



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY MANEUVER CENTER OF EXCELLENCE
1 KARKER STREET
FORT BENNING, GEORGIA 31905-5000

Policy Memorandum 25-54-4

IMSE-BEN-HRS (25)

23 AUG 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort Benning Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

1. REFERENCES:

- a. DoD Instruction 5400.16, Privacy Impact Assessment (PIA) Guidance, 12 Feb 09.
- b. Memorandum, Department of Defense, 18 Aug 06, subject: DoD Guidance on Protecting Personally Identifiable Information.
- c. Memorandum, Office of the Secretary of Defense, 21 Sep 07, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- d. Memorandum, Chief Information Officer (CIO)/G6, 31 Jul 09, subject: Updated Guidance for Submission of Privacy Impact Assessment(s) (PIA)
- e. ALARACT 05012009, February 2009, subject: ALARACT 050/2009 Personally Identifiable Information (PII) Incident Reporting and Notification Procedures

2. PURPOSE: This policy will define personally identifiable information (PII) and includes specific procedures on how to protect and report the loss of PII. This revision also eliminates the PII email footer which can now be accomplished by using the classification banner.

3. POLICY:

- a. All personnel working on Fort Benning have a direct responsibility to ensure privacy act and PII are collected, maintained, used and disseminated only as authorized. Personnel are further required to protect all PII data (hardcopy or electronic) from unauthorized use, access, disclosure, alteration or destruction. PII will not be released to anyone who does not have a duty-related official need to know.
- b. PII is defined as any information about an individual that is intimate or private to the individual, as distinguished from information related solely to the individual's official functions or public life. Information includes, but is not limited to, education, financial transactions, medical history, criminal or employment history, and other information

SUBJECT: Fort Benning Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

which can be used to distinguish or trace an individual's identify (such as, name, social security number, date and place of birth, mother's maiden name, biometric records, and so forth), including other personal information which is linked or linkable to an individual.

c. Personally Identifiable Information will be given the protections afforded "For Official Use Only" documents and protected in accordance with DoD Regulation 5200.1-R, Appendix 3, Jan 97.

d. The acceptable methods for disposal of paper records are tearing, burning, melting, chemical decomposing, pulping, pulverizing, shredding, or mutilating. For electronic records and media disposal methods, such as overwriting, degaussing, disintegrating, pulverizing, burning, melting, incinerating, shredding or sanding are acceptable.

e. All personnel using the Fort Benning computer system are responsible and directed to encrypt all email containing PII.

f. Notification of Personnel Affected by PII Loss: When PII is lost, stolen, or compromised, "Notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered, and the identities of the individuals are ascertained." A sample letter to affected individuals can be accessed at: <http://www.rmda.belvoir.army.mil/rmdaxml/rmdadocuments/FOIA%20Documents/SampleNotificationLetter.pdf>. All personnel must be knowledgeable of the procedures for reporting the loss of PII (enclosure 1). The format to report this information to the G-1 is at enclosure 2. A fine of up to \$5,000.00 can be imposed for failure to protect PII information.

g. Computer Hard Disk Drive (HDD) Responsibilities: All computer hard disk drives to include copiers, facsimile machines, peripherals, electronic typewriters, word processing systems, and others must be purged or cleaned before reuse in a different environment, with a different classification level of data, or with a different need-to-know authorization of users. It is the Activities responsibility to identify those features, parts or functions used to process information that may retain all or part of the information. This policy applies to all hard-drives used to handle U.S. Army information regardless of ownership, such as, Army owned or leased computers, warranty repair or replacement and contractor or vendor owned, operated, managed or provided. For approved methods for destruction or removal of information on Army Computer HDDs, contact the Network Enterprise Command (NEC) at Benn.doim.ia.team@conus.army.mil.

h. Privacy Impact Assessment (PIA). PIAs are developed, coordinated, approved, and published when Personally Identifiable Information (PII) about members of the public,

SUBJECT: Fort Benning Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

Federal personnel, contractors, or foreign nationals employed by U.S. military facilities internationally is collected, maintained, used, or disseminated in electronic form. Commanders and Directors will ensure a PIA is completed for information systems and electronic collections that collect, maintain, use, or disseminate PII about members of the public, Federal personnel, contractors, or foreign nationals.

i. Personnel with authorized access to PII will complete annual training. Training in the Privacy Act and Personally Identifiable Information can be accessed on the DHR SharePoint site at <https://benna0shrpt2/sites/ag/ASD/Forms/AllItems.aspx>. After completion of training, personnel with authorized access to PII shall annually sign a document clearly describing their responsibilities and acknowledging their understanding. The certification document shall be retained in the office to which the employee is assigned or, where contractor personnel are involved, the appropriate office of the DoD Component supported by the contract. The certification document will be subject to inspection during Command Records Management inspections. A copy of the certification is at enclosure 3. A roster containing the unit, names, and date of training will be signed by all individuals with access to PII. Rosters must be provided to the Records Management inspector during the Command Inspection Program (CIP) inspection. Directorates and organizations not subject to the CIP, must E-mail completed rosters to the Privacy Act Officer at Benn.DHR.FOIA.ProjectOfficer@conus.army.mil yearly upon completion of training.

4. SUPERSESSION: The policy memorandum superseded MCoE Policy Memo 25-54-3, 29 Sep 10, same subject.

5. Point of contact is the Fort Benning Freedom of Information/Privacy Act Office at Benn.DHR.FOIA.ProjectOfficer@conus.army.mil or 706-545-5356.

FOR THE COMMANDER:

3 Encls
as



ROBERT J. BATTERS, JR.
Colonel, Infantry
Chief of Staff

DISTRIBUTION:
ADMIN L, CSM/SGM, and MSC DCO/XO Lists

FORT BENNING PROCEDURES
FOR THE
NOTIFICATION OF PII BREACH OR COMPROMISE INCIDENT

1. All incidents must be reported immediately to the Unit Commander, Director, or Staff Activity Chief.

2. Commander, Director, or Staff Activity Chief will notify the appropriate Commander, such as, USAIC; USAG; USAIS; Director DIS; NEC (if electronic breach or compromise) and DHR ATTN: FOIA by E-mail at BENN.DHR.FOIA.ProjectOfficer@conus.army.mil.

3. Within one hour of detecting the breach or compromise, the Commander or Director will submit a report to <http://www.us-cert.gov>. A copy of the report will be E-mailed to: BENN.DHR.FOIA.ProjectOfficer@conus.army.mil. The reporting format can be found at: <https://www2.arims.army.mil/rmdaxml/rmda/privacyactprog-guidance.asp>. An email will also be sent to pii.reporting@us.army.mil with the notification that an initial report has been submitted. PII Incident Report will contain:

a. Organization involved:

b. Date of Incident and estimated number of individuals impacted:

c. Brief Description of Incident (either suspected or confirmed); circumstances of the breach; information lost or compromised:

d. Point of contact (name, telephone number, and email) of individual who discovered the breach or compromise:

Commander's Critical information Requirement
Format for PII Reporting

1. PERSONALLY IDENTIFIABLE INFORMATION:
2. TYPE OF INCIDENT:
3. DATE/TIMEGROUP OF THE INCIDENT:
4. LOCATION:
5. PERSONNEL INVOLVED:
6. SUMMARY OF INCIDENT:
7. REMARKS:
8. PUBLICITY:
9. OFFICIAL REPORTING:
10. POC:

Certification of Initial/Annual Refresher Training

This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information.

(Signature)

(Print Name)

(Date)

(DoD Component/Office)