NGB ARNG G-6 March 12, 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Personally Identifiable Information (PII).

1. Reference:

   a. Office of Management and Budget Memorandum M-07-16, 05 JUN 09, Subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).

   b. Office of Management and Budget Memorandum M-06-19, 12 JUL 06, Subject: Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investments.

   c. DoD Directive 5400.11, “DoD Privacy Program,” 8 May 07.

   d. DoD Regulation, 5400.11-R, “DoD Privacy Program,” 14 May 07

   e. Memorandum, Office of the Secretary of Defense, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, DTD 21 SEP 07

   f. AR 25-2, Chapter 4, Section VIII (page 43, para 4-21), Incident and Intrusion Reporting, DTD 24 OCT 07.

   g. ALARACT 050/2009, Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, DTD 26 FEB 09

   h. ALARACT 147-2007, Army Protection of Personally Identifiable Information (PII) Awareness, DTD 2 JUL 07

   i. AR 25-55, 1 November 1997, Department of Army Freedom of Information Act Program

   j. AR 380-5, Department of the Army Information Security Program, 29 Sep 00

   k. Army “Road Warrior” Laptop Security Version 1.3, Issuance date, 17 FEB 2006 UPDATE: 18 MAR 09

2. Background: Each individual within the Army National Guard (ARNG) has the responsibility for ensuring Personally Identifiable Information (PII) is protected. In addition to government proprietary information, often large quantities of Personnel Identifiable Information (PII) and For Official Use Only (FOUO) data is stored on Laptops, desktop systems, Databases, and also is included within email traffic used for daily business transactions. Unauthorized access to these devices creates potential risks to ARNG operations ranging from disclosure of sensitive personnel and operational information to intrusions and data gathering within our network. PII is identified as; “Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc”.

3. Applicability: All personnel assigned, attached, or subordinate to the Army National Guard (ARNG).

4. Policy. Effective immediately, all activities, and personnel within the ARNG will follow this policy.

   a. Commander, supervisors, leaders and State JFHQ DOIM’s must insure all personnel are aware of their responsibility to prevent the loss or theft of government owned or leased information technology (IT) equipment including mobile IT devices such as laptop computers. In the wrong hands, this information may damage the reputations of the ARNG, the US. Army, and effect the livelihood of our soldiers, civilians, and family members.

   b. Laptop computers are known targets of theft because of their portability, cost and the likelihood to contain sensitive information when laptops are not used, they will be secured with a cable locking device in a locked office or other secure location. Proper use of cable locks are required at all laptops to include when mounted in a docking station when used on a desktop or any other working environment. All ARNG laptops and Mobile devices will be considered as a sensitive item and properly marked as required within the DA “Road Warrior” Laptop Security Version 1.3

   c. When traveling with a laptop, PDA, or other external devices (I.E. Hard Drive) outside of regular place of duty personnel will not leave a laptop unattended in a government owned vehicle or privately owned vehicle. The prohibition applies even if the vehicle is locked, the computer is in the trunk or secured by an approved locking device. Personnel will carry the laptop on their person or otherwise maintain positive visual or physical control of the laptop at all times. When traveling by airplane or train if the carrying case is too large, the laptop will be removed from the case and be hand carried. A Laptop will never be left unattended in an unsecure hotel room or an unsecured residence. Unassigned laptops will be secured in a locked closet, locked cabinet, or locked filing cabinet.

d. All ARNG personnel utilizing ARNG, Department of The Army (DA), and Department of Defense (DOD) email systems will ensure that any email sent with PII information and FOUO data is properly encrypted and digitally signed before sending to any entity to include those outside of DOD. If the email and/or attachments cannot be encrypted with DOD PKI Encryption Technology the email will not be sent.

e. DOD, DA, or ARNG Identifiable Information (PII) and For Official Use Only (FOUO) data will never be transferred or stored on Personnel or Contract owned Information Technology (IT) systems. Contract owned systems if storing PII or FOUO data for Government Business will meet all DOD and DA configuration, Security Technical Implementation Guides (STIGS) and policy standards.

f. The goal of DOD and DA at this time is to have all IT systems to include Laptops, Desktop, and Servers deployed with a Data at Rest solution. The ARNG G6 understands that due to funding restrains that that goal is unachievable at this time.

g. Effective immediately all ARNG systems that are in use on a desktop or in a mobile environment will have a DAR solution installed. The DAR Solution used will either be one from the Army Approved Army Information Assurance Approved Product List (AIAAPL), EFS with Microsoft XP or Bit locker with Microsoft Vista. In addition they will meet physical security requirements mentioned in paragraphs 4 b and c of this policy.

h. When a PII incident is identified the ARNG Army National Guard (ARNG) Reporting Guidance for Personally Identifiable Information (PII) Incidents will be followed. This policy can be obtained with the state G6/DOIM.

5. Any user who violates this policy will be punished in accordance with AR 25-2.

6. Any user/section/division that requires a written exception to this policy must submit their requirements to this office in writing with signature for written approval.

7. POC is Mr. Hair at NGB-ARZ-CIO-IA 703-607-9632

W. Scott Moser
Colonel, GS
G6, Army National Guard