

18 October 2012

Information Management

Army in Europe Information Assurance

*This regulation supersedes AE Regulation 25-2, 7 September 2011.

For the Commander:

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

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes information-assurance policy and procedures for the Army in Europe.

Summary of Change. This revision—

- Incorporates guidance on the use of the Army in Europe Information Technology Training (AE-ITT) Program and addresses the AE-ITT as the primary source for training in theater (para 19).
- Incorporates guidance on issuing Secret Internet Protocol Router Network (SIPRNET) PKI tokens in theater (para 22j).

Applicability. This regulation applies to the Army in Europe and all other organizations with accounts connected to or through Army in Europe information 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 available on the Army Records Information Management System website at <https://www.arims.army.mil>.

Supplementation. Organizations will not supplement this regulation without USAREUR G6 (AEIM-I) approval.

Forms. This regulation prescribes AE Form 25-2A. 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 regulation is the Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR (DSN 334-4811). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G6 (AEIM-I), Unit 29351, APO AE 09014-9351.

CONTENTS

SECTION I GENERAL

1. Purpose
2. References
3. Explanation of Abbreviations and Terms

SECTION II RESPONSIBILITIES

4. USAREUR G1
5. USAREUR G2
6. USAREUR G3
7. Chief Information Officer/USAREUR G6
8. Commanding General, 5th Signal Command
9. Commanders, Directors, and Managers
10. Information Assurance Program Manager
11. RCERT-E
12. Information Assurance Managers
13. Information Assurance Support Officers
14. System Administrators and Network Administrators
15. Data Owners
16. General Users

SECTION III ARMY IN EUROPE INFORMATION ASSURANCE POLICY

17. Overview
18. Funding
19. IA Training
20. Minimum IA Requirements
21. Prohibited Activities
22. Public Key Infrastructure Software Security
23. Tunneling SIPRNET Traffic Through Other Than SIPRNET Connections
24. Password Control
25. Personnel Security Standards
26. Foreign Access to Information Systems
27. Cross-Domain Security Interoperability
28. Network Security
29. Protection of Classified Information
30. IAVM Reporting Process
31. Compliance Reporting
32. Wireless Local Area Networks

- 33. Certification and Accreditation Overview
- 34. Certification
- 35. Accreditation
- 36. Connection-Approval Process
- 37. CYBERCON
- 38. Personally Identifiable Information
- 39. Individual and Organizational Accountability
- 40. Internet-Based Capabilities
- 41. Commander's Quick Reference Guide to Defending Cyberspace

Appendixes

- A. References
- B. Consolidated Information Assurance Training and Certification Requirements
- C. Granting Foreign Liaison Officials Access to the Army in Europe Networks
- D. Wireless Infrastructure Implementation Policy
- E. Use of Internet-Based Capabilities
- F. Defending Cyberspace

Table

- E-1. Collaborative Technologies

Glossary

SECTION I GENERAL

1. PURPOSE

This regulation provides Army in Europe information assurance (IA) policy and procedures for implementing the Army Information Assurance Program for USAREUR and IMCOM-Europe.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

SECTION II RESPONSIBILITIES

4. USAREUR G1

The USAREUR G1 will—

- a. Work with the IMCOM-Europe G1 to ensure central processing facility checklists include the Army in Europe Information and Technology Training (AE-ITT) Program.
- b. Identify position titles of persons performing IA functions (DOD 8570.01-M, paras C7.3.2.1 and C7.3.2.4).
- c. Identify information technology (IT) investigation requirements, IA category and level-of-certification requirements in conditions of employment and vacancy announcements.

5. USAREUR G2

In addition to the responsibilities listed in AR 25-2, paragraph 2-5, the USAREUR G2 will—

- a. Work with 5th Signal Command (5th Sig Cmd) to distribute DOD, Department of the Army (DA), and Army in Europe-level IA threat information.
- b. Manage the Foreign National (FN) Personnel Screening Program in support of requirements in AR 25-2, paragraphs 4-14 and 4-15; and AE Regulation 604-1.
- c. Help requiring activities prepare SF 86 for FN employees.
- d. Provide foreign disclosure (background security checks) to support FN-employee access to Army in Europe information systems (ISs) and Army Knowledge Online (AKO).
- e. Coordinate responses to incidents, intrusions, and compromises of classified information with security managers and the United States Army Criminal Investigation Command (USACIDC).
- f. Provide support, coordination, oversight, and direction to the cyber community in areas involving traditional security, such as classified systems marking, utilization, incident handling, and protected distribution systems (PDSs); and assessment, evaluation, and inspection programs that are affected by these types of systems.
- g. In accordance with AR 380-27, provide support and assistance in submitting and tracking PDS packets (requests for PDS certification) to the Army-certified TEMPEST technical authority.

6. USAREUR G3

In addition to the responsibilities listed in AR 25-2, paragraph 2-6, the USAREUR G3 will—

- a. Manage cyber condition (CYBERCON), Joint Communications Security Monitoring Activity, operations security (OPSEC), and Information Assurance Vulnerability Management (IAVM) Program taskings.
- b. Coordinate and request program services from the Information Operations Vulnerability Assessments Division (IOVAD), 1st Information Operations Command, in coordination with 5th Sig Cmd and the Regional Computer Emergency Response Team - Europe (RCERT-E).

7. CHIEF INFORMATION OFFICER/USAREUR G6

In addition to the responsibilities listed in AR 25-2, paragraph 2-8, the Chief Information Officer (CIO)/USAREUR G6 will—

- a. Serve as the authorizing official (AO) for all Army in Europe network assets.
- b. Appoint and oversee the Army in Europe Information Assurance Program Manager (IAPM).
- c. Provide IA support to customers through network enterprise centers (NECs) and, if necessary, with the assistance of the Army in Europe IAPM.
- d. Determine the IA posture for Army in Europe IT assets. This includes but is not limited to IAVM, CYBERCON, the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), and the Federal Information Security Management Act report.

e. Ensure that Army in Europe-approved computer security baselines, information assurance vulnerability alerts (IAVAs), current antivirus software, and definition files are applied to all systems connected to Army in Europe networks.

f. Ensure that program-managed systems use the security configurations as specified by the program manager.

8. COMMANDING GENERAL, 5TH SIGNAL COMMAND

In addition to the responsibilities listed in AR 25-2, paragraph 2-8, the Commanding General, 5th Sig Cmd, will—

a. Operate, manage, maintain, and defend the enterprise and backbone portion of the NIPRNET and SIPRNET.

b. Coordinate IOVAD program services with the USAREUR G3 and RCERT-E and request services.

c. Provide guidance and priorities to the RCERT-E regarding IA and computer network defense (CND) support.

d. Manage the configuration of and the patches for all network components and systems.

e. Establish tactics, techniques, and procedures for IA and CND activities with the RCERT-E and the Army in Europe IAPM.

f. Conduct vulnerability assessments of top-layer architecture critical assets, devices, and servers, and IA-implemented devices twice a year. The results of these assessments will be reported to the Army in Europe IAPM.

g. Participate with the USAREUR G2, the United States Army Intelligence and Security Command, 1st Information Operations Command, and USACIDC in analyses and studies concerning foreign-intelligence threats and criminal or operational vulnerabilities against which IA countermeasures must be directed.

h. Define IA responsibilities in all service-level agreements between 5th Sig Cmd and supported units for all IT assets under consolidated enterprise management.

i. Perform all IA-related operations, maintenance, and monitoring functions for all IT assets under consolidated enterprise management on behalf of tenant units. This includes but is not limited to IAVM patching, scanning and reporting, implementing and monitoring CYBERCON-related measures, maintaining and monitoring server and desktop IA software, and responding to incidents as specified in service-level agreements with tenant units.

j. Implement and maintain network-security solutions to block, filter, or reprioritize network traffic that may interfere with Army in Europe missions. This includes but is not limited to filtering nonessential, high-bandwidth traffic; potentially malicious websites and e-mail traffic; and traffic that may violate Army workplace standards.

k. Publish clear instructions to tenant units on how to request exceptions to network filtering for clearly defined, mission-critical purposes.

l. Implement, operate, maintain, and monitor the Army in Europe IA infrastructure, including but not limited to firewalls, intrusion-detection systems, intrusion-prevention systems, and patch-deployment tools.

m. Serve as the director of information management for the Army in Europe as defined in AR 25-2, paragraph 2-30.

n. Manage all remote-access devices in the Army in Europe.

o. Ensure that all systems and users comply with Army in Europe remote-access policy.

p. Ensure connections to Army in Europe networks comply with connection-approval processes.

9. COMMANDERS, DIRECTORS, AND MANAGERS

In addition to the responsibilities listed in AR 25-2, paragraph 2-24, commanders, directors, and managers will ensure that—

a. The IA workforce (Soldiers, civilians, and contractors) is trained and certified to safeguard information on Army in Europe ISs. Certifications are required for personnel who perform IA functions or have privileged-user accounts. These personnel must be trained in accordance with IA categories and levels designated by DOD 8570.01-M.

b. Background investigations and security clearances are completed based on the access that personnel will be given before they are given access to Army in Europe ISs.

c. Personnel performing IA functions are appointed in writing and register in the Army Training and Certification Tracking System (ATCTS) (<https://atc.us.army.mil/iastar/index.php>) to do the following:

(1) Upload required documentation.

(2) Complete required training and certification.

(3) Keep their IA account current with new certifications.

(4) Ensure that accounts are verified with the proper validation level.

(5) Inprocess and outprocess new and departing personnel with the Policy, Programs, and Training Branch (PP&TB), Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR; and local information assurance managers (IAMs).

(6) Ensure that contracting officers verify that contractors supporting IA functions are appropriately certified, and provide verification to the Defense Eligibility Enrollment Reporting System.

(7) Ensure that new contracts meet the category and level-of-certification requirements in DOD 8570.01-M, chapter 1.

(8) Modify existing contracts to show DOD 8570.01-M, chapter 1, certification requirements.

(9) Ensure that all Soldiers, civilians, and contractors suspected of engaging in prohibited computer network activities are suspended from network access pending results of an official command inquiry.

(10) Ensure that all IAMs establish an Army Information System Security Program (ISSP) account.

