turnover) for each mission area and deconflict domain ownership between POs, if required.

4. Coordinate directly with USAREUR organizations and, if required, with other Army in Europe organizations to review all documents related to IT-procurement requirements (for example, budget, contracting, manpower, operational-planning (mission) documents).

5. Review and assist in the development of IT contract-acquisition requirements.

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

(b) USAREUR POs (as appointed by the USAREUR DCG ((a)3 above)) will—

1. Define the investment posture for their portfolios.

2. Identify the domains that comprise their portfolios and an agent or domain lead for each domain.

(c) USAREUR-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) USAREUR 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 (new-one-time, recurring, or new-recurring) IT requirements during annual budget lay-downs and funding reviews in URVS for technical validation by the USAREUR G6, validation and approval by the USAREUR G3/5/7, and acquisition coordination by the IT-TBO (para 3-3f). RAs should submit—

a. Valid recurring IT-investment requirements through the URVS for review and pre-acquisition assistance by 12 months before the requested delivery date.

b. New IT-investment acquisition and contract (service and nonservice) requirements through URVS for approval, review, and pre-acquisition assistance by 18 months (24 months for large or complex IT requirements) before the requested delivery date.

2. Immediately submit emergent IT requirements in URVS for technical validation by the USAREUR G6 (if required), validation and approval by the USAREUR G3/5/7, and then acquisition coordination by the IT-TBO.

3. Inform their POs of any IT-investment changes.

4. Submit requirements with all appropriate supporting documents. One or more of the following supporting documents may be required for validation, depending on the solution for the service or nonservice IT requirement:

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 IA 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 with a printout of the Remedy Validators Tab (that verifies the NEC has reviewed and approved the requirement) and a copy of the requester-generated equipment and software list that the NEC reviewed.

i. An independent Government-cost estimate (that is, usually an estimate without tax), a CHESS quote, or a CHESS statement of nonavailability.

j. An analysis or print study of in-house printing requirements before requesting leased copiers, Government-owned (GO) networked printers (black-and-white and color printers), or other GO multifunctional devices (that is, copy, fax, print, and scan or other function-combination devices).

NOTE: More information about copiers and printers is in (9) below and on the USAREUR IT PfM portal at *https://intranet.eur.army.mil/hq/portfoliomgnt*.

k. An approved Army CIO Goal 1 waiver (basic AR, para 3-4d).

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

5. Ensure the RA's IMO or IT technician coordinates with the servicing NEC ((h) below). The requesting tactical unit IMO or IT technician must closely coordinate requirements for C4IM equipment, connectivity, and services with the servicing NEC. The NEC provides garrison-to-tactical networking and interface support with related IT services as agreed on using the DA C4IM service list, the AE Network Service Catalog, and ID-E 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, contracting offices, resource management offices) will maximize the use of DOD and Federal contracts.

(f) The 409th SB (Contracting) will—

1. Serve as the subject-matter expert for all IT-contracting matters.

2. Help develop acquisition strategies and documents.

3. Help define procurement milestones.

(g) HQ USAREUR staff offices and USAREUR MSCs will request and receive all appropriate required approvals as identified below (that is, technical-validation approval (NEC IT-TV, 1 below), USAREUR approval (URVS, 2 below), and HQDA approval (Army CIO Goal 1 waiver, 3 below) for all IT investments (hardware, software, and services) before executing funding:

1. NEC IT-TV approval is required for all hardware and software purchases, regardless of cost.

2. USAREUR approval, in URVS, is required for all of the following types of purchases:

a. All services, regardless of cost.

b. All software, regardless of cost.

c. All IT moratorium items, regardless of cost (para 3-4b(1)(b)).

d. IT investment purchases that use OMA, Subactivity Group 11 (Operational Tempo (OPTEMPO)), funds, regardless of cost or dollar thresholds.

e. Commercial off-the-shelf (COTS) IT hardware costing more than $25,000.

3. An Army CIO Goal 1 waiver is required for all of the following types of purchases:

a. IT moratorium items (basic AR, para 3-3c and d), regardless of cost.

b. IT investment purchases that use OMA OPTEMPO funds, regardless of cost or dollar thresholds.

c. COTS-IT hardware or software that is not purchased through the CHESS system, regardless of cost.

d. COTS-IT hardware or software that costs more than $25,000 and will be purchased using funds that were not programmed in an IT MDEP.

NOTE: More information about the USAREUR IT approval process is available at *https://intranet.eur.army.mil/hq/portfoliomgnt/sitepages/home.aspx*.

