

Army in Europe Bulletin

Number 7

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

July 2016

This bulletin expires 1 year from date of publication.

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 e-mail address 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 all recipients have an official need to know.
 - Messages are opened only when received from trusted sources. This prevents 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 to Personally Identifiable Information (available at <https://www.rmda.belvoir.army.mil/privacy/docs/Army-PII-Users-guide.pdf>)
- AE Poster 340-21, Desktop Information on the Privacy Act (available at https://aepubs.army.mil/pdfpubs/AEPOS340-21_1007328.pdf)

Personnel with questions concerning the protection of PII may contact the USAREUR Privacy Act Officer (mil 537-6343, e-mail: usarmy.badenwur.usareur.mbx.freedom-of-information-act@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 PUBLISHING NEWS

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

Army in Europe Publications:

- [AE Supplement 1 to AR 600-8-7](#), Retirement Services Program, 8 June 2016
- [AE Regulation 600-2](#), The Sergeant Morales Club Membership and Dr. Mary E. Walker Award Programs, 30 June 2016
- [AE Pamphlet 10-10](#), Directory of Army in Europe Key Personnel, 24 June 2016
- IMCOM-Europe Retiree Bulletin, June 2016

Army in Europe Forms:

- [AE Form 190-1AC](#), Certificate of Nondelivery of Vehicle

➤ [AE Form 190-1AD](#), Special Power of Attorney to Operate, Sell, or Otherwise Dispose of a Privately Owned Vehicle (POV)

➤ [AE Form 190-1AF](#), Agent Responsibilities

➤ [AE Form 190-1H](#), Vehicle Mechanical Safety Inspection Record/*Inspektionsbericht über die Mechanische Sicherheit eines Fahrzeug*

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.mbx.pubsmail@mail.mil.

For the Director:

BEVERLY D. MCALISTER
Acting Chief of Staff

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management