BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

[Docket ID: DOD-2013-OS-0023]

RIN 0790-AJ03

DoD Privacy Program

AGENCY: Director of Administration and Management, DoD.

ACTION: Proposed rule; amendment.

SUMMARY: This rule updates the established policies, guidance, and assigned responsibilities of the DoD Privacy Program pursuant to The Privacy Act and Office of Management and Budget (OMB) Circular No. A-130; authorizes the Defense Privacy Board and the Defense Data Integrity Board; prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program; and delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

DATES: Comments must be received by **[insert date 60 days from date of publication]**.

ADDRESSES: You may submit comments, identified by docket number and/or RIN number and title, by any of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria VA 22350-3100.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Samuel P. Jenkins, 703-571-0070.

SUPPLEMENTARY INFORMATION:

Executive Summary

I. Purpose of the Regulatory Action

a. The need for the regulatory action and how the action will meet that need.

An individual's privacy is a fundamental legal right that must be respected and protected. This regulatory action ensures that DoD's need to collect, use, maintain, or disseminate personally identifiable information (PII) about individuals for purposes of discharging its statutory responsibilities will be balanced against their right to be protected against unwarranted privacy invasions. This regulatory action also describes the rules of conduct and responsibilities of DoD personnel DoD contractors, and DoD contractor personnel to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.

b. Succinct statement of legal authority for the regulatory action (explaining, in brief, the legal authority laid out later in the preamble).

Authority: 5 U.S.C. 552a, OMB Circular No. A-130

II. Summary of the Major Provisions of the Regulatory Action in Question

This rule:

a. Establishes rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any system of records.

b. Establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

c. Ensures that guidance, assistance, and subject matter expert support are provided to the combatant command privacy officers in the implementation and execution of and compliance with the DoD Privacy Program.

d. Ensures that laws, policies, procedures, and systems for protecting individual privacy rights are implemented throughout DoD.

III. Costs and Benefits

This regulatory action imposes no monetary costs to the Agency or public. The benefit to the public is the accurate reflection of the Agency's Privacy Program to ensure that policies and procedures are known to the public. The revisions to this rule are part of DoD's retrospective plan under EO 13563 completed in August 2011. DoD's full plan can be accessed at http://exchange.regulations.gov/exchange/topic/eo-13563.

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

It has been certified that 32 CFR part 310 does not:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

Sec. 202, Pub. L. 104-4, "Unfunded Mandates Reform Act"

It has been certified that 32 CFR part 310 does not contain a Federal mandate that may result in expenditure by State, local and tribal governments, in aggregate, or by the private sector, of $100 million or more in any one year.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. 601)

It has been certified that 32 CFR part 310 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been certified that 32 CFR part 310 does not impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

Executive Order 13132, "Federalism"

It has been certified that 32 CFR part 310 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 310

Privacy.

Accordingly 32 CFR part 310 is proposed to be amended to read as follows:

PART 310—[AMENDED]

1. The authority citation for 32 CFR part 310 is revised to read as follows:

Authority: 5 U.S.C. 552a, OMB Circular No. A-130.

2. Section 310.2 is revised to read as follows:

§310.2 Purpose.

This part:

(a) Updates the established policies, guidance, and assigned responsibilities of the DoD Privacy Program pursuant to 5 U.S.C. 552a (also known and referred to in this part as "The Privacy Act") and Office of Management and Budget (OMB) Circular No. A-130.

(b) Authorizes the Defense Privacy Board and the Defense Data Integrity Board.

(c) Prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program.

(d) Delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

3. Section 310.3 is revised to read as follows:

§310.3 Applicability and scope.

(a) This part applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense

Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this part as the "DoD Components").

(b) For the purposes of subsection (i), Criminal penalties, of The Privacy Act, any DoD contractor and any employee of such a contractor will be considered to be an employee of DoD when DoD provides by a contract for the operation by or on behalf of DoD of a system of records to accomplish a DoD function. DoD will, consistent with its authority, cause the requirements of section (m) of The Privacy Act to be applied to such systems.

4. Section 310.4 is revised to read as follows:

§310.4 Definitions.

(a) Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

(b) Agency. For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the Department of Defense is 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 release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of the Privacy Act.

(c) Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information (PII), whether physical or electronic.

(d) Computer matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

(e) 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.

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

(g) DoD contractor. Any individual or other legal entity that:

(1) Directly or indirectly (e.g., through an affiliate) submits offers for or is awarded, or reasonably may be expected to submit offers for or be awarded, a government contract, including a contract for carriage under government or commercial bills of lading, or a subcontract under a government contract; or

(2) Conducts business, or reasonably may be expected to conduct business, with the federal government as an agent or representative of another contractor.

(h) DoD personnel. Service members and federal civilian employees.

(i) 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.

(j) 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).

(k) Individual. A living person who is a U.S. citizen or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual, except as otherwise provided in this part. Members of the Military Services 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 DoD, but persons employed by such organizations or entities are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits).

(l) Individual access. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

(m) Information sharing environment. Defined in Public Law 108-458, "The Intelligence Reform and Terrorism Prevention Act of 2004".

(n) 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 purpose where one or more individuals will be adversely affected. Such incidents also are known as breaches.

(o) Maintain. The collection, maintenance, use, or dissemination of records contained in a system of records.

(p) Member of the public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

(q) Mixed system of records. Any system of records that contains information about individuals as defined by the Privacy Act and non-U.S. citizens and/or aliens not lawfully admitted for permanent residence.

(r) 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.

(s) Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated a need for the record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R.[5]

(t) Personally identifiable information (PII). Information 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, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. For purposes of this part, the term PII also includes personal information and information in identifiable form.

(u) 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.

[5] See footnote 1 to §310.1.

(v) Protected health information (PHI). Defined in DoD 6025.18-R, "DoD Health Information Privacy Regulation" (available at http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf).

(w) Recipient 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.

(x) Record. Any item, collection, or grouping of information in any media (e.g., paper, electronic), about an individual that is maintained by a DoD Component, including, but not limited to, education, financial transactions, medical history, criminal or employment history, and that contains the name, or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph.

(y) Risk assessment. An analysis considering information sensitivity, vulnerabilities, and cost in safeguarding personal information processed or stored in the facility or activity.

(z) 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.

(aa) 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.

(bb) 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.

(cc) System of records. A group of records under the control of a DoD Component from which PII is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular uniquely assigned to an individual.

(dd) System of records notice (SORN). A notice published in the Federal Register that constitutes official notification to the public of the existence of a system of records.

5. Section 310.5 is revised to read as follows:

§310.5 Policy.

It is DoD policy that:

(a) An individual's privacy is a fundamental legal right that must be respected and protected.

(1) The DoD's need to collect, use, maintain, or disseminate (also known and referred to in this part as "maintain") PII about individuals for purposes of discharging its statutory responsibilities will be balanced against their right to be protected against unwarranted privacy invasions.

(2) The DoD protects individual's rights, consistent with federal laws, regulations, and policies, when maintaining their PII.

(3) DoD personnel and DoD contractors have an affirmative responsibility to protect an individual's privacy when maintaining his or her PII.

(4) Consistent with section 1016(d) of Public Law 108-458 and section 1 of Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans", the DoD will protect information privacy and provide other protections relating to civil liberties and legal rights in the development and use of the information sharing environment.

(b) The DoD establishes rules of conduct for DoD personnel and DoD contractors involved in the design, development, operation, or maintenance of any system of records. DoD personnel and DoD contractors will be trained with respect to such rules and the requirements of this

section and any other rules and procedures adopted pursuant to this section and the penalties for noncompliance. The DoD Rules of Conduct are established in §310.8.

(c) DoD personnel and DoD contractors conduct themselves consistent with the established rules of conduct in §310.8, so that records maintained in a system of records will only be maintained as authorized by 5 U.S.C. 552a and this part.

(d) DoD legislative, regulatory, or other policy proposals will be evaluated to ensure consistency with the information privacy requirements of this part.

(e) Pursuant to The Privacy Act, no record will be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution of the United States (referred to in this part as "the First Amendment"), except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation.

(f) Disclosure of records pertaining to an individual from a system of records is prohibited except with his or her consent or as otherwise authorized by 5 U.S.C. 552a and this part or 32 CFR part 286. When DoD Components make such disclosures, the individual may, to the extent authorized by 5 U.S.C. 552a and this part, obtain a description of such disclosures from the Component concerned.

(g) Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency is prohibited to the extent authorized by Public Law 86-36, "National Security Agency-Officers and Employees" and 10 U.S.C. 424. Disclosure of records pertaining

to personnel of overseas, sensitive, or routinely deployable units is prohibited to the extent authorized by 10 U.S.C. 130b.

(h) The DoD establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

(i) Disclosure of PHI will be consistent with DoD 6025.18-R.

(j) All DoD personnel and DoD contractors will be provided training pursuant to 5 U.S.C. 552a and OMB Circular No. A-130.

(k) PII collected, used, maintained, or disseminated will be:

(1) Relevant and necessary to accomplish a lawful DoD purpose required by statute or Executive Order.

(2) Collected to the greatest extent practicable directly from the individual. He or she will be informed as to why the information is being collected, the authority for collection, how it will be used, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

(3) Relevant, timely, complete, and accurate for its intended use.

(4) Protected using appropriate administrative, technical, and physical safeguards based on the media (e.g., paper, electronic) involved. Protection will ensure the security of the records and prevent compromise or misuse during maintenance, including working at authorized alternative worksites.

(l) Individuals are permitted, to the extent authorized by 5 U.S.C. 552a and this part, to:

(1) Upon request by an individual, gain access to records or to any information pertaining to the individual which is contained in a system of records.

(2) Obtain a copy of such records, in whole or in part.

(3) Correct or amend such records once it has been determined that the records are not accurate, relevant, timely, or complete.

(4) Appeal a denial for a request to access or a request to amend a record.

(m) Non-U.S. citizens and aliens not lawfully admitted for permanent residence may request access to and amendment of records pertaining to them; however, this part does not create or extend any right pursuant to The Privacy Act to them.

(n) SORNs and notices of proposed or final rulemaking are published in the Federal Register (FR), and reports are submitted to Congress and OMB, in accordance with 5 U.S.C. 552a, OMB Circular No. A-130, and this part, DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements" (available at http://www.dtic.mil/whs/directives/corres/pdf/891001m.pdf), and DoD Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements" (available at http://www.dtic.mil/whs/directives/corres/pdf/554502p.pdf). Information about an individual maintained in a new system of records will not be collected until the required SORN publication and review requirements are satisfied.

(o) All DoD personnel must make reasonable efforts to inform an individual, at their last known address, when any record about him or her is disclosed:

(1) Due to a compulsory legal process.

(2) In a manner that will become a matter of public record.

(p) Individuals must be notified in a timely manner, consistent with the requirements of this part, if there is a breach of their PII.

(q) At least 30 days prior to disclosure of information pursuant to subparagraph (e)(4)(D) (routine uses) of The Privacy Act, the DoD will publish an FR notice of any new use or intended use of the information in the system, and provide an opportunity for interested people to submit written data, views, or arguments to the agency.

(r) Computer matching programs between the DoD Components and federal, state, or local governmental agencies are conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(s) The DoD will publish in the FR notice any establishment or revision of a matching program at least 30 days prior to conducting such program of such establishment or revision if any DoD Component is a recipient agency or a source agency in a matching program with a non-federal agency.

6. Revise §310.6 to read as follows:

§310.6 Responsibilities.

(a) The Director of Administration and Management (DA&M):

(1) Serves as the Senior Agency Official for Privacy (SAOP) for the DoD. These duties, in accordance with OMB Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy" (available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf), include:

(i) Ensuring DoD implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy.

(ii) Overseeing, coordinating, and facilitating DoD privacy compliance efforts.

(iii) Ensuring that DoD personnel and DoD contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing DoD-specific procedures for handling of PII.

(2) Provides rules of conduct and policy for, and coordinates and oversees administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB Circular No. A-130.

(3) Publishes this part and other guidance to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serves as the chair of the Defense Privacy Board and the Defense Data Integrity Board.

(5) As requested, ensures that guidance, assistance, and subject matter expert support are provided to the combatant command privacy officers in the implementation and execution of and compliance with the DoD Privacy Program.

(6) Acts as The Privacy Act Access and Amendment appellate authority for OSD and the Office of the Chairman of the Joint Chiefs of Staff when an individual is denied access to or amendment of records pursuant to The Privacy Act and DoD Directive 5105.53, “Director of Administration and Management (DA&M)” (available at http://www.dtic.mil/whs/directives/corres/pdf/510553p.pdf).

(b) The Director, Defense Privacy and Civil Liberties Office (DPCLO), under the authority, direction, and control of the DA&M:

(1) Ensures that laws, policies, procedures, and systems for protecting individual privacy rights are implemented throughout DoD.

(2) Oversees and provides strategic direction for the DoD Privacy Program.

(3) Assists the DA&M in performing the responsibilities in paragraphs (a)(1) through (a)(6) of this section.

(4) Reviews DoD legislative, regulatory, and other policy proposals that contain information privacy issues relating to how the DoD keeps its PII. These reviews must include any proposed legislation, testimony, and comments having privacy implications in accordance with DoD Directive 5500.01, "Preparing, Processing, and Coordinating Legislation, Executive Orders, Proclamations, Views Letters, and Testimony" (available at http://www.dtic.mil/whs/directives/corres/pdf/550001p.pdf).

(5) Reviews proposed new, altered, and amended systems of records. Submits required SORNs for publication in the Federal Register (FR) and, when required, provides advance notification to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(6) Reviews proposed DoD Component privacy exemption rules. Submits the exemption rules for publication in the FR, and submits reports to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(7) Develops, coordinates, and maintains all DoD computer matching agreements. Submits required match notices for publication in the FR and provides advance notification to OMB and Congress consistent with 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(8) Provides guidance, assistance, and support to the DoD Components in their implementation of the DoD Privacy Program to ensure that:

(i) All requirements developed to maintain PII conform to the DoD Privacy Program standards.

(ii) Appropriate procedures and safeguards are developed and implemented to protect PII when it is collected, used, maintained, or disseminated in any media.

(iii) Specific procedures and safeguards are developed and implemented when PII is collected and maintained for research purposes.

(9) Compiles data in support of the DoD Chief Information Officer (DoD CIO) submission of the Federal Information Security Management Act (FISMA) Privacy Reports, pursuant to OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information" (available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf); the Biennial Matching Activity Report to OMB, in accordance with OMB Circular No. A-130 and this part; the quarterly Section 803 report in accordance with 42 U.S.C. 2000ee and 2000ee-1; and other reports as required.

(10) Reviews and coordinates on DoD Component privacy program implementation rules to ensure they are in compliance with the DoD-level guidance.

(11) Provides operational and administrative support to the Defense Privacy Board and the Defense Data Integrity Board.

(c) The General Counsel of the Department of Defense (GC DoD):

(1) Provides advice and assistance on all legal matters related to the administration of the DoD Privacy Program.

(2) Appoints a designee to serve as a member of the Defense Privacy Board and the Defense Data Integrity Board.

(3) When a DoD Privacy Program group is created, appoints a designee to serve as a member.

(d) The DoD Component heads:

(1) Provide adequate funding and personnel to establish and support an effective DoD Privacy Program.

(2) Establish DoD Component-specific procedures in compliance with this part and publish these procedures as well as rules of conduct in the FR.

(3) Establish and implement appropriate administrative, physical, and technical safeguards and procedures prescribed in this part and other DoD Privacy Program guidance.

(4) Ensure Component compliance with supplemental guidance and procedures in accordance with all applicable federal laws, regulations, policies, and procedures.

(5) Appoint a Component senior official for privacy (CSOP) to support the SAOP in carrying out the SAOP's duties identified in OMB Memorandum M-05-08.

(6) Appoint a Component privacy officer to administer the DoD Privacy Program, on behalf of the CSOP.

(7) Ensure DoD personnel and DoD contractors having primary responsibility for implementing the DoD Privacy Program receive appropriate privacy training. This training must be consistent with the requirements of this part and will address the provisions of 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(8) Ensure that all DoD Component legislative, regulatory, or other policy proposals are evaluated to ensure consistency with the information privacy requirements of this part.

(9) Assess the impact of technology on the privacy of PII and, when feasible, adopt privacy-enhancing technology to:

(i) Preserve and protect PII contained in a DoD Component system of records.

(ii) Audit compliance with the requirements of this part.

(10) Ensure that officials who have specialized knowledge of the DoD Privacy Program periodically review Component implementation of and compliance with the DoD Privacy Program.

(11) Submit reports, consistent with the requirements of this part, in accordance with 5 U.S.C. 552a and OMB Circular No. A-130, and as otherwise directed by the Director, DPCLO.

(e) Secretaries of the Military Departments. In addition to the responsibilities in paragraph (d) of this section, the Secretaries of the Military Departments provide program and financial support to the combatant commands as identified in DoD Directive 5100.03, "Support to the Headquarters of Combatant and Subordinate Unified Commands" (available at http://www.dtic.mil/whs/directives/corres/pdf/510003p.pdf) to fund, without reimbursement, the administrative and logistic support required by combatant and subordinate unified command headquarters to perform their assigned missions effectively.

§310.7 [Removed and Reserved]

7. Section 310.7 is removed and reserved.

8. Section 310.8 is revised to read as follows:

§310.8 Rules of conduct.

In accordance with section (e)(9) of The Privacy Act, this section provides DoD rules of conduct for the development, operation, and maintenance of systems of records. DoD personnel and DoD contractor personnel will:

(a) Take action to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.

(b) Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policy. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties or administrative sanctions.

(c) Report any unauthorized disclosures of PII from a system of records to the applicable Privacy point of contact (POC) for the respective DoD Component.

(d) Report the maintenance of any system of records not authorized by this part to the applicable Privacy POC for the respective DoD Component.

(e) Minimize the collection of PII to that which is relevant and necessary to accomplish a purpose of the DoD.

(f) Not maintain records describing how any individual exercises rights guaranteed by the First Amendment, except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including authorized intelligence or administrative activities.

(g) Safeguard the privacy of all individuals and the confidentiality of all PII.

(h) Limit the availability of records containing PII to DoD personnel and DoD contractors who have a need to know in order to perform their duties.

(i) Prohibit unlawful possession, collection, or disclosure of PII, whether or not it is within a system of records.

(j) Ensure that all DoD personnel and DoD contractors who either have access to a system of records or develop or supervise procedures for handling records in a system of records are aware of their responsibilities and are properly trained to safeguard PII being maintained under the DoD Privacy Program.

(k) Prepare any required new, amended, or altered SORN for a given system of records and submit the SORN through their DoD Component Privacy POC to the Director, DPCLO, for coordination and submission for publication in the Federal Register (FR).

(l) Not maintain any official files on individuals, which are retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, also known as a system of records, without first ensuring that a notice has been published in the FR. Any official who willfully maintains a system of records without meeting the publication requirements as prescribed by this part and The Privacy Act may be subject to criminal penalties or administrative sanctions.

(m) Maintain all records in a mixed system of records as if all the records in such a system are subject to The Privacy Act.

9. Amend §310.9 by revising paragraphs (a) and (b) to read as follows:

§310.9 Privacy boards and office, composition and responsibilities.

(a) The Defense Privacy Board. (1) Membership. The Board consists of:

(i) Voting Members. Representatives designated by the Secretaries of the Military Departments and the following officials or their designees:

(A) The DA&M, who serves as the chair.

(B) The Director, DPCLO.

(C) The Director for Privacy, DPCLO, who serves as the Executive Secretary and as a member.

(D) The Under Secretary of Defense for Personnel and Readiness.

(E) The Assistant Secretary of Defense for Health Affairs.

(F) The DoD CIO.

(G) The Director, Defense Manpower Data Center.

(H) The Director, Executive Services Directorate, Washington Headquarters Services (WHS).

(I) The GC DoD.

(J) The Chief of the National Guard Bureau.

(ii) Non-Voting Members. Non-voting members are the Director, Enterprise Information Technology Services Directorate (EITSD), WHS; and the representatives designated by Defense Agency and DoD Field Activity directors.

(2) Responsibilities. The Board:

(i) Serves as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary to address issues of common concern to ensure that consistent policy is adopted and followed by the DoD Components. The Board issues advisory opinions, as necessary, on the DoD Privacy Program to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(ii) Establishes and convenes committees as necessary.

(iii) Establishes working groups whose membership is composed of DoD Component privacy officers and others as necessary.

(b) The Defense Data Integrity Board. (1) Membership. The Board consists of:

(i) The DA&M, who serves as the chair.

(ii) The Director, DPCLO.

(iii) The Director for Privacy, DPCLO, who serves as the Executive Secretary.

(iv) The representatives designated by the Secretaries of the Military Departments; the DoD CIO; the GC DoD; the Inspector General of the Department of Defense, who is a non-voting advisory member; the Director, EITSD; and the Director, Defense Manpower Data Center.

(2) Responsibilities. The Board:

(i) Oversees and coordinates, consistent with the requirements of 5 U.S.C. 552a, OMB Circular No. A-130, and this part, all computer matching agreements involving personal records contained in systems of records maintained by the DoD Components.

(ii) Reviews and approves all computer matching agreements between the DoD and other federal, state, or local governmental agencies, as well as any memorandums of understanding, when the match is internal to the DoD. This review ensures that, in accordance with 5 U.S.C. 552a, OMB Circular No. A-130, and this part, appropriate procedural and due process requirements are established before engaging in computer matching activities.

* * * * *

10. Amend §310.10 by revising paragraph (a)(1) to read as follows:

§310.10 General.

(a) * * *

(1) Consist of "records" (as defined in §310.4) that are retrieved by the name of an individual or some other personal identifier; and

* * * * *

Dated: August 19, 2013

Aaron Siegel,
Alternate OSD Federal Register Liaison Officer,
Department of Defense.

[FR Doc. 2013-20515 Filed 08/21/2013 at 8:45 am; Publication Date: 08/22/2013]