(h) The servicing NEC will—

1. Ensure all necessary documentation is complete before approving or disapproving the requirement.

2. In coordination with the subject-matter expert, Army project manager, or both validate the technical solution to ensure the requirement is in compliance with the Army Enterprise Architecture.

(8) The NEC IT-TV Process. The NEC IT-TV process provides an Army in Europe technical review and approval of hardware and software requests. The responsibilities for the NEC IT-TV process are as follows:

(a) IMOs will—

1. Send to the servicing NEC a requirements document and necessary documentation for all IT requirements.

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

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

(b) HQ USAREUR staff offices and the G6 or S6 of USAREUR MSCs, USAREUR specialized commands, and other USAREUR-affiliated organizations will—

1. Validate and send IT requirements to the servicing NEC. Commands that are serviced by multiple NECs will send their requirements to the servicing NEC of the requesting headquarters.

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

3. Ensure the IT requirement is part of the organization's modernization plan.

(9) Army in Europe Copier and Printer Management Program. HQ USAREUR staff offices, USAREUR MSCs, USAREUR specialized commands, and other USAREUR-affiliated organizations will appoint a copier and printing-device manager and provide the manager's name to the Programs and Policy Branch, ODCS, G6, HQ USAREUR.

(a) HQ USAREUR staff offices and USAREUR MSCs will comply with USAREUR Copier Management Program guidance issued by the Programs and Policy Branch, ODCS, G6, HQ USAREUR.

(b) USAREUR specialized commands and other USAREUR-affiliated organizations are responsible for managing their copier management programs according to DOD, HQDA, and their parent higher headquarters' copier-management-program funding and management guidance, but should also keep the Programs and Policy Branch, ODCS, G6, HQ USAREUR, informed of their command's program issues and changes as a courtesy and to help synchronize theater actions.

(c) All Army in Europe copier and printing-device managers will—

1. Identify and manage "copiers" (glossary) and "printing devices" (glossary) throughout their assigned organization.

a. Printing devices comprise GO, network-shared and standalone (black-and-white or color) printers and (black-and-white or color) multifunctional (copy, fax, scan, print) printing devices.

b. Copiers comprise all self-service network-shared multifunctional (copy, fax, scan, print), print-copy-only, and print-only printing devices leased by the Army through the Equipment Management Solutions Program of the Document Services, Defense Logistics Agency. By exception, some locations may have a GO self-service copier.

NOTE: Leased-copier contracts coordinated by the Document Services, Defense Logistics Agency, usually include providing delivery and pickup of copiers, routine maintenance support, and shipment of toner (for user-level installation) as part of the contract. The using organization must provide paper.

2. Routinely conduct an analysis (print study) of network-shared printing devices and copiers and direct device consolidations, as applicable, based on the results. USAREUR managers will conduct their analysis according to USAREUR G6 guidance (available at *https://intranet.eur.army.mil/hq/portfoliomgnt*).

Paragraph 3-4l, Enterprise software licenses. Add subparagraph (5) as follows:

(5) Army in Europe Enterprise-License Agreement (ELA) Software Policy. The USAREUR CIO/G6 is the approval authority for exceptions to this policy. All Army in Europe organizations and units will comply with the Army ELA procedures (basic AR, paras 3-4l(2) and (3)) for software purchases and purchases of product services.

(a) USAREUR specialized commands and other USAREUR-affiliated organizations will coordinate with the G6 of their parent higher headquarters for its supplementary ELA policy and procedures and may use the USAREUR supplementary procedures ((b) below) as a guide.

(b) For HQ USAREUR staff offices and USAREUR MSCs, staff principals and commanders will—

a. Ensure that currently available licenses are reused before requesting and ordering new software licenses through the ELA process.

b. Allow only IMOs with valid appointment orders on file with the NEC to request software. The appointment orders must be signed by the appointee's staff principal or commander, as applicable.

c. Use the ELA process as the sole-source for software and service products covered by an ELA.

d. Report all software license changes to the USAREUR ELA Manager at the ODCS, G6, HQ USAREUR. This includes, but is not limited to, documenting newly procured licenses, releasing unused or unneeded licenses to the USAREUR inventory pool, transferring available licenses to other units, and retiring obsolete licenses from the inventory pool.

e. Ensure the S6 or IMO of the RA—

1. First obtains authorization in accordance with paragraphs 3-3f and g for all software-license procurement requests, regardless of whether the request will be filled through the CHESS License Tracking System or a designated ELA vendor.

2. Follows the procedures in CHESS for items ordered through the CHESS IT E-mart and includes the approved NEC IT-TV number in the CHESS IT E-mart "*Comments*" section to allow cross-referencing during the USAREUR G6-G8 approval and validation process.

a. The CHESS IT E-mart may be accessed through the CHESS SharePoint Portal at *https://peoeis.kc.army.mil/chess/sitepages/home.aspx*.

b. New CHESS users must complete a user profile form (PEO-EIS User Information Update Page) on the PEO EIS SharePoint homepage to access the SharePoint IT E-mart.