10. INFORMATION ASSURANCE PROGRAM MANAGER

In addition to the responsibilities listed in AR 25-2, paragraph 3-2b, the Army in Europe IAPM will—

- a. Chair the Army in Europe IA and CND workgroups.
- b. Provide advice and assistance on the construction, approval, and validation of PDSs.
- c. Serve as the Agent of the Certification Authority (ACA) to process and validate certification and accreditation (C&A) packages for theater ISs in accordance with DOD and Army policy.
- d. Maintain classified and unclassified IA portals to enable bilateral communication in the IA community managed and supported by the Army in Europe IAPM.
- e. Manage the AE-ITT Program to train and certify the IT and IA workforce in accordance with DOD 8570.01-M.
- f. Ensure training and certification assets are available to allow the IA workforce to train and test for certifications as required.
- g. Provide advice and assistance to the AO on the C&A process and maintain a central repository of all AO-approved accreditation packages.
- h. Manage the Army in Europe IAVM Program and provide guidance on compliance-reporting requirements.
- i. Manage the Army in Europe Public Key Infrastructure (PKI) Program.
- j. Approve computer-security baselines for use in the Army in Europe. This involves programs such as the Army Golden Master (AGM), Defense Information Systems Agency (DISA) security technical implementation guides (STIGs), DISA Gold Disk, Federal Desktop Core Configuration, and other relevant Government programs and emerging industry standards.
- k. Serve as a voting member of the 5th Sig Cmd Configuration Control Board (CCB).
- l. Be a participating member of the USAREUR G3 Information Operations (IO) Workgroup.
- m. Validate and approve ISSP submissions from tenant organizations.
- n. Provide technical assistance to the USAREUR G3 on CYBERCON and OPSEC.
- o. Provide IA services in accordance with memorandums of agreement with external organizations (for example, United States Army Africa).
- p. Provide comprehensive planning and programming of Army in Europe IA requirements for management decision evaluation packages (MS4X and MX5T) and advocate the development of Army in Europe IA resources through the planning and budgeting process.

- q. Coordinate computer crime investigations and unit investigations with the USAREUR G2 and the Computer Crime Investigation Unit, USACIDC.
- r. Coordinate responses to computer incidents, intrusions, and compromises of classified information on Army in Europe ISs with the USAREUR G2, USAREUR G3, and USACIDC.
- s. Provide policy and guidance for installing and operating wireless systems.
- t. Provide support for training, procurement, management, and DIACAP requirements to ensure that the Army in Europe wireless infrastructure is properly governed.
- u. Perform announced annual cyber-readiness visits (CRVs) and unannounced CRVs of USAREUR major subordinate and specialized commands and United States Army garrisons (USAGs) to assess unit cyber readiness in accordance with established policy, procedures, best business practices, and baseline configurations. An unannounced CRV is defined as a short-suspense visit (for example, 3 weeks' notice).
- v. Provide cyber-readiness reports to the AO and senior leaders.
- w. Provide a list of approved regulatory DA and DISA IA inspections and USAREUR annual training guidance. Detailed information about inspection programs can be found on the iAssure portal at <https://portal.eur.army.mil/sites/iassure/default.aspx>.

NOTE: IA is a key enabler that protects Soldiers by securing and defending the NIPRNET and SIPRNET, which support net-centric warfare, information superiority, decision superiority, and full-spectrum dominance. As net-centric warfare and the cyber threat increase, IA compliance is critical to the success of worldwide Army operations and to protecting Soldiers. Several inspection programs are mandated by the Chairman of the Joint Chiefs of Staff and the Chief of Staff, Army.

11. RCERT-E

In addition to the responsibilities listed in AR 25-2, chapter 4, the RCERT-E will—

- a. Support Army in Europe computer-network operation synchronization functions.
- b. Provide direct support to 5th Sig Cmd and the Europe - Theater Network Operations and Security Center (E-TNOSC) for CND functions.
- c. Coordinate with the 5th Sig Cmd G2 and G3, E-TNOSC, and the Army in Europe IAPM to integrate CND, information security (INFOSEC), and CYBERCON support.
- d. Provide technical support to enable IO, and inform law-enforcement and counterintelligence units about activities occurring on Army in Europe ISs when appropriate.
- e. Identify critical points of failure and other potential vulnerabilities in computer networks and recommend network-security infrastructure improvements.
- f. In coordination with E-TNOSC, provide briefings on vulnerability findings and recommend computer-security improvements.

g. Request AO approval to perform penetration tests, conduct network threat assessments and analyses, report indications of events that may adversely affect Army in Europe operations, and recommend protective measures to 5th Sig Cmd.

h. Develop and publish Army in Europe incident-response procedures, checklists, and guidelines.

i. Oversee, assist with, and report the status of security-incident mediation in coordination with 5th Sig Cmd, the Army in Europe IAPM, E-TNOSC, NECs, and supporting signal battalions.

j. Coordinate with the USAREUR G3 and the 5th Sig Cmd G3 to request IOVAD program services.

k. Participate as a member of the Army in Europe IA and CND, CCB, and USAREUR G3 IO workgroups.

12. INFORMATION ASSURANCE MANAGERS

In addition to the responsibilities listed in AR 25-2, paragraph 3-2d, IAMs will—

a. Be appointed in writing at each major subordinate command, joint task force, brigade, and equivalent units.

b. Ensure required Army in Europe training on the use of personal electronic devices and removable media storage devices, protection of personally identifiable information (PII), phishing awareness, universal serial bus (USB) drive security, and home computer security is completed.

c. Ensure users pass the annual IA awareness training posted on ATCTS and maintain their signed Acceptable-Use Policy (AUP) Agreement and certificates of training in their personnel records.

d. Ensure personnel with privileged access to an IS have been appointed in writing by an authority equal to the level of access provided. This includes users with administration privileges on their local user systems.

e. Establish an ISSP account to help commanders meet IA and communications security (COMSEC) requirements (MS4X and MX5T), and ensure proper validation and data entry in the ISSP. All entries must be validated with subactivity and subordinate command requirements.

f. Ensure that IT position levels (for example, IT-I, IT-II, IT-III, IT-IV) are identified.

g. Ensure that all users create ATCTS and AE-ITT accounts, and manage ATCTS accounts for their assigned IA personnel at <https://atc.us.army.mil/iastar/index.php>.

h. Request specific network scans in coordination with E-TNOSC and RCERT-E, and report the results to the Army in Europe IAPM and the supporting signal battalion.

13. INFORMATION ASSURANCE SUPPORT OFFICERS

Information assurance support officers (IASOs) will be appointed at all battalion and equivalent-level units, and in lieutenant colonel and equivalent-level staff offices. IASOs will maintain an appointment memorandum (AR 25-2, chap 2-2) in ATCTS and will be assigned to the lowest IA-management level. Enough IASOs will be appointed to effectively execute the responsibilities in this paragraph.

NOTE: The position title “information assurance security officer” has changed to “information assurance support officer” in ATCTS. The former title is no longer used. IASO positions previously associated with the IAM-I category in ATCTS are now in a separate category. IASO responsibilities are not technical or managerial in nature. Therefore, IASOs no longer need IA certification and no vouchers will be provided for certification testing of IASOs. IASOs currently executing technical duties and responsibilities must be reappointed as IA Technician Level I or II based on the functions and tasks they perform. Updated information must be documented in ATCTS.

a. The main role of the IASO is to provide IA oversight, guidance, and support to general users in accordance with the requirements of the command’s IA program. IASOs must be familiar with IA policy, guidance, and training requirements according to AR 25-2, and best business practices.

b. IASOs must successfully complete the Information Assurance Fundamental Course (at <https://ia.signal.army.mil/courses.asp>). This training will be documented in ATCTS.

c. IASOs will—

(1) Verify that all requirements for access to ISs are met and that signed AUP Agreements are kept on file.

(2) Help prepare, coordinate, distribute, and maintain plans, instructions, policy, guidance, and standing operating procedures (SOPs) that are necessary to implement the command IA program, and serve as the subject-matter focal point for the program.

(3) Ensure that supported users receive initial and annual IA awareness training by verifying completion in ATCTS or organization-specific systems. The IASO will report noncompliance to the supporting IAM.

(4) Help the IAM prepare and maintain C&A packages (tactical and garrison) according to DIACAP.

(5) Ensure that command or organization SOPs address the reporting of security violations and incidents to the RCERT-E in accordance with AR 25-2, section VIII.

(6) In coordination with the supporting IAM, ensure that the distribution of incident and security violation reports is not limited to the RCERT-E. Notification must be made in writing to all levels of leadership as established in the command’s policy and procedures.

(7) Help the supporting IAM develop and implement tenant support plans when in a garrison environment.

14. SYSTEM ADMINISTRATORS AND NETWORK ADMINISTRATORS

In addition to the responsibilities listed in AR 25-2, paragraph 3-3a, system and network administrators will—

a. Ensure that all systems are configured with the Army in Europe-approved AGM image.

b. Sign a privileged-level access agreement. The agreement must be uploaded and stored in ATCTS.

c. Meet DOD Directive 8570.01 compliance-certification training requirements for IA levels I, II, and III for their privileged accounts.

d. Ensure non-Army-in-Europe-approved baseline systems are configured using DISA STIGs. If deviation from the Army in Europe baseline or DISA STIGs is necessary, the system or network administrator will coordinate with the IAM to ensure analysis, approval, and documentation is completed before the system is configured.

e. Coordinate with the servicing NEC and IAM when adding new or newly rebuilt networked systems to the network. The system or network administrator must use the approved configuration-management process and submit a 119 trouble ticket to track the change and approval process.

f. Provide operational and technical IA support for the Army in Europe.

15. DATA OWNERS

In addition to the responsibilities listed in AR 25-2, paragraph 3-3b, data owners will—

a. Carefully configure access permission to all data not cleared for public release.

b. Limit the publishing and sharing of sensitive data to personnel with a clearly established need to know.

c. Require the use of two-factor authentication for access to sensitive data.

d. Document data-access requests and grant the minimum access privileges necessary to accomplish the mission.

e. Regularly audit access permissions to published and shared data to ensure users who no longer need access do not have access.

16. GENERAL USERS

In addition to the responsibilities listed in AR 25-2, paragraph 3-3c—

a. General users will—

(1) Complete the IA awareness training, pass the IA awareness test, and sign the AUP Agreement before being authorized network access.

(2) Show care in handling e-mail and web traffic.

(3) Refrain from opening unexpected or suspicious attachments.

(4) Report all suspicious e-mail traffic to the IAM or security manager.

(5) Digitally sign or encrypt e-mail messages that have weblinks.

(6) Digitally sign and encrypt all For Official Use Only (FOUO) information, controlled unclassified information, PII, and other sensitive data.

b. General users should—

(1) Practice good business processes when conducting Government business through commercial Internet channels. Official business should be conducted through official channels.

(2) Be extremely cautious when forwarding links or attachments, as they may contain unauthorized materials, protected data, and viruses.

SECTION III

ARMY IN EUROPE INFORMATION ASSURANCE POLICY

17. OVERVIEW

IA requirements and security checks must be addressed in all Army in Europe performance work statements and included on DD Form 254 for classified contracts.

18. FUNDING

In addition to the requirements listed in AR 25-2, paragraph 4-2—

a. The Army in Europe IAPM will—

(1) Manage funding for IA and COMSEC requirements.

(2) Issue instructions and taskings for submitting COMSEC and IA equipment requirements to HQDA. Urgent needs for COMSEC and IA products require an operational needs statement according to AR 71-9.

b. All Army in Europe organizations and tenant activities will request INFOSEC, COMSEC, and IA requirements through the ISSP.

