



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

REPLY TO
ATTENTION OF

AUG 7 2012

IMPM-ZA

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum #14, Safeguarding and Reporting Personally Identifiable Information (PII)

1. References:

- a. Department of Defense Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, 12 February 2009.
- b. Memorandum for Secretaries of the Military Departments, subject: Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII), 18 August 2006.
- c. Memorandum for Secretaries of the Military Departments, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 21 September 2012.
- d. ALARACT 262121Z Feb 09, subject: ALARACT 050/2009 Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.
- e. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- f. DoD 5400.11-R, Department of Defense Privacy Program, 14 May 2007.
- g. Department of Defense Manual 5200.01, Volume 4, subject: DoD Information Security Program: Controlled Unclassified Information (CUI), 24 February 2012.

2. Purpose: This policy will define personally PII and includes specific procedures on how to protect and report the loss of PII.

3. Policy:

- a. All personnel working on the Presidio of Monterey and Ord Military Community 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.

IMPM-ZA

SUBJECT: Command Policy Memorandum #14, Safeguarding and Reporting Personally Identifiable Information (PII)

b. Per DoD 5400.11-R, DL1.14. PII is defined as information about an individual that identifies, links, relates, is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; and other demographic, biometric, personnel, medical, and financial information, etc. Such information also is known as PII (e.g., information which 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; and biometric records, including any other personal information which is linked or linkable to a specified individual).

c. PII will be given the protections afforded "For Official Use Only" (FOUO) documents and protected and marked in accordance with DoDM 5200.01 Volume 4, 24 February 2012.

d. FOUO documents shall be destroyed by cross-cut shredding with chaff no larger than DIN 32757, Security Level 3: 3/16 inch by 3 inches. Tearing is not permitted. The following shredder models are recommended for use: Fellowes Powershred 99Ci, Whitaker Brothers Destroyit 2604 Cross Cut, or HSM Shredstar BS15C. These models are not authorized for shredding classified information. For electronic records and media disposal methods contact Network Enterprise Center (NEC) Helpdesk at (831) 242-5028 or via e-mail: usarmy.pom.106-sig-bde.list-pres-helpdeskstaff@mail.mil.

e. All personnel using the Presidio of Monterey computer system are responsible and directed to encrypt all e-mail 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: <https://www.rmda.army.mil/privacy/docs/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 Directorate of Human Resources (DHR) 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 other 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 lease computers, warranty repair or replacement, and contractor or vendor owned, operated, managed, or provided. For approved methods of destruction or removal of information on Army computer

IMPM-ZA

SUBJECT: Command Policy Memorandum #14, Safeguarding and Reporting Personally Identifiable Information (PII)

HHDs, see BBP 03-PE-0-002, Reuse of Army Computer Hard Drives, the POM NEC, or contact Property Book Office (PBO) for guidance.

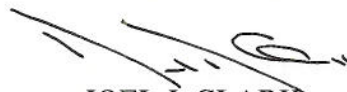
h. Privacy Impact Assessment (PIA). PIAs are developed, coordinated, approved, and published when PII about members of the public, Federal personnel, contractors, or foreign nationals employed by U.S. Military facilities internationally is collected, maintained, used, or disseminated in electronic form. 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 can be accessed at: http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html. 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.

j. Installation Management Command Personally Identifiable Information Reporting Checklist is available at the following link:
http://www.monterey.army.mil/Human_Resources/inc/PII_REPORTING_Chklst_Mar2012.pdf

4. Point of contact is the Presidio of Monterey Freedom of Information Act (FOIA)/Privacy Act (PA) Office at usarmy.pom.106-sig-bde.mail.pres-asb@mail.mil or (831) 242-6319.

3 Encls
as



JOEL J. CLARK
COL, SF
Commanding

DISTRIBUTION:
F

CF:
DLIFLC Commandant
Tenant Unit Commanders

PRESIDIO OF MONTEREY PROCEDURES
FOR THE NOTIFICATION OF PERSONALLY IDENTIFIABLE INFORMATION (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, United States Army Intelligence Center (USAIC); United States Army Garrison (USAG); United States Army Information System (USAIS); Director G-2; Network Enterprise Center (NEC) (if electronic breach or compromise) and Directorate of Human Resources (DHR) ATTN: FOIA by e-mail at usarmy.pom.106-sig-bde.mail.pres-asb@mail.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: usarmy.pom.106-sig-bde.mail.pres-asb@mail.mil and usarmy.pom.106th-sig-bde.mbx.pom-nec-information-assurance@mail.mil. The reporting format can be found at https://www.rmda.army.mil/privacy/docs/DPCL0_Breach_Report_Template.pdf. An e-mail 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 e-mail) of individual who discovered the breach or compromise:

Commander's Critical Information Requirement
Format for Personally Identifiable Information (PII) Reporting

1. PERSONALLY IDENTIFIABLE INFORMATION:
2. TYPE OF INCIDENT:
3. DATE/TIME GROUP 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 (PII) 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 PII, 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)