3. Follows the ELA vendor-ordering procedures for items ordered through a CHESS-designated ELA vendor, as well as any other intermediate command-directed policy and procedures.

4. Maintains accountability and original product materials for all software licenses received through the ELA. Commanders must ensure distribution does not exceed either the quantity authorized or quantity purchased (whichever is less) and will act as the auditing authority for ELA software licenses.

Paragraph 3-4s, Redistribution and disposal of information technology assets. Add subparagraph (3) as follows:

(3) Outdated, defective, and unusable compact discs (CDs) or digital video disks (DVDs) for COTS software applications will be destroyed by cutting, shredding, or breaking them and destroying the software license, if applicable.

(a) Organizations will prepare a statement of destruction that specifies the software name, license number, the number of CDs or DVDs destroyed, and the date and time of their destruction.

(b) At least two people other than the individual destroying the CDs or DVDs must witness the destruction and sign the statement.

(c) Organizations will send the statement to the servicing NEC and keep a record copy.

Paragraph 4-1f, E-mail services. Add subparagraphs (7) through (9) as follows:

(7) Individual Official E-Mail Users—

(a) Will use their individual official DOD-enterprise e-mail address (for example, *john.d.doe.mil@mail.mil*) to exchange routine official (duty-related) information.

(b) Are not authorized to use personal individual e-mail accounts (for example, *doej@yahoo.com*) to send official (duty-related) e-mail.

(c) May use individual official e-mail accounts to correspond with their immediate Family.

1. The individual's "immediate Family" comprises those most closely related to or designated by the user to receive notification in case of emergency. This includes the spouse, children, parents, a person standing in the place of a parent (*in loco parentis*), persons with legal custody, adoptive and half-brothers and sisters, grandparents, and persons listed on DD Form 93.

2. Two-way correspondence between individuals and their immediate Family members is allowed.

(d) To ensure efficient use of the communications bandwidth when communicating by e-mail, Army in Europe personnel should—

1. Avoid sending e-mail messages that are larger than 20 megabytes and instead post attachments to a SharePoint portal and send the uniform resource locator (URL) or link. Government e-mail users may also use the AMRDEC SAFE website (*https://safe.amrdec.army.mil/safe/*) to send files (up to 2 gigabytes in size) without using official e-mail (except to receive SAFE e-mail messages that will provide download URL or delivery confirmations). If a large e-mail must be sent as an attachment, it should be compressed when possible.

2. Eliminate unnecessary and excessive graphics from presentation files before forwarding files by e-mail. 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.

3. Delete unnecessary information (for example, long strings of previous e-mail messages or unrelated comments) before forwarding or replying to e-mail messages.

4. Not routinely use the "delivery receipt" or "read receipt" feature when sending e-mail messages. The receipt features should be used only when the receipt of a message must be verified.

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

(e) All military and civilian personnel who use the Army in Europe network will use signature blocks in official e-mail messages that include only the sender's name, military rank (if applicable and the individual is not retired), title, organization, telephone number (military, civilian, or both), fax number (if applicable), and the Government e-mail address. Figure 2 provides examples of acceptable military and civilian signature blocks.

MAJ John Doe
Chief, XX Division,
ODCS, G6, HQ USAREUR
Bldg XX, Rm XX, Installation (Kaserne), USAG XX
mil: 537-1111
civ : 0611-143-537-1111
fax: 537-1112
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,
ODCS, G6, HQ USAREUR
Bldg XX, Rm XX, Installation (Kaserne), USAG XX
mil: 537-1111
civ : 0611-143-537-1111
fax: 537-1112
NIPR: *john.d.doe.civ@mail.mil*
SIPR: *john.d.doe.civ@mail.smil.mil*
Check out our webpage at: *www.eur.army.mil*

Figure 2. Examples of Military and Civilian E-mail Signature Blocks

1. 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 DOD (AR 25-50, para 6-8c).

2. The signature block may optionally include the sender's location.

3. The inclusion of recognized unit or organizational mottos and logos (for example, "One Team!") is authorized.

4. The inclusion of the unit or staff directorate website URL is authorized.

5. Personal mottos, slogans, quotes, or other forms of personalization are prohibited. This prohibition also includes the areas above and below the signature block.