19. IA TRAINING

a. The AE-ITT Program is the Army in Europe's primary source of IT and IA training. All USAREUR major subordinate and specialized commands and USAGs are required to use the AE-ITT program as the primary source for all instructor-led IT and IA training. The AE-ITT Program—

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

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

(3) Meets DODD 8570.01 requirements by providing certified trainers and a variety of IT and IA courses.

(4) Provides training centers that are certified test centers for Pearson Virtual University Enterprise and ProMetric certifications to meet commercial industry standards.

(5) Ensures the ATCTS is updated and accurately reports certifications required by DOD directives and the Federal Information Security Management Act.

(6) Aligns and updates course completions and certificates in ATCTS.

b. In addition to the requirements listed in AR 25-2, paragraph 4-3, Army in Europe IA personnel will complete—

(1) The IA training provided through the AE-ITT Program at <https://itt.eur.army.mil>.

(2) DOD IA awareness training and testing provided through the Fort Gordon website at <https://ia.signal.army.mil/dodiaa/default.asp>.

c. IA training will include—

(1) IA awareness training.

(2) Army minimum required training (as designated by IA category and level) identified in ATCTS.

(3) DOD baseline certifications according to DOD 8570.01-M.

(a) All Army in Europe personnel holding IA positions (full-time, part-time, or embedded) must obtain the required certifications within 6 months after assuming their duties to remain in their IA position. IA personnel may use the cost-free AE-ITT certification program to acquire the mandated certifications. Failure to acquire the required certifications may result in removal from the position, permanent reassignment, or removal from Federal Service. For local national (LN) employees in Germany, these types of actions must meet the requirements of AE Regulation 690-64. Local human resources offices will provide more information.

1. Individuals who successfully complete the Army or AE-ITT certification preparation test will be provided a voucher for the certification examination.

2. One-time retraining and retesting is authorized.

(b) IA technicians and managers who are prepared for the certification test must coordinate with the PP&TB to schedule testing for their IA position. Testing for certified information security managers and certified IS security professionals must be coordinated with the test proponent (Information Systems Audit and Control Association or International Information Systems Security Certification Consortium).

(4) Computing-environment certification according to DOD 8570.01-M for IA training and Computer Network Defense-Service Provider (CND-SP) (except for CND-SP Manager) categories as identified by individual managers and supervisors.

(5) All individual IA training and certification requirements in appendix B.

20. MINIMUM IA REQUIREMENTS

In addition to the requirements listed in AR 25-2, paragraph 4-5—

a. All Army in Europe systems must be configured—

(1) To use the authorized antivirus program and receive automatic virus signature updates.

(2) With System Center Configuration Manager client and Host Based Security System client and configured to receive patch management updates.

b. Non-Army in Europe systems connecting to the Army in Europe network for exercises or temporary duty for no more than 60 days must meet certain minimum security requirements. They must—

(1) Have approved antivirus software installed and updated with the most current virus signatures.

- (2) Have all required operating system (OS) and software service packs and patches applied.
- (3) Require a DOD-compliant password if the system is not compliant with user-based enforcement.
- (4) Have all current DOD IAVA patches applied to be protected against known vulnerabilities.
- (5) Be configured to use the appropriate AGM, STIG, or Federal desktop core configuration baseline.
- (6) Be scanned to ensure they meet the requirements in (1) through (5) above before being connected to Army in Europe networks.

21. PROHIBITED ACTIVITIES

a. In addition to the prohibitions in AR 25-2, paragraphs 4-5(a)(1) through (9), the following activities are prohibited when using Army in Europe networks:

- (1) Viewing, changing, damaging, deleting, or blocking access to another user's private files without appropriate authorization. This does not apply to another user's files that are on a shared drive, shared portal, public drive, or similar location.
- (2) Using another person's account or identity.
- (3) Obtaining, installing, copying, storing, or using software outside the appropriate Army in Europe business procedures. This includes the use of freeware, shareware, and third-party or unapproved software.
- (4) Granting an unauthorized individual access to a Government-owned or -operated system.
- (5) Hacking into Army in Europe systems or using these systems to hack other systems.
- (6) Masking or hiding network identity.
- (7) Installing and using a modem without explicit approval from the AO.
- (8) Creating or forwarding chain or hoax e-mail messages.
- (9) Hosting personal homepages on Government computers (GCs) or servers.
- (10) Simultaneously connecting to a Government network and a commercial Internet service provider.
- (11) Installing a remote-access server.
- (12) Installing or using unauthorized network monitoring tools.
- (13) Installing or using personal firewalls.
- (14) Installing or using unauthorized wireless devices.
- (15) Installing or playing unauthorized games or simulations.

(16) Sending or forwarding e-mail messages with unauthorized links or attachments with executable files (for example, files with an extension of “.exe”). Users must ensure they know what they send or forward in order to protect sensitive data.

(17) Disclosing PII (for example, social security numbers (SSNs)) and other information protected by the Privacy Act from unauthorized disclosure (AR 340-21).

b. Users should not send or forward e-mail messages or Government data that is sensitive but unclassified, FOUO, classified, or otherwise restricted or protected through commercial Internet channels (for example, America Online (AOL), Facebook, Google, hotmail, Yahoo).

22. PUBLIC KEY INFRASTRUCTURE SOFTWARE SECURITY

a. Foreign liaison officials (FLOs) who have been properly vetted by a valid petitioner and require access to a DOD network to meet a DOD mission are eligible to receive a common access card (CAC). CAC issue and access to facilities or networks are allowed unless otherwise limited or prohibited under international agreements applicable in overseas locations. CACs issued to FLOs—

(1) Must support logical access to GC systems, if authorized.

(2) Will not provide any additional privileges, such as access to morale, welfare, and recreation services. These privileges may be granted only by separate provisions.

b. All official e-mail messages should be digitally signed, including messages originating from or sent to a BlackBerry. Failure to digitally sign a message exposes the network and users to increased risk in terms of data protection and the risk of social engineering.

c. Alternate smart card logon (ASCL) tokens are the alternative means of authentication for Army in Europe networks. The use of ASCL tokens is mandatory for all elevated NIPRNET accounts. DA administers the ASCL Program. ASCL tokens may be requested by contacting the DA Registered Authority (RA) at e-mail: army.ra@us.army.mil.

d. Webservers and domain controllers must be PKI-enabled to facilitate authentication and CAC cryptographic logon. Server and webserver certificates are referred to as equipment certificates.

(1) Fort Huachuca, Arizona, administers the Equipment Certificate Program. Instructions on how to obtain certificates are posted at <https://www.ctnosc.army.mil/documents/pki-general-instructions.pdf>. Before a certificate request may be submitted, the requesting organization must be nominated by the Army in Europe Identity Management Office. The requesting organization should send an e-mail message to usarmy.badenwur.usareur.mbx.pki-team-usareur@mail.mil to request a nomination.

(2) Role-based certificates are created and administered by the DA RA. To request role-based certificates, organizations must contact the DA RA office at e-mail: army.ra@us.army.mil.

e. Only USAREUR-approved or -mandated software may be used to enable certificate-status validation by DISA’s online certificate-status protocol technology. Such software will be installed on all GCs, domain controllers, webservers, BlackBerrys, and other equipment requiring certificate validation.

f. All Army in Europe GCs and servers must have the most current version of ActiveClient middleware installed.

g. CAC personal identification number (PIN) reset (CPR) stations will be used to reset CAC PINs. Each CPR station must have an assigned trusted agent security manager (TASM) and a CAC trusted agent (CTA). TASMs or properly assigned CTAs will conduct monthly updates of CPR systems according to the Defense Manpower Data Center Business Program Policy Document.

h. Commands managing Army in Europe contracts must establish two TASMs and designate two contracting officer's representatives (CORs) as trusted agents (TAs) to support their contractor verification system (CVS) programs. COR TAs—

- (1) Will use the CVS to process contract personnel for CAC issue.
- (2) Are responsible for entering and approving CVS actions for issuing CACs to contractors.

i. Commands managing Army in Europe volunteer access control (VOLAC) programs must establish two TASMs and designate personnel as VOLAC TAs in their geographic areas to support their CVS programs. VOLAC TAs—

- (1) Will use the CVS to process volunteers who have been properly vetted and approved for receipt of a CAC.
- (2) Are responsible for entering and approving CVS actions for issuing CACs to volunteers.

NOTE: More information about CVS programs is available at <https://www.us.army.mil/suite/kc/10342268>.

j. The Army in Europe enhances mission readiness with increased command oversight by implementing and enforcing the use of Secret Internet Protocol Router Network (SIPRNET) tokens for all SIPRNET users. This enhances security and ensures that Army in Europe commands comply with DA IA policies and regulations.

- (1) All new SIPRNET applicants requesting access to the EUR classified domain must be issued a SIPRNET PKI token.
- (2) Army in Europe organizations will ensure that two TAs have valid Secret clearances, are designated as TAs on appointment orders, and are trained to provide SIPRNET PKI tokens to personnel requiring tokens. Local registration authorities will validate, screen, and approve all requests.

23. TUNNELING SIPRNET TRAFFIC THROUGH OTHER THAN SIPRNET CONNECTIONS

a. General. Organizations in the Army in Europe may “tunnel” SIPRNET traffic through other than SIPRNET connections within a base area network (BAN) without obtaining a waiver from DISA.

NOTE: If the policy in this paragraph conflicts with higher directives, the higher directive will take precedence. Conflicting guidance should be brought to the attention of the PP&TB.

(1) Organizations that need to tunnel SIPRNET traffic through other than SIPRNET connections must contact their supporting signal battalion for coordination and assistance. Supporting signal battalion IAMs will coordinate with the Army in Europe IAPM ACA to validate the tunneling implementation.

(2) Organizations will minimize the tunneling of classified information through other than SIPRNET connections to the greatest extent possible.

(3) Where necessary, installation campus area networks (ICANs) and BANs without SIPRNET nodes may be tunneled to the nearest SIPRNET node in a signal battalion area of responsibility.

(4) SIPRNET traffic will not be tunneled across “long-haul” NIPRNET infrastructures unless approved by the DISA Classified Data Service Manager.

(5) Dedicated gateways must be installed between ICAN and BAN NIPRNET and SIPRNET nodes.

(6) All means of tunneling classified information through the NIPRNET must—

(a) Be compliant with the 5th Sig Cmd tunneling solutions.

(b) Remain within the Army in Europe’s four NIPRNET top-level architectures using existing NIPRNET infrastructures.

(7) When the following conditions are met, the Defense Information System Network security criteria outlined in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C are considered as being met:

(a) National Security Agency/Central Security Service-certified and -approved type-1 cryptography for data protection is used.

(b) The tunnel termination point is located in a facility authorized to process the classified information being tunneled when not encrypted (for example, a SIPRNET node facility).

