DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT GORDON
307 CHAMBERLINE
FORT GORDON, GEORGIA 30905-5730

REPLY TO
ATTENTION OF:

IMSE-GOR-HR

NOV 2 2 2011

MEMORANDUM FOR All Garrison Personnel, Fort Gordon, GA 30905

SUBJECT: Garrison Commander's Policy Memorandum No. 22— Safeguarding Personally Identifiable Information (PII)

1. References.

a. Title 5, United States Code, Section 552a, Privacy Act of 1974 and Section 552, Freedom of Information Act.

b. 32 Code of Federal Regulation Part 505, The Anny Privacy Act; Final Rule. Federal Register, (Volume 71, Number 154), dated 10 August 2006.

c. Department of Defense (000) Regulation 5400.11-R. DoD Privacy Act Program, dated 14 May 2007.

d. Office of Management and Budget Memorandum, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, dated 22 May 2007.

e. Army Regulation 25·55, Freedom of Information Act Program, dated 1 November 1997.

f. ALARACT Message, Vice Chief of Staff of the Army, subject: Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, dated 251400JUL07.

g. NETCALL 2007-46, Anny Personnel Responsibility for Safeguarding Personally Identifiable Information, email message, Commanding General, Installation Management Command, dated 17 October 2007.

h. Anny Privacy Act Program Office website, http://www.nnda.belvoir.anny.miUnndaxmVnndalPrivacvActProg-Guidance.asp, retrieved 29 May 2008.

2. Purpose. To establish policy for safeguarding Personally Identifiable Information (PII). In the event of conflicting requirements between this policy and the regulations of higher headquarters, the most stringent will be followed.

3. Applicability. This policy is applicable to all Garrison Directorates and Principal Staff Offices.

4. Background. Personally Identifiable Information is any information which can be potentially used to uniquely identity, contact, or locate a single person or trace a person's identity, including but not limited to social security number (SSN), education, and criminal or employment history, mother's maiden name, date and place of birth, biometric records, medical history, and financial transactions. As a result of the increase in identity theft and change in our security posture due to Overseas Contingency Operations, it has become increasingly important that we implement measures to protect PII. Nonetheless, public law as well as Department of the Defense and Army regulations also mandates that we safeguard individuals' PII.

5. Responsibilities.

a. All Garrison Directors and Principal Staff Officers.

(1) Execute the Privacy Act Program within your areas.

(2) Ensure all Soldiers, civilians and DOD contractors complete mandatory annual and Refresher Privacy Act training, available at: https://www.hrc.army.mil/iws?page id-12250.

(3) Ensure that all personnel are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act Program.

(4) Ensure internal procedures and safeguards are developed, implemented, and maintained to protect PII, to include mandatory reporting of breaches IAW reference 1f.

(5) Review information posted to public website and pubic folder share drives to ensure PII is not stored on command/directorate public websites and public folder share drives.

(6) Ensure Emergency Recall Rosters, social rosters, etc. are only being shared with those who have an official need to know the information and that the information is being marked "For Official Use Only (FOUO)," per reference 1e.

b. Director of Family and Morale Welfare and Recreation Director of Logistics. Monitor the installation's recycle program to ensure PII information is being safeguarded during the disposal recycle process.

c. Director of Public Works. Provide assistance to Garrison personnel who request "day only" cleaning services in order to diminish vulnerability of PII within work areas after duty hours.

d. Director of Human Resources.

(1) Develop/implement policies and procedures to protect PII.

(2) Serve as proponent for PII incident reporting.

(3) Conduct Privacy Act training as needed.

e. Supervisors and Managers. Conduct periodic checks of work areas to ensure/monitor compliance with this policy letter.

f. All Personnel.

(1) Limit the information collected to that which is necessary for military purposes and required by regulation.

(2) Not disclose any personal information contained in a Privacy Act system of records, except as authorized by reference la and c, or other applicable laws.

(3) Maintain PII according to AR 340-21, Army Privacy Act Program, and establish proper administrative, technical, and physical safeguards to ensure the security and confidentiality of records.

(4) Immediately report all incidents involving the actual or suspected breach/compromise of PII in accordance with IMCOM Regulation 190-1, Serious Incident Reports, reference 1g; and the Army reporting procedures in reference 1f.

(5) During duty hours, reasonable steps should be taken to minimize the risk of access to SSN's and FOUO information by unauthorized personnel. After duty hours, documents containing SSN's and FOUO information should be stored in a locked office. If this is not feasible, documents containing SSN's and FOUO information should be stored in a locked container, desk, or file cabinet.

(6) When transmitting via distribution/courier, ensure "FOUO" cover is placed on top of the document and place in a sealed envelope with FOUO annotated on the outside front cover.

(7) Maintain records for the minimum time required in accordance with AR 25-400-2, Army Records Information Management System (ARIMS).

(8) Documents containing FOUO information should be destroyed using strip cut shredding method. If shredding is not possible, destroy the documents by tearing into several pieces or any other means that would ensure all identifiable information has been destroyed.

Dispose of materials in several separate containers to reduce chances of unauthorized collection and reassembly of strip cut and hand torn documents.

6. The proponent for this policy is Chief, Administrative Services Branch, Directorate of Human Resources, 706-791-2004.

ROBERT A. BARKER
COL, SC
Commanding

This memorandum supersedes Garrison Commander's Policy Memorandum No. 35— Safeguarding Personally Identifiable Information (PII), dated 8 March 2010.