DEPARTMENT OF THE ARMY
93D SIGNAL BRIGADE (STRATEGIC)
US ARMY SIGNAL NETWORK ENTERPRISE CTR – FORT GORDON
245 O' CLUB DRIVE
FORT GORDON, GEORGIA 30905

REPLY TO
ATTENTION OF

NETC-SFG-DT

1 February 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Protection of Personally Identifiable Information (PII) Policy

1. REFERENCES:

a. AR 340-21, The Army Privacy Program, 5 July 1985.

b. Memorandum, Department of Defense, 18 August 2006, subject: DoD Guidance on Protecting Personally Identifiable Information.

c. DoD Regulation 5400.11-R, subject: Department of Defense Privacy Program, 14 May 2007.

d. Memorandum, Office of the Secretary of Defense, 21 September 2007, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

e. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008.

f. Memorandum, Department of the Army, 31 July 2009, Subject: Updated Guidance for Submission of Privacy Impact Assessments (PIA).

g. Fort Gordon, GA Policy Memorandum No. 22 Safeguarding Personally Identifiable Information (PII), 22 Nov 11.

2. PURPOSE: Establish a Fort Gordon Network Enterprise Center policy providing the definition of Personally Identifiable Information (PII) and include specific procedures on how to protect, encrypt and report the loss of PII. The NEC mandates the protection and handling of all PII and requires the proper encryption of PII belonging to soldiers, Department of the Army Civilians and Contractors.

3. APPLICABILITY: This document provides policy and guidance for the Fort Gordon Installation and subordinate units as well as any units responsible for processing, maintaining or storing personnel's PII.

4. POLICY:

a. All personnel have a direct responsibility to ensure privacy act and PII are collected, maintained, used and disseminated only as authorized. Fort Gordon personnel are further required to protect all PII data (hardcopy or electronic) from unauthorized use, access, disclosure, alteration or destruction. PII will not be released to anyone who does not have a duty-related official need to know.

b. PII is defined as any information about an individual that is intimate or private to the individual, as distinguished from information related solely to the 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 (such as name, social security number, date and place of birth, mother's maiden name, biometric records, and so forth) including other personal information which is linked or linkable to an individual.

c. PII will be given the protections afforded "For Official Use Only" documents and protected in accordance with DoD Regulation 5200.1-R. Appendix 3, Jan 97.

d. The acceptable methods for disposal of paper records are tearing, burning, melting, chemical decomposing, pulping, pulverizing, shredding, or mutilating. For electronic records and media disposal methods, such as overwriting, degaussing, disintegrating, pulverizing, burning, melting, incinerating, shredding or sanding are acceptable.

e. All Fort Gordon personnel using a government information system, to include offsite Fort Gordon contracted agencies and/or vendors, are responsible and directed to encrypt Sensitive Information per Army Regulation 25-1, 6-4 m (7). Email requiring data integrity, message authenticity, or non-repudiation of DOD sensitive information, other than personal information sent by information-privileged individuals, volunteers, or Reservists, will be signed using DOD-approved certificates. The CAC is the DOD primary token for PKI cryptographic keys and their corresponding certificates. A DOD PKI encryption certificate will be used to sign and encrypt sensitive information for transmission via email. Further, sensitive information transmitted in email messages must be clearly labeled to show its sensitivity, such as “Sensitive - Privacy Act Information.” Signature/encryption will be used to send information that is—

(1) Protected by the Privacy Act, 5 USC 552a. The Privacy Act includes protection of personally identifiable information.

(2) Identified as FOUO.

(3) Protected under HIPAA (See also paragraph 2–21*c* and References).

(4) Otherwise sensitive (as defined in the glossary).

f. Lost/stolen or compromised PII must be reported immediately and within 24 hours of discovery to the Users Information Management Officer/Assurance Officer/Manager (IMO/IASO/IAM) and https://www.rmda.army.mil/privacy/foia-incidentreport1.asp and within one hour to US-CERT https://forms.us-cert.gov/report .

g. Personnel with authorized access to PII will complete the training in the Freedom of Information Act, Privacy Act and Personally Identifiable Information (PII). The "TIA-WPII-5404 Personally Identifiable Information (PII)" course will be completed on the https://ia.gordon.army.mil site and will be verified using the Army Training and Certification Tracking System (ATCTS).

h. Privacy Impact Assessments (PIA) is a checklist that must be performed by all data and system owners and verified by submitting DD Form 2930 on all systems that collect, maintain, use, or disseminate PII on the general public, federal personnel (government civilians, members of the military, and Non-appropriated fund employees), contractors, and in some cases Foreign Nationals and the following additional situations:

(1) Prior to developing or purchasing new DoD information or electronic systems, (this includes information systems and electronic collections supported through contracts with external sources that collect, maintain, use, or disseminate PII).

(2) There is a significant change to a system that collects, maintains, uses or disseminates PII, to include new application functionalities; a change in privacy or security posture; a significant change in how PII is managed on the system; or when a change creates new privacy risks.

(3) For legacy systems and electronic collections that maintain, use or disseminate PII where a PIA has not previously been completed.

(4) When converting from paper-based records that contain PII to an electronic system.

(5) If the system does not collect, maintain, or disseminate PII, only Section 1 of the DD Form 2930 must be completed.

i. A PIA must be reviewed and updated every three years. This may be accomplished in conjunction with the Certification and Accreditation (C&A) cycle as a component of the 000 Information Assurance Certification and Accreditation Process (DIACAP) package.

j. A PIA is not required for Nation Security Systems (including systems that process classified information) or doesn't collect maintain or disseminate PII.

k. All PII shall be evaluated for impact of loss or unauthorized disclosure and protected accordingly.

l. All PII electronic records shall be assigned a High or Moderate PII Impact Category.

m. PII Impact Category: For DoD information assurance purposes, consistent with reference (e) and FIPS 199, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure:

(1) High Impact: Any Defense-wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on *500* or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act. Also, any compilation of electronic records containing PII on less than *500* individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on *500* or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of *500* or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII.

(2) Moderate Impact: Any electronic records containing PII not identified as High Impact.

n. Electronic PII records assigned a High Impact Category shall be protected as follows:

(1) Such records shall not be routinely processed or stored on mobile computing devices or removable electronic media without express approval of the local Designated Accrediting Authority (DAA) (previously Designated Approving Authority).

(2) Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores High Impact electronic records shall be restricted to workplaces that minimally satisfy physical and Environmental Controls for Confidentiality Level Sensitive as referred to as "protected workplaces."

o. Any mobile computing device containing High Impact electronic records removed from protected workplaces, including those approved for routine processing, shall be signed in and out

with a supervising official designated in writing by the organization security official. See Appendix A for sign-in-and -out-card.

5. The point of contact for this action is Queen D. Harts, Installation Information Assurance Manager (IIAM); 706-791-0042; email: queen.d.harts.civ@mail.mil.

LISA E. McCLEASE
Director, Network Enterprise Center-FT Gordon

DISTRIBUTION: A