(8) If compliance cannot be maintained according to (7) above, the connection used to tunnel the classified information will be disapproved and disabled.

b. Responsibilities.

(1) Army in Europe IAPM. The Army in Europe IAPM will—

(a) Determine a need for DISA waivers in the Army in Europe based on the interpretation of DISA guidance and CJCSI 6211.02C.

(b) Ensure all tunneling implementations, approvals, and waivers are annotated in applicable network certification and accreditation documentation.

(2) 5th Sig Cmd. 5th Sig Cmd will ensure that all means of tunneling classified information through the NIPRNET—

(a) Are compliant with existing tunneling solutions.

(b) Remain within the Army in Europe’s four NIPRNET top-level architectures using existing NIPRNET infrastructures.

(3) Supporting Signal Battalions. Supporting signal battalions will—

(a) Ensure dedicated gateways are installed between ICAN and BAN NIPRNET and SIPRNET nodes and coordinate with their NECs for support if needed.

(b) Ensure classified traffic tunneled through other than SIPRNET connections is routed to the nearest SIPRNET node in their area of responsibility (AOR).

(c) Govern all tunneling implementations in their AOR. This includes but is not limited to—

1. Verifying, approving, and managing justifications for tunneling requests.

2. Creating supporting diagrams (for example, network, connectivity, logical).

3. Managing information related to the approval of the DISA SIPRNET connection questionnaire as validated by the IAPM ACA.

NOTE: In the Army in Europe, signal battalions can support more than one geographic area, potentially crossing installation and garrison boundaries.

24. PASSWORD CONTROL

In addition to the requirements listed in AR 25-2, paragraph 4-12—

a. User-generated passwords for computer access must have at least 14 characters (15 for elevated-privilege accounts) and include 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters. The password must not include any words in a dictionary.

b. Passwords must be changed every 60 days on all classified systems, immediately if compromised, or when directed by CYBERCON measures.

c. Passwords must be changed every 90 days on all unclassified but sensitive systems, immediately if compromised, or when directed by CYBERCON measures.

25. PERSONNEL SECURITY STANDARDS

a. For the purpose of this regulation, FN and LN network users are synonymous. Activities that require network access for FN employees will ensure that all required documents are completed and processed for the user. AR 25-2, chapter 4-14, and the local IAM can provide specific information on required documents and current processes. The IAMs who serve the requiring activities will maintain supporting documentation and assist in completing electronic staff-action-summary packages to facilitate requests for network access in accordance with FN employee network-access procedures.

b. The requiring activity and the IAM must ensure that all requirements, including training and background investigations, are met.

NOTE: United States Army Civilian Human Resources Agency, Europe Region, FN and LN positions are thoroughly vetted as part of the hiring process, and the AO must first approve personnel in these positions for NIPRNET access before access is granted.

c. The activity requiring FN employee positions will ensure that all necessary security investigations (or clearance equivalent) required for assignments to positions designated as IT-II are completed before appointments to these positions are made.

d. Before preparing SF 86 for an FN, the requiring activity will contact the Defense Security Service to obtain a pseudo SSN for annotation on the individual's electronic personnel security questionnaire. FN employees will use the foreign identification number issued with their CAC.

e. The requiring activity will immediately inform the local IAM if the security status of the FN employee changes. The IAM will then revoke network or system access if the FN employee does not meet the minimum personnel-security standards outlined in AR 25-2, paragraph 4-14.

26. FOREIGN ACCESS TO INFORMATION SYSTEMS

a. In addition to the requirements listed in AR 25-2, paragraph 4-15, requests—

(1) To authorize a non-U.S. citizen access to the SIPRNET must be sent to the USAREUR G2 for concurrence and to the Army in Europe IAPM to ensure that the C&A documentation for the SIPRNET system being accessed is updated to indicate this authorization.

(2) For FLO NIPRNET access must be made using AE Form 25-2A.

b. Appendix C establishes policy and procedures for granting FLOs access to the Army in Europe NIPRNET.

27. CROSS-DOMAIN SECURITY INTEROPERABILITY

a. Commanders will submit requirements for cross-domain security solutions to the Army in Europe IAPM.

b. Organizations will submit requests for cross-domain connections through the DISA Connection Approval Office. Cross-domain connections will not be allowed until the requesting organization receives an approved Global Information Grid interconnection request from the DISA Connection Approval Office.

28. NETWORK SECURITY

In addition to the requirements listed in AR 25-2, paragraph 4-16—

a. The E-TNOSC will configure exchange servers to quarantine e-mail attachments that have file extensions that are not listed in the Army in Europe-approved exchange baseline.

b. Requests to use unapproved IA tools must be sent through the Army in Europe IAPM to the AO for approval. Unless AO-approved, IA tools that are not on the Army-approved list are prohibited.

c. Any connection from or to a GC on an Army in Europe network must be only for official use. Network access to or from outside an Army in Europe IS to conduct official business and as authorized according to AR 25-1 is permitted using hypertext transfer protocol (HTTP) over port 80 and hypertext transfer protocol secure (HTTPS) over port 443 by 5th Sig Cmd proxy services. Exceptions to permit access using any other ports, protocols, or unproxied services for official Government business must be submitted through the Army in Europe IAPM to the AO for approval.

d. The 5th Sig Cmd will block outbound access to external Internet protocol (IP) ranges that are threatening to the Army in Europe IS. The IP list will be determined by the IA and CND workgroups or as directed by DA, DOD, or the United States Cyber Command.

29. PROTECTION OF CLASSIFIED INFORMATION

The use of removable media storage devices on SIPRNET computer terminals to download (write) classified material is prohibited. SIPRNET users will not be authorized write capability on the SIPRNET. Users who wish to request a waiver to this prohibition must submit a request to the 5th Sig Cmd Enterprise Service Desk for approval.

30. IAVM REPORTING PROCESS

In addition to the requirements in AR 25-2, paragraph 4-24—

a. The USAREUR G3, in coordination with the Army in Europe IAPM, will issue IAVA taskings to all units throughout the Army in Europe. For critical network threats requiring immediate action, the USAREUR G3, in coordination with the Army in Europe IAPM, may issue a “Dragon Lightning” alert. Technical information about each IAVA is available at <https://www.cybercom.mil/j3/iavm/default.aspx>.

b. Personnel responsible for remediation of IAVAs will acquire access to the Army Global Network Operations and Security Center reporting tool at <http://armynetcrop.army.smil.mil/protected/reporting> and report compliance using that tool.

31. COMPLIANCE REPORTING

In addition to the requirements in AR 25-2, paragraph 4-25, compliance and mitigation reporting for—

a. Command cyber-readiness inspections will be processed using the DISA Vulnerability Management System.

b. Department of the Army Inspector General (DAIG) inspections will be processed using documents and instructions provided by the DAIG team.

c. Force protection assessment team (FPAT) inspections will be processed using documents and instructions provided by the FPAT.

32. WIRELESS LOCAL AREA NETWORKS

In addition to the requirements in AR 25-2, paragraphs 4-30—

a. The existence of wireless technology (for example, scanners, personal digital assistants) must explicitly be identified and described in the site’s C&A documentation. Assistance to customers in the Army in Europe will be provided by the unit’s IAM and supporting IA specialist or the Army in Europe IAPM. This assistance will include the required certification testing before accreditation. Guidance for deploying wireless networks in the Army in Europe is available at <https://portal.eur.army.mil/sites/iassure/default.aspx>.

(1) NECs will scan for unauthorized wireless devices each month. Scans will include frequency-spectrum scanning to detect active wireless network interface cards and access points. Given the small size of Army in Europe installations and the proximity to the local community, unauthorized devices may be difficult to locate. NECs will use the results of the spectrum scans and cross-reference them to the mission-assurance category addresses of devices attached to the network.

(2) NECs are authorized to detect the presence of unauthorized devices, but are not authorized to monitor traffic on wireless networks at any time. Failure to adhere to this policy may result in administrative action and host-nation action by local authorities. If an NEC suspects or confirms an unauthorized wireless device attached to an Army in Europe network, the NEC will immediately report it through appropriate channels to the Army in Europe IAPM.

b. All requests to use wireless devices must be sent to the Army in Europe IAPM and coordinated with the 5th Sig Cmd G3 for engineering, evaluation, and approval. Each request must support an operational or mission need that cannot be met without the use of the proposed wireless IS. Requesting units must coordinate with the Frequency Management Branch, Architecture Division, Office of the G3, 5th Sig Cmd. Units will not purchase or install equipment without Army in Europe IAPM review and AO approval.

c. The Army in Europe IAPM will certify that the device meets spectrum supportability and Military Communications-Electronics Board standards, and the requirements of DOD Directive 5000.01, AR 5-12, and the host nation.

d. The use of Bluetooth technology with Government devices (including cell phones) is prohibited except for Bluetooth CAC readers for unit-issued BlackBerrys.

e. Appendix D provides policy for implementing wireless infrastructure.

33. CERTIFICATION AND ACCREDITATION OVERVIEW

In addition to the requirements listed in AR 25-2, paragraph 5-1, accreditation of classified systems will include a facility TEMPEST technical assessment. Certification agents must submit requests in accordance with AR 380-27 and AE Regulation 380-85.

34. CERTIFICATION

In addition to the requirements listed in AR 25-2, paragraph 5-2, organizations introducing new COMSEC equipment into the European theater must consult the United States Army Communications Security Logistics Agency IA adviser (assigned to the USAREUR G2) and the National Security Agency IA liaison officer (assigned to the Army in Europe IAPM) to ensure current and future cryptographic requirements are addressed.

35. ACCREDITATION

The Army in Europe IAPM will help units prepare local accreditation packets that meet the requirements in AR 25-2, paragraph 5-4.

a. AO-approved accreditation packets will be sent directly to the unit's supporting NEC. The unit's IAM is the primary unit POC for accreditation issues.

b. The NEC will keep copies and track the status of all accreditation packets in its AOR.

36. CONNECTION-APPROVAL PROCESS

Units preparing C&A documents in accordance with published Army in Europe processes and templates (SOPs and checklists) must comply with AR 25-2, paragraph 5-7; and DISA connection-approval process requirements.

37. CYBERCON

a. Changes to CYBERCON levels are normally specified by DA but may be declared by the USEUCOM J3 and USAREUR G3 acting on behalf of the Army service component command of USEUCOM. Subordinate commands may implement more stringent CYBERCON measures, but will not decrease any CYBERCON measures imposed by a higher headquarters or authority.

b. USEUCOM Directive 25-5, appendix H, describes CYBERCON levels and response measures.

c. AR 25-2, paragraph 7-1, provides more information about CYBERCONs.

38. PERSONALLY IDENTIFIABLE INFORMATION

a. All PII will be evaluated for loss or unauthorized disclosure and protected accordingly.

b. All electronic PII records will be assigned a high or moderate “PII impact category” and protected at a confidentiality level of sensitive or higher unless specifically cleared for public release.

