INFORMATION PAPER

ARNG-IMN-S
1 March 2011

SUBJECT: Army National Guard (ARNG) Reporting Guidance for Personally Identifiable Information (PII) Incidents

1. Purpose: To provide guidance procedures for reporting PII incidents.

2. References:

a. Office of Management and Budget Memorandum M-07-16, 22 May 07, Subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).
b. (Superseded by M-07-16 22 May 07) (Superseded by 5 Jun 09 DoD Policy) (Superseded by 5 Jun 09 DoD Policy)Department of Defense Director of Administration and Management Memorandum, 5 Jun 09, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
c. Department of Defense Regulation 5400.11-R, 14 May 07, Department of Defense Privacy Program.
d. The Army Privacy Program Final Rule, 10 Aug 06, 32 CFR Part 505
e. AR 25-2, Rapid Action Revision (RAR) Chapter 4, Section VIII (page 43, para 4-21), Incident and Intrusion Reporting, DTD 24 OCT 07 (superseded by 23 Mar 09 DoD Policy).
f. ALARACT 050/2009, Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, DTD 26 FEB 09 (Superseded by 26 Feb 09 ALARACT).

3. Facts: In the event of loss or suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of PII involving computer related technology (Example: lost or stolen laptops or other computer devices, and e-mails sent to individuals without a need to know) utilize the following step-by-step reporting procedures. If the PII incident is not computer related (Example: loss of paper records or verbal disclosure) immediately contact your local Freedom of Information Act (FOIA)/Privacy Officer or the NGB Privacy Office.

a. Individual(s) will **immediately notify** chain-of-command and local State DOIM of intent to submit a PII Breach Report incident report (available at https://www.rmda.army.mil/privacy/docs/DoD-PII-Incident-Reporting-Template.doc).

b. **Within one (1) hour** of the loss or suspected loss of PII, the incident will be reported to the US-CERT at https://forms.us-cert.gov/report/.

c. **Within four (4) hours** of the incident the State G6/J6 will contact their local FOIA/Privacy office and the DoD PII Breach Report will be completed. Once the PII Breach Report is completed, the report in (MS Word) will be sent by your local FOIA/Privacy office to the NGB Privacy Office at privacy@ng.army.mil. Their office will review and make necessary updates to the report and forward it to the DA Privacy Office for further reporting to the DoD Privacy Office. A courtesy copy of the submission will be provided to the State FOIA/Privacy Office and the NGB CND Analysis Team.

d. **Within four (4) hours** of the incident the State Joint Operations center will file a Serious Incident Report (SIR) with the National Guard Bureau Joint Operations Center (NGB JOC).

e. **Within four (4) hours** of the incident the State G6/J6 will contact the NGB CND Analysis Team at Cert-Analysis@ng.army.mil (COMM 703-607-8455 / DSN 327-8455) and open an incident ticket. Copies of all documents, to include reports filed with the US-CERT, the Serious Incident Report (SIR), and the PII Breach Report need to be forwarded (via signed email) to NGB CND Analysis.

f. In compliance with DoD's 5 Jun 09 Policy, found at http://privacy.defense.gov/files/PII_Memo_Safeguard.pdf, a Risk Assessment, (found on page 17 of the policy), will be completed to determine whether or not impacted individuals must be notified of the incident. This overall assessment will be indicated in block H of the DoD PII Breach Report.

g. If the overall risk assessment is "HIGH", the State chain-of-command will notify affected individuals of the incident within 10 days using first-class mail using the guidance found on pages 11-13 of DoD's 5 Jun 09 policy. A sample notification letter can be found in Appendix 2 of DoD 5400.11-R, Defense Privacy Program. In addition to the contents of the sample letter, you may wish to include the NG Identity Theft Website as a resource for impacted individuals to obtain information about identity theft, http://www.ng.mil/features/identity/default.aspx.

h. If the unit is unable to ascertain specific individuals that are impacted, they will issue a generalized (substitute) notice to the potentially impacted population (Ref DoD 5400.11-R, paragraph C1.5. and page 13 of DoD 5 Jun 09 Policy). A sample notification letter is located on the NGB Privacy website, https://gkoportal.ngb.army.mil/sites/NGB-SpecialStaff/JA/privacy/default.aspx.

i. Coordinate with NGB Public Affairs office prior to notifying or discussing the incident with the media. If there is a significant breach impacting thousands of individuals, the state may consider informing the media of the incident when necessary. The NGB Public Affairs should be given notice of any such press releases.

4. POC is Mr. John Hair, ARNG IAPM, 703-607-9632, john.hair@us.army.mil. This document along with other important PII information is located on the ARNG IMN-S PII web site https://gkoportal.ngb.army.mil/sites/AIN/IA/CND/PII/default.aspx.

Action Officer: John C. Hair / 703-607-9632
Approved by: LTC Susan Camoroda, ARNG-IMN