

Army in Europe Bulletin

Number 9

IMCOM-Europe (IMEU-GD), Unit 23103, APO AE 09136-3103

September 2015

This bulletin expires 1 year from date of publication.

COMMUNICATIONS SECURITY

Personnel in the Army in Europe will not process, store, or send classified information on nonsecure data networks and telecommunications systems. DOD communications systems include computer networks, fax machines, modems, telephones, and radios. Use of official DOD data networks and telecommunications systems constitutes user consent to information systems security monitoring.

Commanders will ensure the following telecommunications security notification requirements are met:

➤ Official Army telephone or communications directories published in the Army in Europe will display the following security notice on the front cover or prominently in the general information section:

ATTENTION!

DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD DATA NETWORKS AND TELECOMMUNICATIONS SYSTEMS (INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS) ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD COMMUNICATIONS SYSTEMS CONSTITUTES CONSENT TO INFORMATION SYSTEMS MONITORING.

➤ DD Form 2056 (Telephone Monitoring Notification Decal) must be on telephones (excluding tactical telephones) and fax machines (excluding machines that are part of another device), including secure terminal equipment (STE). When DD Form 2056 is put on STE instruments and fax machines used to send and receive classified information, the statement "DO NOT DISCUSS CLASSIFIED INFORMATION" will be removed.

➤ A computer logon security notice is on all computer systems (AR 380-53).

➤ New personnel receive a briefing on the information above.

Representatives of the USAREUR G2 can provide more information about communications security (mil 537-2104).

MEASURES TO PROTECT SOCIAL SECURITY NUMBERS AND OTHER PERSONALLY IDENTIFIABLE INFORMATION (PII)

According to Department of Defense Instruction (DODI) 1000.30, Reduction of Social Security Number (SSN) Use Within DOD, all DOD personnel must reduce or eliminate the use of the SSN in any form (including the last four digits) and substitute the SSN with the DOD ID number or other unique identifier whenever possible. The continued collection of the SSN must meet one of the acceptable use criteria in DODI 1000.30 and be formally justified in writing. The SSN must never be listed in a personnel roster and not be posted on any publicly accessible website. If the use of the SSN meets one of the acceptable use criteria and the use is approved, the SSN must only be used in officially issued forms. Forms collecting PII must also have a Privacy Act Statement.

▶ When sending e-mail messages with PII, personnel will ensure the following:

➤ The message is digitally signed and encrypted.

➤ The message is not transmitted from a Government server to a private server, that is, from a .mil to a .com e-mail address.

➤ The subject line includes "FOUO."

➤ The body of the message includes the following warning: "FOR OFFICIAL USE ONLY."

➤ The message is addressed to the correct recipients and that all recipients have an official need to know.

➤ Messages are opened only when received from trusted sources to avoid phishing attacks.

The rules above also apply to e-mail that may not include PII in the body of the message, but in attachments.

▶ When printing material with PII, personnel will ensure the following:

➤ The printer location is verified before printing a document with PII.

➤ All printed documents with PII are properly marked “FOR OFFICIAL USE ONLY.”

➤ A “Privacy Act Cover Sheet” (DD Form 2923) is used.

➤ All documents are safeguarded when not in the user’s direct possession. This prevents access by those without an official need to know.

▶ The following publications provide more information:

➤ Department of the Army PII User’s Guide on Personally Identifiable Information (available at **Error! Hyperlink reference not valid.**)

➤ AE Poster 340-21, Desktop Information on the Privacy Act (available at <https://aepubs.army.mil/ae/public/main.aspx>).

Personnel with questions concerning the protection of PII may contact the USAREUR Privacy Act Officer (mil 337-3600, e-mail: usarmyeurope.foia@mail.mil).

FORWARDING SPAM

Forwarding spam (unsolicited “junk” e-mail distributed in bulk) using Government computers is a violation of DOD and U.S. Army policy (DOD 5500.7-R, Joint Ethics Regulation (JER)).

This policy is defined in the DOD Cyber Awareness Challenge Training that employees in the Army in Europe must complete together with the annual DOD Cyber Awareness Challenge Exam before obtaining a network user account. It is also in the Acceptable-Use Policy Agreement that employees must sign. Personnel who forward spam using Government computers may lose their e-mail and network access privileges.

Examples of spam include e-mail messages that—

➤ Use fake technical or emotional language.

➤ Offer “get-rich-quick” schemes.

➤ Include heartrending pleas for help.

➤ Tell the recipient to forward the message to protect others from a devastating virus. (These messages are often viruses themselves.)