(1) Electronic PII records assigned a high-impact category must not be routinely processed or stored on mobile computing devices or removable electronic media without the express approval of the AO.

(2) Except for compelling operational needs, mobile computing devices and removable electronic media that process or store high-impact electronic records must be restricted to workplaces that meet at least the physical and environmental controls for the confidentiality level of sensitive.

c. Mobile computing devices storing high-impact electronic records that are removed from protected workplaces, including those approved for routine processing, must—

(1) Be signed in and out with a supervising official designated in writing by the organization security official.

(2) Require certificate-based authentication using a DOD or DOD-approved PKI certificate on an approved hardware token to access the device.

(3) Implement IA control PESL-1 (screen lock) with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

(4) Encrypt all data at rest (DAR) (that is, all hard drives or other storage media in the device and all removable media created by or written from the device) while outside a protected workplace. The cryptography must meet the certification standards of the National Institute of Standards and Technology (for example, Federal Information Processing Standards Pub 140-2 or higher).

d. All PII and DAR must be encrypted using DA encryption software for mobile devices, desktops, or remote storage manager (RSM) devices. Stand-alone portable RSM devices that cannot be encrypted using DA encryption technologies will not be used to store sensitive data or PII.

e. All program managers and system integrators who manage systems with sensitive information or PII will update information and provide guidance to users to incorporate the DAR encryption solution for their respective ISS or networks.

39. INDIVIDUAL AND ORGANIZATIONAL ACCOUNTABILITY

a. Users of Army in Europe information and assets are responsible for protecting this information and these assets. The standards for the protection of DOD information systems is in the DOD 8500-series directives and instructions, DOD 5200.1-R, AE Pamphlet 25-25, and supplemental Army in Europe policy and procedures. Military and civilian personnel who knowingly, willfully, or negligently compromise, damage, or place at risk Army in Europe data or information systems through a violation of AR 25-2, AR 340-21, AR 380-5, or paragraph 19 of this regulation may be subject to administrative, nonjudicial, or judicial sanctions.

(1) Sanctions for military personnel may range from oral or written warnings or reprimands to administrative measures or nonjudicial or judicial punishment authorized by the Uniform Code of Military Justice.

(2) Sanctions for civilian personnel may include oral or written warnings or reprimands, adverse performance evaluations, or suspension from work. Sanctions may also include prosecution in a court of law.

(3) Defense contractors are responsible for ensuring employees perform under the terms of the contract and applicable directives, laws, and regulations, and must maintain employee discipline.

b. Commanders may choose to impose nonpunitive actions, such as suspending the offender's access to classified or unclassified networks, or requiring the offender to repeat required training (for example, IA awareness training and examination).

40. INTERNET-BASED CAPABILITIES

In March 2010, the Army CIO/G-6 issued guidance that authorized access to Internet-based capabilities (IBCs), including network-based collaborative technologies (also known as social media tools), through the Army NIPRNET. As a result, access to social networking systems (SNSs) such as Facebook, MySpace, Twitter, and YouTube has been enabled on the Army in Europe NIPRNET. Personal use of GCs to access SNSs is authorized according to DOD 5500.7-R and AR 25-1.

a. SNSs provide a means of communication and information-sharing among users with similar interests. Users, however, should be aware of the dangers associated with using new capabilities. When accessing SNS portals from a GC, the GC may be exposed to—

(1) Address and identity spoofing.

(2) Cookies that, when placed on the system, may redirect the GC to questionable sites.

(3) Malware.

(4) Session hijacking.

b. Visiting SNS sites raises serious security concerns, since these sites are accessible to enemies who try to compile information of use to them. For this reason, the following must never be disclosed on these sites:

(1) Classified or FOUO information.

(2) Information considered essential elements of friendly information.

- (3) Information identified on current critical information lists.
- (4) Information protected by the Privacy Act.
- (5) Information regarding incidents under investigation.
- (6) Information related to Government acquisitions or contracts.
- (7) Information that if disclosed would adversely affect the interests of the U.S. Government, DOD, DA, USEUCOM, USAREUR, or U.S. allies.
- (8) Mission-essential information.
- (9) PII.
- (10) Sensitive information, such as casualty information before the next of kin has been formally notified by the military Service concerned.

NOTE: Local public affairs offices can provide additional guidance on SNSs.

c. During periods of heightened network activity, the Army in Europe may minimize nonmission-essential activity on its networks. When such an order is in effect, personal use of GCs on Army in Europe networks is prohibited except for e-mail messages between deployed Soldiers and their Families.

d. The Army in Europe IAPM has developed SNS training that is available to all DOD employees and their Family members.

(1) Commanders will encourage and facilitate participation in this dynamic training, which addresses the evolving challenges and risks of using IBCs. Commanders will also designate at least one representative who will become the SNS trainer for their organization through the “train-the-trainer” program offered by the AE-ITT Program at <https://itt.eur.army.mil>. This train-the-trainer program provides designated SNS trainers the material they will need to conduct training in their organizations.

(2) In addition to classroom and online SNS training, the mandated annual OPSEC and Threat Awareness and Reporting Program training will include training on the use of SNSs.

e. Appendix E provides guidance on the official and unofficial use of IBCs and a list of collaborative technologies.

41. DEFENDING CYBERSPACE

Commanders must protect and defend cyberspace as vigilantly as they would protect and defend any other area of operation. All communications over military networks are subject to monitoring. A risk imposed by one is a risk assumed by all. Appendix F provides a guide for defending cyberspace.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

Code of Federal Regulations, Title 5, part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

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

DOD Directive 5000.01, The Defense Acquisition System

DOD Instruction 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP)

DOD 5200.1-R, Information Security Program

DOD 5500.7-R, Joint Ethics Regulation (JER)

DOD 8570.01-M, Information Assurance Workforce Improvement Program

AR 5-12, Army Management of the Electromagnetic Spectrum

AR 25-1, Army Knowledge Management and Information Technology

AR 25-2, Information Assurance

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

AR 71-9, Warfighting Capabilities Determination

AR 340-21, The Army Privacy Program

AR 360-1, The Army Public Affairs Program

AR 380-5, Department of the Army Information Security Program

AR 380-10, Foreign Disclosure and Contacts With Foreign Representatives

AR 380-27, Control of Compromising Emanations

AR 380-67, Personnel Security Program

AR 530-1, Operations Security (OPSEC)

USEUCOM Directive 25-5, Information Assurance

AE Regulation 380-85, Technical Counterintelligence Services

AE Regulation 604-1, Local National Screening Program in Germany

AE Regulation 690-64, Standards of Conduct, Corrective Actions, Termination Process, and Grievances (Local National Employees in Germany)

AE Pamphlet 25-25, Army in Europe Information Technology Users Guide

Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>)

Defense Information Systems Agency Security Technical Implementation Guides (<http://iase.disa.mil/stigs/>)

SECTION II FORMS

SF 86, Questionnaire for National Security Positions

DD Form 254, Contract Security Classification Specification, Department of Defense

DD Form 1172-2, Application for Identification Card/DEERS Enrollment

DD Form 2875, System Authorization Access Request (SAAR)

DA Form 2028, Recommended Changes to Publications and Blank Forms

AE Form 25-2A, Army in Europe Foreign Liaison Official Unclassified Network Access Request

**APPENDIX B
CONSOLIDATED INFORMATION ASSURANCE TRAINING AND CERTIFICATION
REQUIREMENTS**

| Army in Europe Information Assurance (IA) Training and Certification Requirements | | | | | |
|--|--|--|--|--|--|
| Echelon | Frequency | Position | Course Title or Training | Reference | Training Proponent |
| Individual | Annual | Computer user | DOD Information Assurance Awareness Training Must sign Acceptable-Use Policy Agreement | AR 25-2, paragraphs 3-3c and 4-3(8)(a) AE Pamphlet 25-25 AE-ITT website at https://itt.eur.army.mil | Information Assurance Program Manager (IAPM) |
| Individual | As required | IA manager, IA support officer, and any person with elevated privileges on Army in Europe networks | 1) Must meet Army minimum required training according to Army Training and Certification Tracking System (ATCTS) and IA Best Business Practice not later than 6 months after appointment to the IA position 2) DOD-approved baseline certification 3) Information Assurance Management and Support Staff Course | AR-25-2, paragraph 3-2(f) DOD 8570.01-M, paragraph 3.4.2 DOD 8570.01-M, table AP3.T1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | As required | System administrator and network administrator | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Information Assurance Security Course (IASC) 3) DOD-approved baseline certification 4) Must obtain computing environment operating system (OS) certification | AR 25-2, paragraph 3-3(a) DOD 8570.01-M, paragraph 3.3.1 DOD 8570.01-M, table AP3.T1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA technical level I position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) Network+/A+ offered through AE-ITT Program/Certified Training Program (CTP) 4) Must obtain computing environment OS certification | DOD 8570.01-M, paragraph 3.3.1 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 3.2.4.8.3 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA technical level II position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) IASC above will meet the requirement through AE-ITT Program/CTP 4) Must obtain computing environment OS certification | DOD 8570.01-M, paragraph 3.4 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 3.4.1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |

| Army in Europe Information Assurance (IA) Training and Certification Requirements | | | | | |
|---|--|---|---|--|--------------------|
| Echelon | Frequency | Position | Course Title or Training | Reference | Training Proponent |
| Individual | Not later than 6 months after assuming IA position | IA technical level III position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) Certified Information Systems Security Professional (CISSP) offered through AE-ITT Program/CTP 4) Must obtain computing environment OS certification | DOD 8570.01-M, paragraph 3.5 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 3.5.1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA management level I position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) IASC above will meet the requirement through AE-ITT Program/CTP | DOD 8570.01-M, paragraph 4.2 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 4.3 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA management level II position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) CISSP/Certified Information Security Manager (CISM) offered through AE-ITT Program/CTP | DOD 8570.01-M, paragraph 4.4 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 4.4.1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA management level III position | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Must complete DOD-approved baseline certification 3) CISSP/CISM offered through AE-ITT Program/CTP | DOD 8570.01-M, paragraph 4.5 DOD 8570.01-M, table AP3.T1 DOD 8570.01-M, paragraph 4.5.1 ATCTS website at https://atc.us.army.mil/iastar/index.php AE-ITT website at https://itt.eur.army.mil | IAPM |
| Individual | As required | Designated approving authority (DAA) | 1) Must meet Army minimum required training according to ATCTS not later than 6 months after appointment to the IA position 2) Complete DOD DAA computer-based training or web-based training located on the DOD IA portal not later than 60 days after assignment to the position | DOD 8570.01-M, paragraph 5.1 AR 25-2, paragraph 5-8 DAA training at http://iase.disa.mil/ | IAPM |
| Individual | Not later than 6 months after assuming IA position | IA personnel with elevated privileges on networks | Do-It-Yourself Vulnerability Assessment Program course available from Regional Computer Emergency Response Team - Europe (RCERT-E) | AR 25-2, paragraph 4-28j | RCERT-E |

NOTE: Individuals filling the positions listed above (except computer users) must be appointed in writing. Additional Army in Europe training requirements must be completed 1 year before appointment. More information on training requirements is available at <https://portal.eur.army.mil/sites/iassure/default.aspx>.

