



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
UNITED STATES ARMY FORCE MANAGEMENT SCHOOL
5500 21ST STREET, BUILDING 247, SUITE 1400
FORT BELVOIR, VIRGINIA 22060-5923

SEP 28 2015

DAMO-FMS

MEMORANDUM FOR Staff and Faculty of the Army Force Management School
(AFMS)

SUBJECT: AFMS Policy Letter #7 – Army Force Management School Personally
Identifiable Information (PII) Procedures

1. References:

- a. ALARACT 134/2008, subject: Army Encryption of Data at Rest Protection Strategy.
- b. ALARACT 050/2009, subject: PII Incident Reporting and Notification Procedures.
- c. Department of Defense (DoD) 5400.1 I-R, 14 May 2001, DoD Privacy Program.
- d. DoD Instruction 8500.2, 6 February 2003, subject: Information Awareness (IA) Implementation.
- e. Memorandum, DoD Chief Information Officer, 18 August 2006, subject: DoD Guidance on Protecting PII.
- f. Memorandum, OMB, M07 – 16, 22 May 2007, subject: Safeguarding Against and Responding to the Breach of PII.
- g. DoD Memorandum, 21 September 2007, subject: Safeguarding Against and Responding to the Breach of PII.
- h. Memorandum, USA, 10 May 2013, subject: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incidents.

2. Protecting PII is a critical intellectual property of the DCS, G-3/5/7. Inadvertent release or loss can have detrimental consequences.

DAMO-FMS

SUBJECT: AFMS Policy Letter #7 – Army Force Management School Personally Identifiable Information (PII) Procedures

3. Background.

a. PII is any information about an individual 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, and biometric records. This information can be in hardcopy (paper copy files) or electronic format, stored on personal computers, laptops, and personal electronic devices such as blackberries, and found within databases, this includes but is not limited to, education records, financial transactions, medical files, criminal records, or employment history.

b. A PII incident occurs when it is suspected or confirmed that PII is lost, stolen, or otherwise made available to individuals without a duty related, official need-to-know. Examples include sending PII via e-mail to unauthorized recipients, providing hard copies of PII to individuals without a need-to-know, losing electronic devices storing PII, posting PII on public websites, and unauthorized internal/external access to PII stored in databases.

4. Purpose. This directive outlines the necessary procedures for the proper identification, transmission, and storage of PII. It also defines the reporting process upon discovery of a PII incident within the DCS, G-3/5/7.

5. Scope. This directive applies to all AFMS personnel, contractors, business partners, developers, and system owners with access to PII. The safeguards within this directive apply to AFMS owned or controlled information systems that receive, process, store, display, transmit information, regardless of mission assurance category, classification or sensitivity.

6. Safeguarding PII. All AFMS personnel have a responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating personal information about an individual, regardless of format (electronic or hardcopy).

a. Electronic PII. System proponents and device users must implement and follow procedures to safeguard and reduce the risk of all PII incidents. This includes, but is not limited to the following:

(1) Encrypt and digitally sign all outgoing e-mail containing PII. Such e-mail must also be labeled FOUO.

(2) Each user and administrator is granted access only to PII information for which they have valid need-to-know.

DAMO-FMS

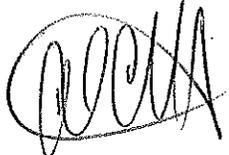
SUBJECT: AFMS Policy Letter #7 – Army Force Management School Personally Identifiable Information (PII) Directive

(3) Remote access requires two-factor authentication, i.e., Common Access Card and Personal Identification Number.

(4) Limit the amount of PII collected and stored on workstations, mobile computing devices and removable storage media (i.e., laptops, Universal Serial Bus (USB) drives, Blackberry devices, DVD/CD-ROMs, etc.).

(5) In accordance with reference 1(a), encrypt data on mobile devices before transporting outside protected workplace. This includes data contained on Blackberry devices, smart phones, hard drives and other storage media, such as USB drives, DVD/CD-ROMs. etc. If an encrypted volume cannot be created on a device containing PII, the device shall not be transported.

b. Hardcopy PII. To reduce the risk of mishandling PII, personnel must safeguard all hardcopy.

A handwritten signature in black ink, appearing to read 'A. Notgrass', enclosed within a hand-drawn oval.

ALAN C. NOTGRASS
Colonel, U.S. Army
Commandant