(f) All contractor personnel who use the Army in Europe network must clearly identify their contractor status in all official e-mail messages. Contractors must include the sender's name, the name of the contractor's firm, the name of the supported organization, the location (optional), and the sender's telephone number (military, civilian, or both), fax number (optional, if applicable), and the e-mail address. Figure 3 provides an example of an acceptable contractor e-mail signature block.

Mr. John Doe
Contractor, ABC Company
ODCS, G6, HQ USAREUR
Bldg ####, Rm ###, Installation (Kaserne), USAG Xxxxx
mil: 537-1111
civ : 0611-143-537-1111
fax: 537-1112
NIPR: *john.d.doe.ctr@mail.mil*
SIPR: *john.d.doe.ctr@mail.smil.mil*

Figure 3. Example of a Contractor E-mail Signature Block

(8) Receiving and Forwarding Unauthorized E-Mail.

(a) The receipt of e-mail messages is not completely controllable. Most Army e-mail systems interconnect with other Government and commercial e-mail systems. If unauthorized or illegal e-mail messages are received, the recipient is ultimately responsible for deleting, destroying, reporting, or otherwise properly disposing of messages that do not belong on the Government system.

(b) Forwarding unauthorized or illegal e-mail messages violates Army e-mail policy, even if the person sending (forwarding) the message is not the originator. The recipient, regardless of whether the message was sent to an individual or organizational e-mail address, is responsible for ensuring that only authorized and approved messages are forwarded. Chain e-mail, 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.

(9) E-Mail Security.

(a) Users must comply with the security and privacy restrictions in AR 25-2, AR 25-55, and AR 340-21 when sending e-mail.

(b) E-mail 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.

(c) Under no circumstances will users send e-mail containing classified information through nonsecure, common-user e-mail systems (for example, the nonsecure Internet protocol router network (NIPRNET)).

(d) Users may send e-mail that contains unclassified but sensitive information or personally identifiable information through nonsecure, common-user e-mail systems (for example, the NIPRNET), provided the message is encrypted by using Public Key Infrastructure (PKI).

Paragraph 5-3b, Visual information activities responsibilities. Add subparagraphs (13) through (21) as follows:

(13) The local TSCs (operating under the TSAE, JMTC), the Training Aid Production Center (TAPC), TSAE, and the Visual Information Services, Europe (VISE); Garrison Support Element; ID-E, all provide above-baseline VI services for the Army in Europe.

(a) Customers will send requests for above-baseline services using the web-based Visual Information Ordering Site (VIOS) to their local TSAE TSC, the TAPC, or VISE depending on the type of product and the most cost-effective, timely, and reliable method of delivery to the customer.

(b) When necessary (usually if the workorder requirement exceeds local capabilities), local TSCs will forward workorders through VIOS to the TAPC or VISE.

(14) The TSAE VI Program Manager, JMTC, as the USAREUR multimedia and visual information (M/VI) manager, will—

(a) Manage the regional training support division VI managers and ensure appropriate staff support is provided for those managers. This includes appointing a dedicated MDEP budget analyst for MDEP MU1M (that is, VI Mission Support).

(b) Manage authorized TSAE VI activities at TSCs and the TAPC.

(c) Ensure 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).

(d) Ensure that all above-baseline services are provided locally at the TSC or forwarded to the TAPC or VISE for production, and ensure that reimbursements for above-baseline services are obtained and properly managed.

(e) Review the operation of authorized USAREUR VI activities annually to determine if products and services are cost-effective and systems are being fully utilized.

(f) Conduct or arrange for technical training for assigned VI personnel.

(g) Protect assigned access-identification numbers and implement local policy and procedures for use of Army files in the Defense Imagery Management Operations Center (DIMOC). This includes ensuring that USAREUR VI personnel send all pertinent material (for example, graphics, photos, videos) to DIMOC for permanent archiving.

(h) Plan, program, and budget for OMA funds to support VI-mission requirements (for example, equipment, personnel, products, systems).

(i) Prepare directives for implementation of VI policy and procedures.

(j) Serve as the administrator for all USAREUR VIOS activities and ensure VIOS is implemented at all authorized USAREUR VI activities for the collection and reporting of VI support requested by and provided to customers.

(k) Develop 5-year plans for acquiring VI investment systems based on HQDA strategy and in accordance with the basic AR.

(15) VISE, as the Army-appointed enterprise multimedia center for Europe, will provide an individual who serves as the enterprise-level-appointed global administrator for VIOS Europe and will ensure VIOS is implemented at all authorized Army in Europe VI activities for the collection and reporting of VI support requested by and provided to customers.

(16) All Army M/VI activities in Europe will use the networking component of the VIOS. All VIOS requests will be sent to the local supporting TSC for approval or forwarding to the TAPC or VISE, as appropriate. 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 organization for coordination, routing for approval or disapproval, and execution if approved.