Spam is also used to spread hoaxes and myths. Some of these messages are sent only to consume bandwidth and other resources or to damage the reputation of companies.

Computer users are strongly encouraged to report spam e-mail to their information assurance managers or information management officers.

Personnel who need refresher training on the appropriate use of e-mail should take the DOD Cyber Awareness Challenge Exam (available at <https://ia.signal.army.mil/DoDIAA/default.asp>).

ARMY IN EUROPE LIBRARY & PUBLISHING SYSTEM NEWS

The following have been published and are available in the Army in Europe Library & Publishing System:

Army in Europe Command Memorandums:

➤ [Delegation of Authority for Foreign Area Tour Extensions and Waivers of Physical Presence Requirement](#), AEPE-CB, (mil 537-1532), 21 July 2015

➤ [Family Housing Assignment Policy for the Army in Europe](#), AECG, (mil 544-4403), 28 July 2015

➤ [IMCOM-Europe Guidance on Participation of FMWR Employees and Volunteers in Tournaments](#), IMEU-MWR-B, (mil 544-9427), 5 August 2015

➤ [Announcement of the Army in Europe Barracks Inspection and Recognition Program](#), AECG, 3 August 2015

➤ [Army in Europe Barracks Inspection and Recognition Program](#), AELG-X, (mil 537-4003), 3 August 2015

➤ [Guidance on the Acquisition and Disposal of Real Estate](#), IMEU-GR, (mil 544-0542), 22 January 2015

➤ [Host-Nation Labor-Relations Synchronization Discussion Group \(Local National Employees in Germany\)](#), AEPE-C, (mil 537-1501), 17 August 2015

Army in Europe Publications:

➤ [AE Regulation 11-2](#), USAREUR Managers' Internal Control Program, 25 August 2015

➤ [AE Regulation 55-4](#), Safe Movement of Hazardous Goods by Surface Modes, 19 August 2015

➤ [AE Regulation 350-1](#), Training and Leader Development in Europe, 3 September 2015

➤ [AE Pamphlet 11-2](#), Guide to the USAREUR Managers' Internal Control Program, 25 August 2015

Army in Europe Forms:

➤ [AE Form 95-40C](#), Initial Notification of Downed Aircraft

➤ [AE Form 190-1T](#), Application for U.S. Forces POV Certificate of License and Allied Transactions

➤ [AE Form 190-6D](#), U.S. Forces Application for Registration of a Firearm

➤ [AE Form 190-6G](#), Weapons Bill of Sale / *Schusswaffenkaufvertrag*

➤ [AE Form 190-6J](#), Request for Cancellation of Privately Owned Firearm

➤ [AE Form 190-16C](#), Record of Destruction

➤ [AE Form 220-5C](#), USAREUR Movement Directive Worksheet

➤ [AE Form 381-2A](#), Forward Area Limited Observing Program

➤ [AE Form 420-1F](#), Army in Europe Barracks Inspection and Recognition Program (BIRP) Checklist

➤ [AE Form 420-1G](#), High-Value Personal Property Inventory Record

➤ [AE Form 550-50A](#), Status of Forces Incident Report

➤ [AE Form 690-99E](#), Request for Additional Leave Entitlements pursuant to the *Sozialgesetzbuch IX* (Social Security Code IX), Part 2 (Severely Handicapped Persons' Law)/*Antrag auf Zusatzurlaub gemäss Sozialgesetzbuch (SGB) IX Teil 2 (Schwerbehindertenrecht)*

➤ [AE Form 690-99F](#), Daily Record of Work Performed under Specially Severe Conditions

HOW TO USE THIS BULLETIN

IMCOM-Europe publishes the Army in Europe Bulletin during the 1st week of each month. Only members of HQ USAREUR staff offices, HQ IMCOM-Europe staff offices, and the United States Army Civilian Human Resources Agency, Northeast/Europe Region, may submit items for publication in the Army in Europe Bulletin.

Personnel assigned to USAREUR major subordinate and specialized commands may submit items for publication, provided the request is sent through the command's affiliated HQ USAREUR staff office.

Personnel assigned to United States Army garrisons may also submit items for publication, provided the request is sent through the IMCOM-Europe SGS.

Personnel with questions or comments about this bulletin may contact the editor by telephone (mil 544-1460/1450) or by e-mail: (*USARMY Sembach IMCOM Europe Mailbox PUBSMail*).

For the Director:

ROBERT L. MYERS
Chief of Staff

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management