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

AMIM-PMG-ZA (1oo) 21 August 2024

MEMORANDUM FOR Presidio of Monterey Installation

SUBJECT: United States Army Garrison (USAG) Presidio of Monterey (PoM), Command Policy #15 – Privacy Act Policy

1. Reference: AR 25-22 (The Army Privacy and Civil Liberties Program)

2. I am committed to protecting the privacy and civil liberties of Soldiers, DA Civilians, and individuals considered members of the public to the greatest extent possible, consistent with our mission and operational requirements regarding the collection, use and sharing of personal information.

3. The Privacy Act promotes and safeguards personal information maintained by a System of Record (SOR). This policy reinforces the way USAG PoM collects, stores, uses, and discloses personal information for compliance with operational requirements of this command and as established by the Privacy Act of 1974 (5 U.S.C. § 552a) and AR 25-22.

4. The policy and procedures outlined below are applicable to all US Army military, civilian and contractor personnel assigned to or under the operational control of USAG PoM.

5. Policy: USAG PoM employees will only collect personal information that is legally authorized and minimally necessary to support operations.

a. Disclosure of records pertaining to an individual from a SOR is strictly prohibited in the absence of the individual's written consent except as authorized by the Privacy Act of 1974 and the Freedom of Information Act.

b. Employees will ensure the security and confidentiality of personal records, protect records in their possession against possible threats or hazards and permit access to these records to only those authorized persons with a verified need-to-know.

6. Procedures: IMCOM employees will only transmit and secure records containing PII using one of the methods shown below

a. Paper records containing PII will be placed in secured areas (locked file cabinets or locked room) when not being used by an employee to conduct government business.

b. When sending emails that contain social security numbers or other PII, ensure that the email is encrypted. Also, confirm that the recipient's email address is correct. Most importantly, use "Reply All" with extreme caution, if at all.

c. Electronic records being transmitted (via email) to non-DOD personnel (without a .mil account) with a verified need to know, will be sent encrypted using Department of Defense Secure Access File Exchange (DOD-SAFE) at: https://safe.apps.mil or other electronic means that require a passphrase to access. This will also be the method to transmit records containing PII when a .mil recipient cannot receive encrypted emails, i.e., group/generic boxes.

d. Transmitting records containing PII by hand to other offices inside or outside USAG PoM will require the use of a Standard Form (SF) 901 Controlled Unclassified Information (CUI) cover sheet(s).

7. Individuals who perceive an alleged violation or want to file a Privacy Act complaint, will contact their appointed Privacy Act Officer prior to entering the suspected breach into the Defense Privacy Information Management System (DPIMS) Home (https://dpims.disa.mil/eCasePortal/Home.aspx). In the event your privacy official is unavailable, contact the HQ IMCOM Privacy office at (210) 466-0414 or email at usarmy.jbs.imcom-hq.mbx.privacy-management@army.mil

8. Proponent. USAG PoM Administrative Services Division, Directorate of Human Resources at (831)242-6215 or via email at: usarmy.pom.usag.mbx.asb@army.mil.

Date:
2024.08.21
13:44:31 -07'00'

Encl
PII Brochure

DANIEL S. ARTINO
COL, AV
Commanding

BREACH REPORTING

- Army activities will no longer report technology related Personally Identifiable Information (PII) breaches to U.S. Computer Emergency Readiness Team (US_CERT). Instead, Army activities are to first report suspected or confirmed breaches in army medium or form, including paper, oral, and electronic by entering data into the Department of Defense Privacy Information Management System (DPIMS) within 24 hours of breach discovery. DPIMS populates DD Form 2959 Breach of Personally Identifiable Information (PII)Report).

DoD manual 5400.11 Vol. 2

INDIVIDUAL NOTIFICATION

Low/Moderate/High Risk or Harm notification is necessary, helpful, or otherwise required, the Senior Component Official for Privacy (SCOP), or other more senior-level individuals within the DoD Component, should notify potentially affected individuals. When a breach involves a well-known DoD Component or well-known system, the Component head should issue the notification.

Notify individuals potentially affected by a breach as expeditiously as practicable and without unreasonable delay. Balance the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm to potentially affected individuals. DoD Manual 5400.11, Volume 2

U.S. Army Presidio of Monterey
393 Patton Avenue
BLDG 272

Phone: 831-242-6215/6319
DSN:768-6979
FAX: 831-242-6979

REPORTING REQUIREMENTS AT—A—GLANCE

Department of Defense Privacy Information Management System (DPIMS)

https://dpims.disa.mil/eCasePortal/Home.aspx

Presidio Of Monterey Privacy email:

usarmy.pom.usag.mbx.asb@army.mil

Army FOIA/PA Office within 24 hours at

https://dpims.disa.mil/eCasePortal/Home.aspx

Determine nature of breach and type by assessing Low/Moderate/High Risk or Harm

Additional Information for PII/Breach

https://armyeitaas.sharepoint-mil.us/sites/HQDA-CIO-ISES-RMP

NOTE: A breach results when there is an actual or possible loss of control, unauthorized disclosure, or unauthorized access to information contained in a system of record possible loss of control, unauthorized disclo- sure, or unauthorized access to infor-

REPORTING
PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACHES

REPORTING REQUIREMENTS https://dpims.disa.mil/eCasePortal/Home.aspx

Within-24-Hours

The individual discovering the breach/ compromise, in coordination with the Command/Agency that created the data is known, must report all incidents involving the actual or suspected breach/compromise of PII to the Department of Defense Privacy Information management System (DPIMS).

The reporting format and submission guidelines are located at Defense Privacy Information Management System. Submit updated reports, reflecting the results of investigative.

Additional Information

DoD Manual 5400.11, Volume 2 (DoD Privacy and Civil Liberties Program: Preparedness and Response Plan.

AR 25-22- The Army Privacy and Civil Liberties Program

Privacy Act of 1974 (5 U.S.C. § 552a)

Following Internal Command

Continue to follow existing Internal Command Procedures to notify local command officials. This includes but is not limited to Serious Incident Reports (IMCOM Regulation 190-1). Document all breaches and actions taken in response to a breach using the Department of defense (DD) Form 2959, "Breach of Personally Identifiable Information (PII) Report". Contact FOIA/ PA Office for further guidance on PII breaches. Additional resources on PII/ Breach can be found at DoD 5400.11 Vol 2.

DETERMINING THE NATURE OF THE BREACH AND TYPE OF PII INVOLVED

FACTORS	Risk	Comments
a. The name of one or more individuals was released (a separate notification must be made for each individual affected.)	Low	
b. An individual's name and one or more identifiers were released ("Identifiers" are any information that relates to or is unique to and individual's identity	Moderate	
c. A name together with the named person's social security number, together with medical or financial information.	High	
d. A password was compromised. (Assess the likelihood of the pass word being accessible and useable.	Low, Moderate or high as applicable	
e. Assess the likelihood of the breach leading to harming the individual affected	Moderate or High as applicable	
f. Determine if the data was compromised with or without malicious intent.	Low if without malicious intent/	
g. Determine if the breach was caused by a loss of the information (loss of wallet, purse)		
h. Determine if the breach was caused by theft (for example, stolen wallet, purse, or laptop).		