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

(18) The purchase of VI equipment, systems, and services must be validated and the procurement must be made according to AE Pamphlet 70-13-45 and the USAREUR IT PfM Program procedures (*https://intranet.eur.army.mil/hq/portfoliomgnt*).

(a) Purchases costing less than $25,000 (except IT moratorium items) of hardware and software must be technically validated by the local NEC. IT moratorium items must be approved by the USAREUR G3/5/7 (through the URVS process) or the ID-E approval process, which both include a technical validation. IT that is procured outside of the CHESS system (basic AR, para 3-4a) may also require an Army CIO Goal 1 waiver through the ITAS approval process.

(b) Purchases of hardware and software equipment costing $25,000 or more must be technically validated by the local NEC and approved by the USAREUR G3/5/7 (through the URVS process) before procurement. Purchases costing $25,000 or more (basic AR, para 3-4) may also require an Army CIO Goal 1 waiver through the ITAS approval process.

(c) Equipment costing less than $50,000, if approved, may be procured locally or referred to the Army Multimedia and Visual Information Directorate (AMVID), Production Acquisition Division (PAD), Television-Audio Support Activity (T-ASA), Armed Forces Network, Defense Media Activity.

(d) Equipment exceeding $50,000, if approved, must be procured by the T-ASA in accordance with the basic AR, paragraph 5-3b(11).

(e) In accordance with most applicable European host-nation law, ergonomic requirements must be considered when purchasing and installing equipment. Systems will be installed to meet the ergonomic requirements of users.

(19) 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.

(a) Examples of top-priority imagery include the following:

1. Current operations.

2. Contingency operations.

3. Major exercises, especially joint and combined exercises.

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

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

6. Significant local events that would be of interest to higher HQ.

7. Major accidents.

8. Major construction projects, from start to finish.

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

10. Memorials.

11. Assumption-of-command, change-of-command, and change of responsibility ceremonies (directors or command sergeants major) and other official ceremonies for officers who are colonels or higher and civilian directors who are colonel-equivalents or higher.

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

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

(20) The following are the general rules for processing and documenting VI products:

(a) Time-sensitive imagery should be accessioned to the DIMOC within 72 hours after the event. Non-time-sensitive imagery will be accessioned to DIMOC within 10 workdays after the event.

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

(c) All captions will be created in accordance with the DOD captioning style guide.

(d) Only public affairs offices have releasing authority for VI imagery, media, and captions. Public affairs officers 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 instruction.

(21) Paragraph 2-3n provides additional guidance on providing COMCAM support.

Paragraph 5-4, Records management. Add subparagraph i as follows:

i. Army in Europe Records Management. AE Regulation 25-400-2 prescribes Army in Europe policy and procedures for managing record information (paper and digital).

Paragraph 5-5, Publishing and printing. Add subparagraphs d and e as follows:

d. Army in Europe Publishing and Printing. AE Regulation 25-30 prescribes Army in Europe policy on publishing and printing.

e. Army in Europe Copier Management. In the Army in Europe, IMOs at the organization or unit level are responsible for managing all Army-leased (through the Document Services, Defense Logistics Agency, Equipment Management Solutions program) duplicating devices (that is, copiers). In addition to the procedures in paragraph 3-4d(9) of the supplement, Army in Europe IMOs and copier users will—

(1) Ensure AE Label 25-1A is posted in a clearly visible location on all leased copiers. This label identifies that users may not contact the copier vendor directly, but must coordinate through their IMO.

(2) Use the 119 ticket system (*https://119.eur.army.mil*) to request and coordinate assistance for all copier problems. Users will not contact the vendor directly for any issue. Use of the 119 ticket system ensures that Army in Europe organizations capture and validate all costs associated with the leased copier program and helps limit installation access to only those vendors requiring access.

(a) Users will submit a 119 ticket that identifies the nature of the problem and the copier make, model, serial number, and exact location (that is, kaserne, building, and room number).

(b) The 119 ticket system will route the ticket to the appropriate IMO. The IMO will determine whether he or she should contact the vendor immediately (for example, routine service issues (no toner)), diagnose and remedy the issue remotely or in person (for example, changing settings that require administrator privileges), or, after diagnosis, contact the vendor to request repair.