APPENDIX C

GRANTING FOREIGN LIAISON OFFICIALS ACCESS TO ARMY IN EUROPE NETWORKS

C-1. GENERAL

a. This appendix—

(1) Provides procedures for granting foreign liaison officials (FLOs) access to the Army in Europe NIPRNET.

(2) Must be used with AR 25-2 and AR 380-67.

(3) Does not address the Army Knowledge Online (AKO) or Defense Knowledge Online (DKO) account-request process. AKO and DKO websites provide instructions on how to request AKO and DKO accounts.

b. Following the procedures in this appendix will ensure that—

(1) Army networks are secure from unauthorized access.

(2) Authorized access to networks is properly monitored, documented in applicable network certification and accreditation (C&A) packages, and approved by the USAREUR Designated Approving Authority (AR 25-2, para 4-14c).

c. The procedures in this appendix are based on DOD and DA directives. If anything in this appendix conflicts with higher level directives, the higher level directive will take precedence. Conflicting guidance should be brought to the attention of the Policy, Programs, and Training Branch (PP&TB), Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR, at e-mail: usareur.iapm@us.army.mil.

C-2. APPLICABILITY

This appendix applies to all FLOs assigned to Army organizations in Europe.

C-3. PROCEDURES

AE Form 25-2A must be used to ensure requirements in Army and AE regulations are met. This form provides a means for requesting, controlling, and managing FLO network access. The form can be downloaded from the Army in Europe Library & Publishing System (AEPUBS) at <https://aepubs.army.mil/>.

a. The steps and definitions below explain the requirements, responsibilities, and roles of those involved in managing FLO access to Army in Europe networks. For the purpose of this appendix, “network user” is defined as the FLO requesting access to Army in Europe networks.

(1) Step 1, Unit Information Assurance Manager (IAM). The unit IAM will—

(a) Download AE Form 25-2A from AEPUBS.

(b) Complete the *User Information* section on behalf of the FLO with information provided about the level of network access being requested.

(2) Step 2, U.S. Supervisor. The U.S. supervisor is the immediate supervisor of the FLO and the approving authority for requesting network access for FLOs. The U.S. supervisor must understand the requirements of the position the FLO will occupy as a network user and must verify that the network-access request is valid. The U.S. supervisor and the U.S. sponsor must not be the same person. The U.S. supervisor will—

- (a) Complete the *Supervisor/Commander* section of AE Form 25-2A.
- (b) Sign the *Supervisor/Commander* section of AE Form 25-2A.
- (c) Send the form to the unit security manager for processing related to the background-investigation verification.

(3) Step 3, Unit Security Manager. The G2 or S2 security manager of the U.S. sponsor will—

(a) Verify the status of the network user's background investigation, security clearance, or both, if applicable. The security manager is responsible for ensuring that personnel-security procedures are followed. If the status of the background investigation or security clearance cannot be verified, the security manager will initiate required investigation processes.

- (b) Complete the *Unit Security Manager* section of AE Form 25-2A.
- (c) Sign the *Unit Security Manager* section of AE Form 25-2A.
- (d) Send the form to the unit information assurance manager (IAM).

(4) Step 4, Unit IAM. The unit IAM will—

- (a) Complete the *IAM* section of AE Form 25-2A.
- (b) Certify the information entered in all sections of the form.
- (c) Verify that the network user has signed the Acceptable-Use Policy Agreement.
- (d) Validate that the network user has completed all required training.
- (e) Conduct and document annual reviews of network users to verify that required annual training is completed, active-directory account expiration dates are current, and account requirements are still valid.
- (f) Keep a copy of the completed AE Form 25-2A until the network user leaves the unit.

b. The following additional steps must be taken if the FLO will require a common access card (CAC) for computer access:

(1) Step 1, U.S. Sponsor. The U.S. sponsor will—

(a) Contact the Status of Forces Agreement (SOFA) Policy Officer, Military Personnel Branch, Office of the Assistant Chief of Staff, G1, IMCOM-Europe, at DSN 496-5804 to determine if the FLO may be issued a CAC. The PP&TB cannot validate the need for a CAC.

(b) Once confirmation is received from the SOFA Policy Officer, send a digitally signed and encrypted e-mail message stating “FLO Network Access” in the subject line to usarmy.badenwur.usareur.mbx.pki-team-usareur@mail.mil. A completed AE Form 25-2A must be attached to the e-mail message.

(c) After receiving network-access validation from the PP&TB, prepare DD Form 1172-2 for the network user to request a CAC. The form and instructions on completing it are available at <https://portal.eur.army.mil/sites/iassure/default.aspx>.

(d) Send a digitally encrypted copy of the completed DD Form 1172-2 by e-mail to usarmy.badenwur.usareur.mbx.pki-team-usareur@mail.mil.

(e) Take the network user and the DD Form 1172-2 to the nearest ID card office to finalize the CAC-issuance process.

(2) Step 2, PP&TB. The PP&TB will—

(a) Keep a copy of AE Form 25-2A for each approved FLO request.

(b) Validate the FLO’s requirement for network access if requested by the SOFA Policy Officer ((1)(a) above).

(c) Act as the liaison between the SOFA Policy Officer and the U.S. sponsor for network-access validation.

C-4. ENFORCEMENT

A policy is effective only if enforced. Commanders, policy-enforcement officers, network enterprise center IAMs, unit IAMs, information assurance officers, system administrators, information management officers, and security managers are essential to the security of Army in Europe information systems and networks. All of them will enforce the policy in AR 25-2 and in this regulation.

APPENDIX D

WIRELESS INFRASTRUCTURE IMPLEMENTATION POLICY

5th Signal Command has established the following baseline for wireless infrastructure in the Army in Europe:

- a. Wireless solutions to be procured must be compatible with the existing wired infrastructure. Wireless solutions must have a certificate of worthiness and the approval of the USAREUR Designated Approving Authority.
- b. Wireless local area network (LAN) solutions must use certified Federal Information Processing Standards Publication 140-2 encryption products in configurations approved by the Army Information Assurance Office.
- c. Current and future wireless infrastructure products must be on the existing host-nation (HN) frequency. Systems in use that are not on the HN frequency must be immediately reported to the local network enterprise center (NEC) service provider. NEC service providers will be required to mediate in finding a solution to the problem, and systems must be disconnected until the problem is corrected.
- d. Existing wireless infrastructures connected to an Army in Europe LAN must meet the same certification and accreditation (C&A) security requirements as all other wired LAN information systems approved for use by the Army in Europe. All wireless systems must be documented in the C&A documentation and reported to the local NEC. Units will work with local NECs to ensure systems are certified and accredited. If a system is not certified and accredited, it must be disconnected from the Army in Europe network.
- e. Wired and wireless infrastructures will share the same management platform or the platforms they use must integrate seamlessly. Each wireless infrastructure must be configured with firewall and intrusion-detection and -prevention systems that allow for direct connection to the local wireless access point.
- f. Disparate “islands” of wireless network implementations are not permitted in Army in Europe worksite locations.
- g. Army in Europe wireless applications (for example, identification and location tracking systems, the Installation Access Control System, logistics support systems) must be compatible with and integrated into the Army in Europe wireless infrastructure for wireless data-transport requirements. All units with special wireless application requirements must report their requirements to the local NEC.
- h. Wireless mobile devices capable of running antivirus software must have current antivirus software loaded and be compliant with information assurance vulnerability alerts (IAVAs). Wireless mobile devices capable of data storage must meet Army in Europe data-at-rest encryption requirements.
- i. All wireless systems not meeting Army in Europe standards will be removed to reduce the risk to Army in Europe networks.
- j. All wireless systems and infrastructure must have a current and approved Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). Offices with systems that do not have a current DIACAP will work with their local NEC to obtain DIACAP and will shut down systems until C&A is obtained.

k. Local Army in Europe NECs will manage wireless intrusion-detection systems and wireless infrastructure.

l. Units currently performing duties in support of wireless-infrastructure implementation will work with their local NECs to develop a plan to transition those responsibilities to the servicing NEC.

m. All maintenance of wireless infrastructure (access points and wireless intrusion-detection systems) such as installing firmware and hardware upgrades and processing configuration changes will be performed at the enterprise level.

APPENDIX E

USE OF INTERNET-BASED CAPABILITIES

E-1. GENERAL

Internet-based capabilities (IBCs), including social-media tools such as social networking systems (SNSs), provide significant new and attractive capabilities, but can also expose networks to serious harm. Commanders must ensure that personnel who use IBCs do not engage in activities that disrupt their duties or adversely affect network responsiveness. In addition, users of IBCs must understand that they may inadvertently release information to a community that extends well beyond their intended audience. For these reasons, users must follow operations security (OPSEC) and information assurance (IA) directives precisely as written.

E-2. SOCIAL MEDIA TOOLS

a. The use of official social media tools can greatly enhance mission effectiveness. When using these tools, it is imperative that IA, information security, and OPSEC measures be followed in accordance with AR 25-2, AR 380-5, and AR 530-1. Army personnel must safeguard classified and sensitive information in all online communications and must understand that online communications on the Internet are directed at the public. Contacts made through online communications with the public are unverifiable and therefore should not be trusted.

b. Official Government sites may be established on commercial social-networking venues to create a transparent information-sharing environment and gain feedback from the public only by exception. A waiver is required if websites, including social-media sites, on the Internet are being used beyond the exceptions in AR 25-1, which include education, public affairs, and recruiting. Requests for waivers must be submitted by the parent command to the Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR (e-mail: usareur.iapm@us.army.mil).

c. Organizations that want to implement social-media sites must contact the appropriate IA manager and Privacy Act official to learn about the risks associated with implementing the sites and to obtain advice on secure implementation.

d. Because of the potential of exploitation and other risks, all Army in Europe sites and accounts operating in an official capacity will not be used for personal use, must be linked to an Army Knowledge Online (AKO) e-mail address, and must never be used to communicate directly with Family, friends, or other official Army or Government representatives. Content posted on these sites by site administrators will not be of a political or discriminatory nature and will not endorse, appear to endorse, or show favoritism to nonfederal entities. Content or views posted on these sites by site administrators must comply with U.S. Government policy and may not appear to endorse views contrary to U.S. Government policy.

NOTE: Social-media tools are often used in environments that are not under the Army's direct control. Therefore, the individuals who use these tools are responsible for protecting sensitive information.

