



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT DRUM
10000 10TH MOUNTAIN DIVISION DRIVE
FORT DRUM, NEW YORK 13602-5000

JUL 15 2009

IMNE-DRM-GC

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Garrison Policy Memorandum # 09-15, Personally Identifiable Information (PII)

1. References:

- a. AR 340-21, The Army Privacy Program, 5 July 1985.
- b. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- c. Memorandum, DoD CIO, 28 October 2005, subject: Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance.
- d. Memorandum, DoD CIO, 18 August 2006, subject: Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII).
- e. Department of Defense 5400.11-R, Department of Defense Privacy Program, 14 May 2007.
- f. Memorandum, OMB, M07-16, 22 May 2007, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- g. VCSA ALARACT 174/2007, 110029ZJUN 07, subject: Safeguarding and Reporting Procedures for Personally Identifiable Information.
- h. AR 25-2, Information Assurance, 3 August 2007.

2. Purpose. This policy explains PII and includes specific procedures on how to protect and report the loss of PII.

3. Applicability. This policy applies to all organizations/units/activities and their personnel (Soldiers, civilians, and contractors) who receive computer service from the Fort Drum Directorate of Information Management or are employed by and/or conduct business on Fort Drum.

4. Policy:

- a. All personnel are required to protect all PII (in physical or electronic form) from unauthorized use, access, disclosure, alteration, or destruction.
- b. Personally identifiable information is defined as any information about an individual that is intimate or private to the individual, as distinguished from information related solely to the

IMNE-DRM-GC

SUBJECT: Garrison Policy Memorandum # 09-15, Personally Identifiable Information (PII)

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 (i.e., name, social security number, date and place of birth, mother's maiden name, biometric records, etc.) including other personal information which is linked or linkable to an individual. Personally identifiable information may be found in hard copy document form and/or stored electronically on computer/laptop hard drives and various media storage devices (i.e., diskettes, DVDs, CDs, thumb drives, flash media cards, paper files, etc.).

c. A breach or loss is defined as the actual or possible loss of control, unauthorized disclosure, or unauthorized access to PII.

d. All personnel must be knowledgeable of the procedures for protecting PII (Encl 1) and reporting the breach or loss of PII (Encl 2).

e. All personnel should limit the amount of PII collected and stored on workstations and mobile communication devices such as a laptop computer, BlackBerry, or cell phone, and Removable Storage Media such as thumb drives, DVDs, CD-ROMs, SD/flash memory cards, etc.

f. An incident is when PII is suspected or confirmed to be lost, stolen, or otherwise available to individuals without a duty-related official need to know. This may include posting PII on public-facing websites, sending PII via e-mail to unauthorized recipients, providing hard copies of PII to individuals without a need to know, and losing electronic devices storing PII.

g. Media containing PII will be destroyed IAW reference 1b above (sensitive).

h. Failure to protect PII may result in punitive action.

5. Point of contact is the Chief, Administrative Services Division, at 772-5288 and the Installation Information Assurance Manager at 772-2246.

2 Encls

1. Procedures for Protection of PII
2. Procedures for Reporting PII


KENNETH H. RIDDLE
Colonel, Armor
Garrison Commander

DISTRIBUTION:

A

**FORT DRUM PROCEDURES
FOR THE
PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)**

1. All users of Mobile Communication Devices (MCDs) (i.e., laptops/notebooks, BlackBerry phones, etc.) and Removable Storage Media (RSM) (i.e., USB drives, CD-ROMS, diskettes, etc.) that contain PII will ensure PII is stored in an encrypted folder. If an encrypted folder cannot be created on the device or media, the PII will not be transported. Users will contact their Information Management Officer/Information Assurance Security Officer if they have questions on how to create or use an encrypted folder.
2. All users of MCDs and RSM will ensure their devices have an encrypted folder for PII data and are properly labeled to indicate they are properly protected and authorized for travel. Forms are available from the Fort Drum Directorate of Information Help Desk (772-6610).
3. All users will encrypt e-mail when PII is included. Personal and private information (for example, individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974 (see reference 1a).

**FORT DRUM PROCEDURES
FOR
REPORTING THE BREACH/LOSS OF
PERSONALLY IDENTIFIABLE INFORMATION (PII)**

1. Individuals who are aware of an incident must **immediately** notify their Director/Commander. Regardless of the situation, the initial notification must take place within **one hour** of initial discovery of a possible breach or loss of PII.