Paragraph 5-6, Information assurance. Add subparagraphs a and b as follows:

a. As the USAREUR Authorizing Official, the USAREUR CIO/G6 will appoint a USAREUR IAPM in writing. The USAREUR IAPM will establish, manage, and assess the effectiveness of all aspects of the Army in Europe IA Program. As delegated by DOD through HQDA to HQ USAREUR, the IAPM is also the Security Controls Assessor (SCA) agent for Army in Europe networks and systems (DODI 8510.01, encl 4, para 1b(3)(b)).

b. HQ USAREUR staff offices, USAREUR MSCs, USAREUR specialized commands, and other USAREUR-affiliated organizations will implement IA programs in accordance with AR 25-2; Army in Europe policy; and tactics, techniques, and procedures provided by the USAREUR IAPM.

Paragraph 6-3, Complying with Defense Information Systems Registry standards. At the end of the paragraph, add the following:

In Europe, evaluations of acquisitions will be conducted for DISR compliance within the framework of USAREUR IT technical evaluations (para 3-4(d)(8)).

Paragraph 7-2, Information technology support services for Army organizations on Army installations. Add subparagraphs a through d as follows:

a. In the European theater, the RCC-E is responsible for regional oversight of local data networks (or local area networks (LANs)) that are connected to Defense Information Systems Agency networks. These LANs include all LANs using the Army in Europe NIPRNET for unclassified data and the Army in Europe Secret Internet protocol router network (SIPRNET) for classified data.

NOTE: The overall Army NIPRNET is also referred to as the Land Warrior Network (Unclassified) (LandWarNet (unclas)) in the basic AR.

b. NECs are responsible for LAN administration and network management.

c. A "remote user" is a person who enters the Army in Europe NIPRNET from outside the physical or logical boundary of the installation or unit internal LAN. The remote-access system creates a protected extension of the Army in Europe NIPRNET (usually using a virtual private network (VPN) connection) for authorized remote users.

(1) Army in Europe Remote User Policy.

(a) Remote users are not authorized to use employee-owned ISs to connect to the Army in Europe NIPRNET. Remote users may use only GO ISs or select approved CO ISs, if applicable.

(b) Army in Europe network users must request approval for remote access using the appropriate AE form for their employment category (that is, AE Form 25-1H for Category 1 (DOD military members, civilian employees, local-national employees, and "long-term contractors" (glossary)) and AE Form 25-1J for Category 2 ("temporary-duty contractors" (glossary))).

(2) 5th Sig Cmd Remote-User Responsibilities. The 5th Sig Cmd will—

(a) Be the sole provider of VPN services for Army in Europe networks.

(b) Manage all remote-access points.

(c) Configure all remote-access equipment to require authentication using a Common Access Card (CAC) and encryption.

(3) Remote-User Approval Authority. Only commanders who are a captain or higher, civilian supervisors who are a GS-13 or higher, or other supervisors in equivalent grades may approve requests for remote access. These approval authorities will also be responsible for—

(a) Preapproving any reimbursement for temporary duty or home-station remote-access connection charges.

(b) Setting specific limits when preapproving reimbursement for connection charges. Usually, home-station remote-access users should not be reimbursed, because those users could alternatively go to their Government office for access.

(c) Paying approved reimbursements for remote-access charges using appropriate funds (usually the organization's own OMA funds).

(4) Unit Responsibilities. If the unit approval authority determines that an individual needs remote access, the unit must also provide the GO IS or IT solution to be used for remote access or specify that a contractor will provide an approved CO IS to the contractor's employee.

(5) IMO Responsibilities. IMOs will—

(a) Use the appropriate remote-access request form (AE Form 25-1H for category 1 users (that is, DOD military members, civilian employees, local-national employees, and "long-term contractors") or AE Form 25-1J for category 2 users (that is, "temporary-duty contractors")) to request approval for remote access for their requesting user from their servicing NEC.

(b) Use AE Form 25-1K to conduct computer security compliance inspections of GO and CO ISs to ensure they are correctly configured before approving or forwarding remote-access requests.

NOTE: CO ISs must be otherwise authorized access to the Army in Europe network before remote-access requests may be approved.

(c) Keep completed forms in unit records and coordinate new and deleted accounts with the servicing NEC.

(6) Army in Europe Network Users. Users will request approval for remote access through their unit IMO using the appropriate AE form for their employment category ((1)(b) above).

d. All organizations and units that use the Army in Europe network will—

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

(2) Request an exception to policy from the USAREUR CIO/G6 or ID-E G6, as applicable, if they have an operational requirement to retain non-IPv6-compatible equipment. The request for exception 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 exceptions to this policy must be routed through the user's servicing NEC to the USAREUR G6 (AEIM-A) or to the ID-E G6.

(3) Not transition to IPv6 without approval from the USAREUR CIO/G6 or the ID-E G6, as applicable. The servicing NEC will send all customer requests for transition to IPv6 through the USAREUR G6 or ID-E G6. Once approved, 5th Sig Cmd will provide an implementation plan in coordination with NETCOM (for USAREUR requesters) or ID-E (for ID-E requesters).

Paragraph 7-11b, Requirements for floor space intended for information technology systems. Add subparagraphs (1) through (7) as follows:

(1) Army organizations in Europe will not purchase servers without an Army CIO Goal 1 waiver approved through the ITAS approval-system.

(2) Before an organization connects or reconnects a server to the Army in Europe network, the server must be certified and accredited. Organizational IAMs must conduct certification testing and prepare RMF-certification documents for RMF accreditation.

(a) Certification testing is required to ensure that the Army in Europe computer-security baseline, service packs, critical updates, and all identified IAVAs have been applied to the server.

(b) Test results must be included in the organization's RMF-certification documentation and provided to the Certification and Accreditation Branch, Information Assurance Program Division, ODCS, G6, HQ USAREUR, for review and acceptance by the agent for the certification authority.

(c) The agent for the certification authority will send the documentation to the designated accreditation authority (DAA) for the DAA to provide an acceptance of residual risks and formal approval to connect to the network. The Army in Europe IAPM and the servicing NEC can provide technical assistance on certification testing and the accreditation process. Units must plan on at least 90 days for the IAM to complete certification testing and for processing and forwarding RMF documentation to the DAA.

(d) If a server must be connected to meet urgent operational warfighting requirements before the server has been certified or accredited, the server will be registered as soon as possible after being connected. This is authorized by the G3, 5th Sig Cmd.

(3) No Army in Europe organization may activate a server without approval from the 5th Sig Cmd Enterprise Configuration Management Board.

(4) Organizations that have server hardware systems that are not capable of operating at the latest operating-system (OS) standard, as established by the United States Army Cyber Command and 5th Sig Cmd, must request an exception to policy from the USAREUR CIO/G6.

(a) The request for exception to policy must fully justify why the old OS must remain in use and provide the expected timeline to upgrade the OS to the current baseline.

(b) All requests for migrations and file storage must be coordinated with 5th Sig Cmd.

(5) After a server is connected to the Army in Europe network, the IAPM's information infrastructure assessment team will make periodic inspections to ensure that regulatory guidelines are being followed.

(6) The Defensive Cyber Operations Division and RCC-E will periodically conduct random network scans to verify server compliance and quarantine any servers that are not in compliance.

(7) For any server system quarantined as a result of periodic inspections or network scans, the owning organization is responsible for taking the steps necessary to reestablish compliance.

Appendix A, Section I, Required Publications. Add the following:

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

DOD Instruction 5040.02, Visual Information (VI)

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

Unified Capabilities Requirements 2013 (UCR 2013), Office of the DOD Chief Information Officer, January 2013, subject: Department of Defense Unified Capabilities Requirements 2013 (available at *http://jitc.fhu.disa.mil/jitc_dri/pdfs/ucr_2013_combined_signed.pdf*)

AR 25-50, Preparing and Managing Correspondence

AE Regulation 25-30, The Army in Europe Publishing Program

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

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

Appendix A, Section III, Prescribed Forms. Add the following:

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

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

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

AE Form 25-1N, Authorized Service Interruption (ASI) Request Form

AE Label 25-1A, Leased Copier Service Instructions

Appendix A, Section IV, Referenced Forms. Add the following:

DD Form 93, Record of Emergency Data

DD Form 1144, Support Agreement

Glossary, Section I, Abbreviations. Add the following:

409th SB (Contracting)	409th Support Brigade (Contracting)
5th Sig Cmd	5th Signal Command
AE	Army in Europe
AKM	Army Knowledge Management
AOR	area of responsibility
APO	Army post office
ASI	authorized service interruption
C4IM	command, control, communications, computers, and information management
CAC	Common Access Card
CCMD	combatant command
CD	compact disc
CHESS	Computer Hardware, Enterprise Software, and Solutions, Program Executive Officer for Enterprise Information Systems
CIO	chief information officer
CO	contractor-owned
COMCAM	combat camera
COTS	commercial off the shelf
CG, USAREUR	Commanding General, United States Army Europe
DA	Department of the Army
DAA	designated accreditation authority
DEROS	date eligible for return from overseas
DIMOC	Defense Imagery Management Operations Center
DISR	Department of Defense Information Technology Standards Registry
DODI	Department of Defense instruction
DRMO	Defense Reutilization Marketing Office
DRSN	Defense Red Switch Network
ELA	enterprise license agreement
GFEBS	General Fund Enterprise Business System
GO	Government-owned
HAZCON	hazardous condition
HQ	headquarters
HQ USAREUR	Headquarters, United States Army Europe
IA	information assurance
IAM	information assurance manager
IAPM	information assurance program manager
IASO	information assurance security officer
IAVA	information assurance vulnerability alert
ID-E	United States Army Installation Management Command Directorate-Europe
IM	information management
IMO	information management officer
IPv6	Internet Protocol version 6
IS	information system
IT	information technology
IT PfM	information technology portfolio management
IT-TBO	Information Technology-Theater Business Office, Office of the Deputy Chief of Staff, G6, Headquarters, United States Army Europe
IT-TV	information technology technical validation