E-3. PROTECTION OF SENSITIVE AND CLASSIFIED INFORMATION

Social-media tools provide opportunities for adversarial groups, such as foreign intelligence services, to gather personal information for use in directly targeting Army in Europe users. All personnel in the Army in Europe have a personal and professional responsibility to ensure no information that may jeopardize Soldiers or be of use to enemies (including local criminal elements) is posted on public sites. Sensitive organizational information, including sensitive but unclassified information, must not be discussed on any externally facing site.

a. The requirements of the Information Security Program address the safeguarding and disclosure of classified and sensitive information. Both types of information will be afforded the level of protection against unauthorized disclosure commensurate with the level of classification and sensitivity assigned. Personnel in the Army in Europe are responsible for ensuring that classified and sensitive information and materials are protected from compromise.

b. Army in Europe commanders must maintain up-to-date critical information lists and must ensure that all employees are trained to protect sensitive information from public release. Commanders must ensure public affairs officers and website managers work closely with OPSEC officers to develop processes to prevent inadvertent disclosure of information, including the disclosure of sensitive but unclassified and For Official Use Only (FOUO) information, through the public domain.

c. OPSEC officers must ensure that their OPSEC orientation and annual refresher briefings include training on the vulnerabilities associated with the use of the Internet and SNSs. OPSEC officers who need assistance with developing materials to be included in command briefings should contact the USAREUR OPSEC Manager, Operations Effects (Information Operations), Heidelberg, Germany (DSN 370-6831/6832, civilian 06221-57-6831/6832). OPSEC officers may also contact the Army OPSEC Support Element, 1st Information Operations Command, at DSN (312) 221-4506/4785.

E-4. ESTABLISHING PERSONAL ACCOUNTS ON SOCIAL MEDIA SITES

a. Army in Europe personnel, Family members, and contractors may establish personal accounts on social-media sites. Personal accounts, however, should not be established with Government e-mail addresses, use Government logos, be used to conduct official business, release official agency information, or be used for any other official communication related to the employee's Government position or activities.

b. Personnel who use social-media technology must ensure that they comply with the rules in the Joint Ethics Regulation and the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635). These rules include prohibiting the release of nonpublic information, requiring appropriate disclaimers of opinions being expressed, and restricting the use of Government computers to access and manage personal sites during official duty time.

E-5. INFORMATION ON PUBLIC WEBSITES

Information on publicly accessible websites is subject to the policy and clearance procedures described in AR 360-1, chapter 5, for the release of information to the public. Furthermore, all organizations engaging in social media must consider records-management requirements as described in AR 25-400-2.

a. Individuals with an approved exception to establish and maintain official social-media sites on a commercial website must—

(1) Validate the security and management of the systems and networks to be used.

(2) Complete updated OPSEC training once a year as described in paragraph E-3c.

(3) Ensure the local public affairs office and the OPSEC office approve site content before it is released or otherwise disclosed.

b. Commanders must ensure that—

(1) Information posted on their public websites is not of use to enemies and does not jeopardize Soldiers or Army in Europe missions.

(2) Their personnel know how to protect sensitive information and personally identifiable information from unintended disclosure.

E-6. COLLABORATIVE TECHNOLOGIES

Table E-1 provides a list of command collaborative-technology terms.

| Table E-1 Collaborative Technologies | |
|---|---|
| Aggregator | A site that gathers information from multiple websites, typically through really simple syndication (RSS). Aggregators let websites remix the information from multiple websites (for example, by republishing all the news related to a particular keyword). |
| Blog | A frequently updated, chronologically ordered publication of personal thoughts and opinions with permanent links to other sources, creating a historical archive. Blogs may be published on personal websites or institutional websites as communication tools. |
| Mashup | A web application that combines data from more than one source into a single integrated tool (for example, the use of cartographic data from Google Maps to add location information to real-estate data from Craigslist, thereby creating a new and distinct web service that was not originally provided by either source). |
| Open-source software | Software developed in the public domain by multiple developers that is available for sharing, enhancing, and various other uses (for example, Linux, Pearl). |
| Peer-to-peer (P2P) computing | The direct sharing of files between personal computers using the web as the platform. Examples of P2P computing include BitTorrent, FreeNet, and Gnutella. P2P connections between users can form large networks that can also be used to distribute telephony in real time. |
| Perpetual beta | Software or a system that never leaves the development stage of beta. Perpetual beta is associated with the development and release of a service in which constant updates are the foundation for the habitability and usability of a service, as is common with many Web 2.0 applications. |
| Podcasts and vlogs | Online audio and video blogs that can be downloaded to personal computers or handheld devices (for example, iPods, MP3 players, wireless phones). These can be subscription-based or free and have single- or repeated-use content. |
| Really simple syndication | A group of web-feed formats used to push frequently updated content such as blog entries, news headlines, or podcasts to users' personal computers or devices. An RSS document, which is called a "feed," "web-feed," or "channel," has either a summary of content from an associated website or the full text. RSS enables people to keep up with their favorite websites in an automated way that is easier than checking them manually. |

| Table E-1 Collaborative Technologies (cont) | |
|--|--|
| Social bookmarking | A service (for example, del.icio.us, Furl) that allows users to store their favorite websites online. This is the collaborative equivalent of storing favorites or bookmarks within a web browser. Social-bookmarking services also allow users to share their favorite websites with others, making them a way to discover new websites or colleagues who share similar interests. |
| Social-networking system | An online networking platform that allows registered users to interact with other users for social or professional purposes (for example, Facebook, LinkedIn, MySpace). |
| Tag | A keyword or term associated with or assigned to a piece of information. Tags are often used to classify items such as blog posts, mapped locations, and photographs into specific categories or organizations. |
| Virtual worlds | A computer-based simulated environment intended for its users to inhabit and interact through avatars. This habitation is usually represented in the form of two- or three-dimensional graphical representations of humanoids (or other graphical or text-based avatars). Most virtual worlds allow for multiple users. The world being computer-simulated typically appears similar to the real world, including features such as communication, gravity, locomotion, real-time actions, and topography. Until recently, communication has been in the form of text, but now real-time voice communication using voice over Internet protocol is available. This type of virtual world is now most common in massively multiplayer online games. Examples include Active Worlds, Second Life, There, and Visual Internet Operating System. Examples of virtual environments that are not games per se and can include gaming are Entropia Universe, Kaneva, Red Light Center, and The Sims Online. Massively multiplayer online role-playing games include AdventureQuest, EverQuest, Guild Wars, Lineage, RuneScape, Ultima Online, and World of Warcraft. |
| Wikis | Collaborative publishing technology that allows multiple users to work on and publish documents online with appropriate version control. Wikis allow hypertext links to content in any form, enhancing user experience and interactions. |

**APPENDIX F
COMMANDER’S QUICK REFERENCE GUIDE TO DEFENDING CYBERSPACE**

| COMMANDER’S QUICK REFERENCE GUIDE TO DEFENDING CYBERSPACE | | |
|---|--|--|
| <p>Purpose: To provide commanders at all levels with a tool to identify and manage cyber risk. The Army in Europe network is a weapon system. Commanders must protect and defend cyberspace as vigilantly as they would protect and defend any other area of operation. All communications over military networks are subject to monitoring. A risk imposed by one is a risk assumed by all.</p> | | |
| <p>IAW AR 25-2, military and civilian personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policy and procedures. <i>Violations are listed in AR 25-2, paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5.</i></p> | | |
| KEY PROHIBITED ACTIVITIES | | |
| <p>Introducing unauthorized hardware/devices to Army in Europe networks</p> | <ul style="list-style-type: none"> • Personally owned computers • MP3 players (iPod, Zune, etc.) • GPS • PDAs/EBook readers • Smart phones • Digital cameras | <ul style="list-style-type: none"> • Unauthorized/personally owned wireless access points • Unauthorized/personally owned gaming consoles (XBOX, Wii, PS3, etc.) • Personally owned external hard drives • Any flash-based removable media |
| <p>Accessing prohibited Internet content types</p> | <ul style="list-style-type: none"> • Pornography • Auctions (eBay) • Chat/instant messaging • Gambling/gaming • Hacking/malware • Illegal drugs • Internet telephony (Skype, Vonage) | <ul style="list-style-type: none"> • Online storage • Pay to surf • Peer-to-peer (BitTorrent, Kazaa, etc.) • Personals/dating • Unauthorized software/software downloads • Proxy avoidance/anonymizer • Violence/hate/racism/terrorist themes |
| <p>Accessing information without proper authorization or valid need to know</p> | <ul style="list-style-type: none"> • Viewing/obtaining data/files/folders specifically identified as belonging to a person/office/area that is not within their area of responsibility (classified or unclassified) • Random searching/viewing of data and undue interest or downloading with no valid need-to-know – Think Wikileaks | |
| <p>Physically relocating systems between classification domains</p> | <ul style="list-style-type: none"> • Unauthorized burning of data to removable media on SIPRNET • Incorrect labeling of network equipment, wall jacks, and systems • Moving of data between SIPRNET to NIPRNET, BICES, or JWICS without using established air-gapping processes • Moving systems from a higher classification to a lower one | |
| <p>Disabling, modifying, or bypassing protective software and/or data logs</p> | <ul style="list-style-type: none"> • Unauthorized purging of system event logs, Internet browsing history, Internet cookies • Unauthorized enabling of restricted settings to bypass security measures (e.g., enabling USB ports) • Making modifications to a system that is involved with an incident-response event | |
| <p>Abuse of privileged access for non-mission-related tasks</p> | <ul style="list-style-type: none"> • Logging in with elevated credentials to conduct user-level tasks • Knowingly enabling restricted settings on systems for the specific purpose of bypassing system security measures • Browsing the Internet with elevated credentials | |
| <p>Unauthorized release of FOUO and higher information, including critical information list (CIL) data</p> | <ul style="list-style-type: none"> • Release, disclosure, transfer, possession, or alteration of information without the consent of the data owner, the original classification authority as defined by AR 380-5, the individual's supervisory chain of command, FOIA official, PAO, or disclosure officer • Classified message incident (spillage) • IP addresses, passwords, user names, VIP travel plans, etc. • Think Wikileaks | |
| <p>Forwarding official information to personal accounts</p> | <ul style="list-style-type: none"> • Sending work e-mail to personal e-mail accounts (Yahoo, Hotmail, Gmail, etc.) • Uploading/storage of work-related documents to commercial online data storage sites | |
| <p>Sharing account details</p> | <ul style="list-style-type: none"> • PINs and passwords • Permitting the use of remote access capabilities (VPN) through Government-provided resources by any unauthorized individual | |
| <p>Unauthorized commercial connections</p> | <ul style="list-style-type: none"> • Connecting to a commercial DSL/ISDN connection without a GIG waiver authorization letter as a minimum | |
| <p>Using systems for unlawful or unauthorized activities</p> | <ul style="list-style-type: none"> • Activities such as file-sharing of media, music, movies, photographs, or software that is protected by Federal or State law, including copyright or other intellectual property status • Bypassing network security controls | |
| <p>Installing/using unauthorized software</p> | <ul style="list-style-type: none"> • Keyloggers • Freeware/shareware • Hacker tools • Password cracking | <ul style="list-style-type: none"> • Network traffic-capturing tools • Peer-to-peer (Kazaa, Limewire, Napster) • Any software not on approved software list |