2. The Director/Commander will:

a. Immediately notify the Fort Drum Mountain Operations Center (MOC) at 315-772-6324.

b. Notify the US-CERT at <http://www.us-cert.gov> **within one hour** of discovering the incident. **Note: Internal command notification may not delay the one-hour US-CERT notification.**

c. Immediately send an e-mail to piireporting@us.army.mil including information obtained on FD Form 599-E (Attachment A to Encl 2) and provide a copy of the e-mail to drum.foia-pa@conus.army.mil.

d. Complete a serious incident report (see AR 190-45 for appropriate format).

e. Coordinate with the local Staff Judge Advocate for sending affected individuals a notification letter within 10 days. Notification should occur from a sufficient management level (Garrison Commander or Chief of Staff) to reassure impacted individuals of the seriousness of the event.

f. Continue to update the US-CERT via e-mail and the piireporting@us.army.mil until the investigation is closed and all individuals have been notified.

3. The MOC will notify the Chief, Information Assurance Division (IAD) and the Chief, Administrative Services Division (ASD), during normal duty hours and/or after duty hours using after duty hours cell phone numbers who, in turn, will notify the Installation Information Assurance Manager at 772-2246.

4. The Chief, ASD and/or the Chief, IAD will report the incident to:

a. The Fort Drum Freedom of Information Act (FOIA)/Privacy Act (PA) officer 315-772-1500.

b. CONUS-TNOSC (conus.tnosc@us.army.mil), RCERT-CONUS at rcert.conus@us.army.mil.

5. The FOIA officer will complete the FOIA/PA formatted report and forward it to the HQDA FOIA/PA office within 24 hours of receiving notification.

Encl 2 to Garrison Policy Memorandum 09-15, 15 Jul 09, subject: Personally Identifiable Information (PII)

LOSS OR SUSPECTED LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

For use of this form, see AR 25-2. The proponent is the Directorate of Human Resources/Administrative Services Division.

1. DATE OF INCIDENT:

2. NUMBER OF INDIVIDUALS AFFECTED:

DA Civilians (DACs)

Contractors

Military

Civilians (other than DAC)

Retirees

Family Members

3. WHAT TYPE OF PII DATA WAS DISCLOSED (I.E., NAMES, ADDRESSES, PHONE NUMBERS, SOCIAL SECURITY NUMBERS, ETC.)?

4. WHAT WAS THE SCOPE OF THE DISCLOSURE (I.E., INTERNAL, EXTERNAL, HOW MANY UNAUTHORIZED INDIVIDUALS HAD ACCESS, ETC.)?

5. PROVIDE A DETAILED DESCRIPTION OF HOW THE PII WAS DISCLOSED (I.E., UNAUTHORIZED ACCESS, THEFT, DATA SPILLAGE, ETC.). INCLUDE FACTS AND CIRCUMSTANCES SURROUNDING THE LOSS, THEFT, OR COMPROMISE.

6. DESCRIBE WHAT ACTIONS HAVE BEEN TAKEN SO FAR IN RESPONSE TO THE INCIDENT. INCLUDE WHETHER THE INCIDENT WAS INVESTIGATED AND BY WHOM, PRELIMINARY RESULTS OF THE INQUIRY IF KNOWN, ACTIONS TAKEN TO MITIGATE ANY HARM THAT COULD RESULT FROM THE LOSS, NAMES OF INDIVIDUALS WHO MAY BE AFFECTED, AND WHETHER THE IMPACTED INDIVIDUALS ARE BEING NOTIFIED.

7. WHAT REMEDIAL ACTIONS HAVE BEEN OR WILL BE TAKEN TO PREVENT A SIMILAR INCIDENT IN THE FUTURE?

8. PROVIDE A SUMMARY OF THE MITIGATION STEPS TAKEN AND/OR STRATEGY TO CONTAIN THE INCIDENT; IMPACTED SYSTEMS (FILE SERVER, PRINT, MAIL SERVER, WEB SERVER, ETC.) TAKEN OFFLINE; SANITIZED; CACHED DATA DELETED; ONSITE/OFFSITE BACKUPS, ETC. DO NOT DISCLOSE THE ACTUAL PII INFORMATION (NAMES, SOCIAL SECURITY NUMBERS, ETC.) TO US-CERT.

NAME AND TITLE:

SIGNATURE:

DATE SIGNED: