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

OCT 1 9 2018

IMPM-HR

MEMORANDUM FOR SEE DISTRIBUTION

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

1. References:

a. Office of the Secretary of Defense Memorandum, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), 21 Sep 07.

b. DoD Directive 5400.11, DoD Privacy Program, 29 Oct 14

c. DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, 14 Jul 15.

d. DoD Chief Information Officer Memorandum, subject: DoD Guidance on PII, 18 Aug 06.

2. Purpose: This policy will define PII and includes specific procedures on how to protect and report the loss of PII. This Command Policy supersedes Command Policy Memorandum # 14, Safeguarding and Reporting Personally Identifiable Information (PII) dated 7 August 2012.

3. Proponent: POM Freedom of Information Act (FOIA)/Privacy Act (PA) Office at usarmy.pom.106-sig-bde.mail.pres-asb@mail.mil or (831) 242-6215.

4. Policy:

a. All DoD employees, contractors, and other personnel who are assigned to or otherwise work 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. All personnel have an affirmative responsibility to protect an individual's privacy when maintaining his or her 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. All personnel must be knowledgeable of the procedures for the reporting of PII breach or compromise incident (Enclosure 1). Failure to safeguard PII can result in disciplinary actions. As a Government employee you can personally suffer criminal or civil charges and penalties for failure to protect PII. Failure to safeguard PII can also erode confidence in the government's ability to protect information, impact business practices, lead to major legal action, and lead to identity theft which can be costly to both the individual and the government.

d. 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. Use Privacy Act Data Cover Sheet, DD Form 2923, Sep 10, (Enclosure 2) for documents that may contain personal or privileged information. Filing cabinets or authorized storage equipment where records that contain personal or privileged information should have DD Form 2923 displayed on the outside of the container. DD Form 2923 can also be downloaded from the DoD Forms Management Program website at http://www.dtic.mil/whs/directives/forms/eforms/dd2923.pdf.

e. 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) Cybersecurity Division and Installation System Security Manager at (831) 242-7181 or usarmy.pom.106-sig-bde.mbx.pom.nec-information-assurance@mail.mil.

f. All personnel using the Presidio of Monterey computer system are responsible and directed to digitally sign and encrypt all email containing PII.

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 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 and submitted for information and electronic systems that collect, maintain, use, or disseminate PII about members of the public, Federal personnel, contractors, or foreign nationals. More information regarding PIA is available at the Records Management and Declassification Agency (RMDA) website at https://www.rmda.army.mil/privacy/RMDA-PO-PIA.html.

i. All applicable personnel will complete PII training IAW the applicable policies and regulations. Those personnel, determined by Directors and Staff Agency Heads, with authorized access to PII will complete PII training annually. Training can be accessed at the U.S. Army Information Assurance Virtual Training website: https://iatraining.us.army.mil. The PII training Certificate of Completion 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.

5. At Enclosure 1 is a link to the Department of Army Personally Identifiable Information User's Guide for dissemination to all employees.

3 Encls
as

GREGORY J. FORD
COL, MI
Commanding

DISTRIBUTION:
G

PRESIDIO OF MONTEREY PROCEDURES
FOR THE REPORTING 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. Continue to follow existing Internal Command Procedures to notify local command officials. For the U.S. Army Garrison, Presidio of Monterey, prepare the report IAW with the Serious Incident Reports (IMCOM Regulation 190-1). For the Defense Language Institute Foreign Language Center, follow procedures IAW the Training and Doctrine Command's Leader's Guide to Protecting PII flyer attached. Contact the United States Computer Emergency Response Team (US-CERT) for network intrusion incidents.

3. Report all cyber-related incidents involving the actual or suspected breach/compromise of PII within one hour of discovery to the United States Computer Emergency Readiness Team (US-CERT) by completing and submitting the US-CERT report at https://www.us-cert.gov/forms/report. A copy of the report will be e-mailed to:

   a. usarmy.pom.106-sig-bde.mail.pres-asb@mail.mil, and

   b. usarmy.pom.106th-sig-bde.mbx.pom-nec-information-assurance@mail.mil.

4. The individual discovering the breach or compromise, in coordination with the organization that created the data, if known, must report both electronic and physical related incidents to the Army Privacy Office within 24 hours of discovery by completing the Breach of PII report via the Privacy Act Tracking System (PATS) at https://www.privacy.army.mil/PATS/.

5. More information regarding PII is available at the RMDA website at https://www.rmda.army.mil/privacy/PII/PII.html.

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)