UNITED STATES OF AMERICA	)	
	)	
v.	)	**PROSECUTION MOTION**
	)	**FOR JUDICIAL NOTICE**
Manning, Bradley E.	)	
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	**Enclosure 9**
Joint Base Myer-Henderson Hall	)	
Fort Myer, Virginia 22211	)	**24 June 2013**

DoD 5400.11-R

DEPARTMENT OF DEFENSE PRIVACY PROGRAM

May 14, 2007

OFFICE OF THE DIRECTOR, ADMINISTRATION AND MANAGEMENT

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION AND MANAGEMENT

MAY 1 4 2007

FOREWORD

This Regulation is reissued under the authority of DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007 (Reference (a)). It provides guidance on section 552a of title 5 United States Code (U.S.C.), the Privacy Act of 1974, as amended, (Reference (b)), and prescribes uniform procedures for implementation of the DoD Privacy Program.

DoD 5400.11-R, "Department of Defense Privacy Program," August 13, 1983, is hereby canceled.

This Regulation applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to as the "DoD Components").

The provisions of this Regulation shall be applicable by contract or other legally binding action to U.S. Government contractors whenever a DoD contract requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records on behalf of the contracting DoD Component. When maintaining a system of records or a portion of a system of records, contractors and their employees shall be considered employees of the contracting DoD Component for purposes of the criminal penalties of the Act.

This Regulation does not apply to:

- Requests for information made under the Freedom of Information Act (DoD Directive 5400.7) (Reference (c)). They are processed in accordance with DoD 5400.7-R (Reference (d)).

- Requests for information from systems of records controlled by the Office of Personnel Management (OPM), although maintained by a DoD Component. These are processed in accordance with policies established by OPM (Reference (e)).

- Requests for personal information from the General Accountability Office. These are processed in accordance with DoD Directive 7650.1 (Reference (f)).

- Requests for personal information from Congress. These are processed in accordance with DoD Directive 5400.4 (Reference (g)), except for the specific provisions in Chapter 4 of this Regulation.

This Regulation is effective immediately and its use is mandatory for all DoD Components. The Heads of the DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their Components. Such instructions may not conflict with the provisions of this Regulation.

Send recommended changes to this Regulation to the following address:

Director, Defense Privacy Office
1901 South Bell Street, Room 920
Arlington, VA 22202-4512

The DoD Components may obtain copies of this Regulation through their own publication channels. Approved for public release; distribution unlimited. Copies are available via the World Wide Web at http://www.dtic.mil/whs/directives. Authorized registered users may obtain copies of the publication from the Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218. Other Federal Agencies and the public may obtain copies from the U.S Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

Michael B. Donley
DoD Senior Privacy Official

DL1. DEFINITIONS

DL1.1. Access. For the purposes of this Regulation, the review of a record or a copy of a record, or parts thereof, in a system of records by any individual.

DL1.2. Agency. For the purposes of disclosing records subject to the Privacy Act (Reference (b)) among the DoD Components, the Department of Defense is a considered a single agency. For all other purposes, to include requests for access and amendment, denial of access, or amendment, appeals from denials, and record keeping, as relating to the release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of Reference (b).

DL1.3. Computer Matches. The computerized comparison of two or more automated systems of records or a system of records with non-Federal records. Manual comparison of systems of records or a system of records with non-Federal records are not covered.

DL1.4. Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise, if made on or after September 27, 1975, that the person's or the organization's identity shall be held in confidence or under an implied promise of such confidentiality if this implied promise was made on or before September 26, 1975.

DL1.5. Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

DL1.6. Federal Benefit Program. A program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

DL1.7. Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits).

DL1.8. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual may also act on behalf of an individual. Members of the U.S. Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals" when acting in an entrepreneurial capacity with the Department of Defense, but are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits, etc.).

DL1.9. Individual Access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

DL1.10. Lost, Stolen, or Compromised Information. Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches.

DL1.11. Maintain. To maintain, collect, use, or disseminate records contained in a system of records.

DL1.12. Non-Federal Agency. Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a computer matching program.

DL1.13. Official Use. Within the context of this Regulation, this term is used when officials and employees of a DoD Component have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R (Reference h)).

DL1.14. Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).

DL1.15. Privacy Act. The Privacy Act of 1974, as amended, 5 U.S.C. 552a (Reference (b)).

DL1.16. Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

DL1.17. Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

DL1.18. Recipient (matching) Agency. Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a computer matching program.

DL1.19. Record. Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.), about an individual that is maintained by a DoD Component, including, but not limited to, an individual's education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.

DL1.20. Risk Assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

DL1.21. Routine Use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

DL1.22. Source Agency. Any agency which discloses records contained in a system of records to be used in a computer-matching program, or any state or local government or agency thereof, which discloses records to be used in a computer-matching program.

DL1.23. Statistical Record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

DL1.24. System of Records. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

AP1. APPENDIX 1

SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

AP1.1. GENERAL

AP1.1.1. The IT environment subjects personal information to special hazards as to unauthorized compromise, alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in IT systems consistent with the requirements of DoD Directive 8500.1 (Reference (ac)) and (ae).

AP1.1.2. Personally identifiable information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

AP1.1.3. IT facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated "FOUO." (See Reference (h).)

AP1.2. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

AP1.2.1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse. (See OMB Circular A-130, Reference (ab) and DoD Instruction 8500.2 (Reference (ae).)

AP1.2.2. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

AP1.3. MINIMUM ADMINISTRATIVE SAFEGUARDS

The minimum safeguarding standards as set forth in paragraph C1.4.2. of Chapter 1 apply to all personal data within any IT system. In addition:

AP1.3.1. Consider the following when establishing IT safeguards:

AP1.3.1.1. The sensitivity of the data being processed, stored and accessed.

AP1.3.1.2. The installation environment.

AP1.3.1.3. The risk of exposure.

AP1.3.1.4. The cost of the safeguard under consideration.

AP1.3.2. Label or designate media products containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products "For Official Use Only" in accordance with Reference (h) satisfies this requirement.

AP1.3.3. Mark and protect all computer products containing classified data in accordance with References (h) and (ac).

AP1.3.4. Mark and protect all computer products containing "For Official Use Only" material in accordance with Reference (h).

AP1.3.5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

AP1.3.6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

AP1.3.7. Train personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

AP1.4. PHYSICAL SAFEGUARDS

AP1.4.1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

AP1.4.2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

AP1.4.3. Safeguard on-line devices directly coupled to IT systems that contain or process information from systems of records to prevent unauthorized disclosure, use, or alteration.

AP1.4.4. Dispose of paper records following appropriate record destruction procedures. (See paragraph C1.4.3. and Reference (h).)

AP1.5. TECHNICAL SAFEGUARDS

AP1.5.1. Components are to ensure that all PII not explicitly cleared for public release is protected according to Confidentially Level Sensitive, as established in DoD Instruction 8500.2 (Reference (ae)). In addition, all DoD information and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing.

AP1.5.2. Encrypt unclassified personal information in accordance with current Information Assurance (IA) policies and procedures, as issued.

AP1.5.3. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

AP1.5.4. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

AP1.5.5 Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to IA controls specified in Reference (ae).

AP1.5.6 Remote access for processing PII should comply with the latest IA policies and procedures.

AP1.5.7. Minimize access to data fields necessary to accomplish an employee's task - normally, access shall be granted only to those data elements (fields) required for the employee to perform his or her job rather than granting access to the entire database.

AP1.5.8. Do not totally rely on proprietary software products to protect personnel data during processing or storage.

AP1.6. SPECIAL PROCEDURES

AP1.6.1. Managers shall:

AP1.6.1.1. Prepare and submit for publication all system notices and amendments and alterations thereto. (See paragraph C6.1.6. of Chapter 6.)

AP1.6.1.2. Identify required controls and individuals authorized access to PII and maintain updates to the access authorizations.

AP1.6.1.3. When required, ensure Privacy Impact Assessments are prepared consistent with the requirements of Section 3501 of title 44, U.S.C. (Reference (ad)) and the DoD Deputy Chief Information Officer Memorandum (Reference (af)).

AP1.6.1.4. Train all personnel whose official duties require access to the system of records in the proper safeguarding and use of the information and ensure that they receive Privacy Act training.

AP1.7. RECORD DISPOSAL

AP1.7.1. Dispose of records subject to this Regulation so as to prevent compromise. (See paragraph C1.4.3. of Chapter 1.) Magnetic tapes or other magnetic medium may be cleared by degaussing, overwriting, or erasing. (See the DoD Memorandum (Reference (ag).)

AP1.7.2. Do not use respliced waste computer products containing personal data.