| | |
|---|--|
| <p>Identification and Reporting. Army in Europe networks are continuously monitored for unauthorized and suspicious activity. Commanders typically receive notification of violations through the unit information assurance manager (IAM). However, notification may also come from the Chief Information Officer/USAREUR G6, Army cyber crime investigative unit, Army counterintelligence, USCYBERCOM, or others.</p> | |
| <p>Commanders Response Actions – Training to Sanctions</p> | |
| <p>Military personnel</p> | <p>May include but are not limited to the following administrative actions:</p> <ul style="list-style-type: none"> • Oral or written warning or reprimand • Adverse performance evaluation • Loss or suspension of access to IS or networks and classified material and programs • Any administrative action authorized by Service directives and any nonjudicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ) |
| <p>Civilian personnel</p> | <p>Sanctions may be imposed only by civilian managers or military officials who have authority to impose the specific sanctions proposed. These may include but are not limited to some or all of the following administrative actions:</p> <ul style="list-style-type: none"> • Oral or written warning or reprimand • Adverse performance evaluation • Suspension with or without pay • Loss or suspension of access to IS or networks and classified material and programs • Any other administrative sanctions authorized by contract or agreement • Dismissal from employment and civil or criminal prosecution |
| <p>Contractor personnel</p> | <p>Leverage the contracting officer or designee as the liaison with the defense contractor for directing or controlling contractor performance. The contractor is responsible for disciplining contractor personnel, except when criminal misconduct is involved, which is outside the contractor's jurisdiction to address.</p> |
| <p>Commanders have authority to take immediate and necessary actions in response to prohibited activities. Personnel who violate procedures and standards established in AR 25-2 and the signed Acceptable-Use Policy (AUP) Agreement will be counseled and retrained. Violators may also be subject to the following administrative and punitive actions. In all instances, the command must assess if the incident is first reportable to counterintelligence IAW AR 381-12 or to law-enforcement authorities.</p> | |
| <p>First offense or simple error</p> | <ul style="list-style-type: none"> • Retake the IA Awareness training modules • Re-sign the current AUP Agreement and upload copies to the Army Training and Certification Tracking System (ATCTS) • Provide EXSUM and corresponding copies to the Army in Europe Information Assurance Program Manager (IAPM) within 7 workdays |
| <p>Second offense or serious error</p> | <ul style="list-style-type: none"> • Retake the IA Awareness training modules • Re-sign the current AUP Agreement and upload copies to ATCTS • Provide EXSUM and corresponding copies to the Army in Europe IAPM within 7 workdays • Letter of counseling by unit commander • Suspend network account until the required documentation has been received and corrective training has been completed and verified by the Army in Europe IAPM • Entry into Joint Personnel Adjudication System (JPAS) for violation • Consider UCMJ action |
| <p>Third offense or deliberate misconduct <i>Commanders can request the following supporting data from their IAM: user web-browser history; user .pst file, and files on desktop/hard drive</i></p> | <ul style="list-style-type: none"> • Retake the IA Awareness training modules • Re-sign the current AUP Agreement and upload copies to ACTCS • Provide EXSUM and corresponding copies to the Army in Europe IAPM within 7 workdays • Letter of counseling by unit commander • Suspension of network access for 30 days • Entry into JPAS for violation • Suspension of security clearance • Consider UCMJ action |
| <p>Setting the Example – How You Can Help Defend Cyberspace</p> | |
| <p>Set the example</p> | <p>The following list is not all-inclusive. For further information, see AE Pamphlet 25-25.</p> <ul style="list-style-type: none"> • Adhere to the guidelines of this checklist • Do not open unsolicited e-mail (open only from trusted or known sources) • Do not click on links embedded in e-mail (visit website directly) • Digitally sign official e-mail and encrypt when contents include sensitive information (FOUO, PII, OPSEC, and nonpublicly releasable information) • Do not send or forward e-mail with inappropriate content • Practice good OPSEC at work, at home, and online |
| <p><i>For further information, contact the Army in Europe IAPM at DSN 380-5207 or e-mail: iapm@eur.army.mil</i></p> | |

GLOSSARY

SECTION I ABBREVIATIONS

| | |
|-------------|---|
| 5th Sig Cmd | 5th Signal Command |
| ACA | Agent of the Certification Authority |
| AE | Army in Europe |
| AE-ITT | Army in Europe Information Technology Training |
| AEPUBS | Army in Europe Library & Publishing System |
| AGM | Army Golden Master |
| AKO | Army Knowledge Online |
| AO | authorizing official |
| AOR | area of responsibility |
| AR | Army regulation |
| ASCL | alternate smart card logon |
| ATCTS | Army Training and Certification Tracking System |
| AUP | Acceptable-Use Policy |
| BAN | base area network |
| C&A | certification and accreditation |
| CAC | common access card |
| CCB | configuration control board |
| CFR | Code of Federal Regulations |
| CIO | chief information officer |
| CISM | certified information security manager |
| CISSP | certification information systems security professional |
| CJCSI | Chairman of the Joint Chiefs of Staff instruction |
| CND | computer network defense |
| CND-SP | Computer Network Defense-Service Provider |
| COMSEC | communications security |
| COR | contracting officer's representative |
| CPR | common access card personal identification number reset |
| CRV | cyber-readiness visit |
| CTA | common access card trusted agent |
| CTP | certified training program |
| CVS | contractor verification system |
| CYBERCON | cyber condition |
| DA | Department of the Army |
| DAA | designated approving authority |
| DAIG | Department of the Army Inspector General |
| DAR | data at rest |
| DIACAP | Department of Defense Information Assurance Certification and Accreditation Process |
| DISA | Defense Information Systems Agency |
| DKO | Defense Knowledge Online |
| DOD | Department of Defense |
| DSN | Defense Switched Network |
| E-TNOSC | Europe - Theater Network Operations and Security Center |
| FIPS | Federal Information Processing Standards |

| | |
|-----------------|--|
| FLO | foreign liaison official |
| FN | foreign national |
| FOUO | For Official Use Only |
| FPAT | force protection assessment team |
| G1 | deputy chief of staff, G1 (personnel) |
| G2 | deputy chief of staff, G2 (intelligence) |
| G3 | deputy chief of staff, G3 (operations) |
| GC | Government computer |
| HN | host nation |
| HQ | headquarters |
| HQDA | Headquarters, Department of the Army |
| HTTP | hypertext transfer protocol |
| HTTPS | hypertext transfer protocol secure |
| IA | information assurance |
| IAM | information assurance manager |
| IAPM | information assurance program manager |
| IASC | Information Assurance Security Course |
| IASO | information assurance support officer |
| IAVA | information assurance vulnerability alert |
| IAVM | information assurance vulnerability management |
| IBC | Internet-based capability |
| ICAN | installation campus area network |
| IMCOM-Europe | United States Army Installation Management Command, Europe Region |
| IMCOM-Europe G1 | Office of the Assistant Chief of Staff, G1, United States Army Installation Management Command, Europe Region |
| INFOSEC | information security |
| IO | information operations |
| IOVAD | Information Operations Vulnerability Assessments Division, 1st Information Operations Command |
| IP | Internet protocol |
| IS | information system |
| ISSP | information system security program |
| IT | information technology |
| J3 | director of plans and operations |
| LN | local national |
| NEC | network enterprise center |
| NIPRNET | Unclassified but Sensitive Internet Protocol Router Network |
| OPSEC | operations security |
| OS | operating system |
| P2P | peer-to-peer |
| PDS | protected distribution system |
| PII | personally identifiable information |
| PIN | personal identification number |
| PKI | public key infrastructure |
| POC | point of contact |
| PP&TB | Policy, Programs, and Training Branch, Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, Headquarters, United States Army Europe |
| RA | [Department of the Army] Registered Authority |

| | |
|---------|--|
| RCERT-E | Regional Computer Emergency Response Team - Europe |
| RSM | remote storage manager |
| RSS | really simple syndication |
| S2 | intelligence officer |
| SF | standard form |
| SIPRNET | Secret Internet Protocol Router Network |
| SNS | social networking system |
| SOFA | status of forces agreement |
| SOP | standing operating procedure |
| SSN | social security number |
| STIG | security technical implementation guide |
| TA | trusted agent |
| TASM | trusted agent security manager |
| U.S. | United States |
| USACIDC | United States Army Criminal Investigation Command |
| USAREUR | United States Army Europe |
| USEUCOM | United States European Command |
| VOLAC | volunteer access control |

SECTION II

TERMS

base area network

A base, post, camp, or station local area network.

cyber condition

A uniform system of five progressive conditions within which commanders and DOD component heads will ensure network availability and protection of mission critical/essential systems and integrate approved response options to defend operational, business, and intelligence functions in cyberspace.

foreign national

An individual who is not a U.S. citizen, including U.S. military personnel, DOD civilian employees, and contractors.

information technology

The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This includes automatic data processing equipment, computers, and telecommunications; any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, distribute, process, store, or control data or information.

installation campus area network

The common transport network provided by the responsible network enterprise center on every Army post, camp, and station, and the associated common network services, including network management and information assurance services.

personally identifiable information (PII)

Any information about an individual, including but not limited to education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, or any other personal information that is linked or can be linked to an individual.

personally identifiable information (PII) electronic record

Any item, collection, or grouping of information in electronic form maintained by a DOD component that associates personal information such as education, financial transactions, medical history, criminal or employment history with an individual. This includes any item, collection, or grouping of information in electronic form that associates two or more individual identifiers (for example, name and social security number). Electronic records that include information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

personally identifiable information (PII) impact category

For DOD information assurance purposes, consistent with Federal Information Processing Standards Publication 199, electronic PII records are categorized according to the potential adverse effect caused by losing or disclosing the PII to unauthorized personnel. The two PII impact categories are as follows:

- **high impact.** PII concerning any Defense-wide organization (for example, unit or office) or program, or project-level compilation of electronic records that have PII on 500 or more individuals stored on a single device or accessible through a single application or service, regardless of whether or not the compilation is subject to the Privacy Act. This includes any compilation of electronic records with PII on less than 500 individuals identified by the information or data owner as requiring additional protection measures. Examples include a single mobile computing or storage device with PII on 500 or more individuals, even if the PII is distributed across multiple files or directories. A DOD enclave of 500 or more users with the PII for each user embedded in his or her individual workstation is not considered high impact PII.
- **moderate impact.** Any electronic records with PII not identified as high impact PII.

remote access

Enclave-level access for authorized users external to the enclave that is established through a controlled access point (for example, communications server, remote access server) at the enclave boundary.