JA	judge advocate
JMTC	Seventh Army Joint Multinational Training Command
LandWarNet	Land Warrior Network
M/VI	multimedia and visual information
MDEP	management decision evaluation package
MFR	memorandum for record
MSN	mission
NEC	network enterprise center
NETCOM	United States Army Network Enterprise Technology Command
no.	number
OMA	Operations and Maintenance, Army (funds)
OP	operational
OPTEMPO	operational tempo
PfM	portfolio management
PMO	program management office
PO	portfolio owner
RA	requiring activity
RCC-E	Regional Cyber Center-Europe
RFC	request for change
RMF	risk-management framework
sig bn	signal battalion
SLA	service-level agreement
SSB	supporting signal battalion
STE	secure telephone equipment
suppl	supplement
TAPC	Training Aid Production Center
TSAE	Training Support Activity Europe
TSC	training support center
unclas	unclassified
URVS	United States Army Europe Requirements Validation System
U.S.	United States
USAG	United States Army garrison
USAREUR	United States Army Europe
USAREUR CIO/G6	Chief Information Officer and Deputy Chief of Staff, G6, 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
USC	United States Code
USCYBERCOM	United States Cyber Command, United States Strategic Command
VIOS	Visual Information Ordering Site
VIP	very important person
VISE	Visual Information Services, Europe; Garrison Support Element; United States Army Installation Management Command Directorate-Europe
VOIP	voice over Internet protocol
VoSIP	voice over secure Internet protocol
VPN	virtual private network

Glossary, Section II, Terms. Add the following:

copier
A duplicating machine that, for the purposes of this supplement, comprises all self-service network-shared multifunctional (copy, fax, scan, print), print-copy only, and print-only printing devices leased by the Army through the Equipment Management Solutions Program of the Document Services, Defense Logistics Agency (see also: printer)

emergent operation
A specific, immediate mission or operation (for example, initial entry into Iraq and Afghanistan, noncombatant evacuation operation, Haiti earthquake assistance) that is not already an "ongoing operation" (for example, Operation Enduring Freedom, Area Support Team (AST) Balkans operations, AST Black Sea operations)

long-term contractor
An employee of a civilian company, which was contracted by the DOD, Army, or other service to perform a mission in support of the U.S. Armed Forces, who is expected to be working full-time in support of a DOD entity over an extended period (that is, at least 6 months and usually 1 or more years)

moratorium item
Information technology equipment that HQDA has restricted Army units from purchasing without HQDA approval (basic AR, paras 3-3c and d) to prevent duplicating existing enterprise-level services, promote standardization, reduce costs, and reduce redundancy (for example, commercial mobile devices, data centers, servers, software, video-teleconference equipment)

operational tempo funds
Money that is programmed through the DOD budget process in the Operations and Maintenance, Army (OMA), Subactivity Group (SAG) 11, category

printer or printing device
A machine producing a printout that, for the purposes of this supplement, comprise all Government-owned, network-shared and standalone, black-and-white or color multifunctional (copy, fax, scan, print), print-only, or print-copy devices (these devices usually meet no more than the DOD Volume Band 1 criteria (that is, no more than 5,000 black-white and 2,000 color copies per month) because devices meeting higher volume-band requirements usually must be supplied by the Document Services, Defense Logistics Agency) (see also: copier)

temporary-duty contractor
An employee of a civilian company, which was contracted by the DOD, Army, or other service to perform a mission in support of the U.S. Armed Forces, who is expected to be working only part-time or only for the duration that a unit is using the Army in Europe network. As with a regular Army temporary duty assignment, temporary duty assignments for contractors are normally less than 6 months.

USAREUR Automation Table of Equipment
A list of information technology (IT) equipment approved by the USAREUR G3/5/7 that serves as the IT equipment authorization document for HQ USAREUR. The USAREUR G6 acquires and manages the life cycle of this IT equipment. This list supplements IT equipment authorizations on the modified table of equipment and table of distribution and allowances and documents authorizations that are usually based on but may also exceed common table of allowances (CTA) authorized quantities or vary from CTA-identified equipment types.