

Army in Europe Bulletin

Numbers 3 & 4

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

Mar/Apr 2016

This bulletin expires 1 year from date of publication.

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>).

SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION

All employees have specific responsibilities for safeguarding personally identifiable information (PII). All military and civilian personnel and contractors have a fiduciary responsibility to ensure PII is maintained, used, and distributed only as authorized by law and that PII is continually safeguarded.

According to DOD Directive 5400.11, enclosure 3, the “Rules of Conduct” for safeguarding PII are as follows:

DOD personnel will—

- Take such actions, as considered appropriate, to ensure that any personal information contained in a system of records, of which they have access to and are using to conduct official business, shall be protected so that the security and confidentiality of the information shall be preserved.
- Not disclose any personal information contained in any system of records, except as authorized by reference (d) [DOD 5400.11-R], or other applicable laws or regulations. Personnel willfully making such disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties or administrative sanctions.
- Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this Directive [DOD Dir 5400.11] to the applicable Privacy POC for his or her DOD Component.

DOD System Managers for each system of records shall ensure that all personnel who either shall have access to the system of records or who shall develop

or supervise procedures for handling records in the system of records shall be aware of their responsibilities and are properly trained to safeguard personal information being collected and maintained under the DOD Privacy Program.

For more information, the USAREUR Privacy Act Officer may be contacted at military 337-3600.

ARMY IN EUROPE PUBLISHING NEWS

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

Army in Europe Command Memorandums:

- [Strong Europe 2016-2017](#), AECG, 2 March 2016
- [Delegation of Authority to Approve, Disapprove, or Downgrade Recommendations for Awards under Peacetime Criteria](#), AEPE-AGP (mil 537-1143), 15 March 2016

Army in Europe Publications:

- [AE Regulation 600-25](#), USAREUR Salute Battery, 16 February 2016
- [AE Regulation 608-2](#), Family Readiness, 15 March 2016
- [AE Regulation 672-10](#), Civilian Personnel Incentive Awards in IMCOM-Europe, 29 February 2016

Army in Europe Forms:

- [AE Form 1-3B](#), Request for Approval of Unauthorized ACSA Transaction
- [AE Form 55-50B](#), Accident/Incident Report on Occurrences During the Carriage of Dangerous Goods/Hazardous Waste
- [AE Form 350-22E](#), U.S. Forces Request for Maneuver

➤ [AE Form 600-25A](#), Request for USAREUR Salute Battery Support

➤ [AE Form 690-70A](#), *Bewerbung*/Application

HOW TO USE THIS BULLETIN

IMCOM-Europe publishes the Army in Europe Bulletin once a 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) 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