



DEPARTMENT OF THE ARMY
HEADQUARTERS, JOINT READINESS TRAINING CENTER AND FORT POLK
6661 WARRIOR TRAIL, BUILDING 350
FORT POLK, LOUISIANA 71459-5339

AFZX-IM

MAY 04 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

1. References.

- a. Army Regulation 340-21, The Army Privacy Program, 5 Jul 85.
- b. Memorandum, Department of Defense, Chief Information Officer, 18 Aug 06, subject: Department of Defense Guidance on Protecting Personally Identifiable Information (PII).
- c. DoD 5400.11-R, Department of Defense Privacy Program, 14 May 07.
- d. Message, ALARACT 50/2009, 26 Feb 09, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures.
- e. Memorandum, Office of the Secretary of Defense, 5 Jun 09, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

2. Purpose. This standing operating procedure (SOP) will define PII and include specific procedures on how to protect and report the loss of PII.

3. Applicability. All Fort Polk units assigned or attached and Installation activities.

4. Definition. 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 which can be used to distinguish or trace an individual's identity (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.

5. Policy. All personnel working on the Joint Readiness Training Center (JRTC) and Fort Polk have a direct responsibility to ensure Privacy Act information and PII are collected, maintained, used and disseminated only as authorized. Personnel are further

AFZX-IM

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

required to protect all PII data (hardcopy or electronic) from unauthorized use, access, disclosure, alteration or destruction. The PII will not be released to anyone who does not have an official need to know. Individuals who violate their responsibilities may be subject to adverse administrative, disciplinary, or other actions.

a. Assess. All records identified by data owners as containing PII will be assigned the appropriate impact category of high (500 + PII records) or moderate (any electronic record containing PII that is not identified as high impact). In addition, any high impact electronic PII record stored on a mobile computing device or portable media that is removed from the government (protected) workplace will be required to log and track these devices in accordance with (IAW) the established SOP using the form at enclosure 1.

b. Train. All users will complete the Department of Defense Cyber Awareness Challenge Training prior to accessing the Fort Polk NIPRNet.

c. Secure.

(1). The JRTC and Fort Polk approved data-at-rest (DAR) solution is the encrypting file system (EFS) folder. Other active measures in protecting PII are access control through common access card/public key infrastructure (CAC/PKI) and automatic screen lock-out enforcement. In addition, all personnel using JRTC and Fort Polk computer systems are responsible and directed to encrypt all email containing PII.

(2). The acceptable methods for disposal of paper records are tearing, burning, melting, chemical decomposing, pulping, pulverizing, shredding, or mutilating. Acceptable disposal methods for electronic records and media are overwriting, degaussing, disintegrating, pulverizing, burning, melting, incinerating, shredding or sanding. A risk assessment on all PII records will be evaluated for impact of loss or unauthorized disclosure and protected accordingly using the factors within enclosure 2.

d. Report. All breaches will be reported IAW the JRTC and Fort Polk Incident Response Plan, see enclosure 3:

- Within one (1) hour: incident reported to US-CERT (<http://www.us-cert.gov/>), S1/G1, S2/G2, S6/G6, Network Enterprise Center Information Assurance Manager, and the Installation Operations Center.

- Within 24 hours: incident reported to the JRTC and Fort Polk Freedom of Information Act/Privacy Act office at 531-1612.

AFZX-IM

SUBJECT: Command Policy Memorandum G6-02 – Command Policy for Safeguarding and Reporting Personally Identifiable Information (PII)

- Within 48 hours: incident reported to Army leadership at pii.reporting@us.army.mil.

e. 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/organization/pa-guidance.shtml> and is also at enclosure 4. All personnel must be knowledgeable of the procedures for reporting the loss of PII. The format to report this information is contained within enclosure 3.

f. Reimburse. A fine of up to \$5,000.00 can be imposed for failure to protect PII.

6. This policy supersedes and rescinds all previous policies and SOPs on this subject matter.

7. The point of contact for this SOP is the ACofS G6 at commercial (337) 531-5995 or DSN 863-5995.

4 Encls

1. High Impact PII Log Form
2. Risk Assessment Model
3. DD Form 2959 (PII Breach Report)
4. Sample Letters



GARY M. BRITO
Brigadier General, USA
Commanding

DISTRIBUTION:

A+