This document is scheduled to be published in the Federal Register on 01/27/2015 and available online at **http://federalregister.gov/a/2015-01262**, and on **FDsys.gov**

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: Deputy Chief Management Officer, DoD.

ACTION: Final 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.

This rule is part of DoD's retrospective plan, completed in August 2011, under Executive Order 13563, ''Improving Regulation and Regulatory Review.'' DoD's full plan and updates can be accessed at: *http://exchange.regulations.gov/exchange/topic/eo-13563*.

DATES: This rule is effective **[insert date 30 days from date of publication in the Federal Register]**.

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, The Privacy Act of 1974, as amended, which requires the implementation of the Act by Federal agencies.

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.

Public Comments

The Department published a proposed rule on August 22, 2013 (78 FR 52117), with a request for comments. The following comments were received and are addressed below:

COMMENT 1: An argument against the elimination of the term (and position/role) "System Manager". Yes, it is every employee's responsibility to ensure PII is properly handled, but the System Manager is the 'control valve' for each specific SOR and should continue to have a big say in determining 'who' should have access to sensitive material. Much like the world of classified information, being trained and having the 'clearance' to access the information is only part of the equation… the concept of "need-to-know" is equally important when determining access, and the System Manager is the POC that checks "need-to-know". In addition, the System Manager knows (or should know) which SORN authorizes the collection of their SOR, they know with whom the info can be shared, they know what should be in the SOR and they verify

that info every year, they keep track of disclosure accounting, etc. The average user with access only knows to protect it, and they wouldn't know a SORN if they tripped over it. I would suggest returning the “System Manager” to this document.

DoD RESPONSE: This Comment addresses the Rules of Conduct as described under 32 CFR Part 310.8(b)(1)-(3). These particular requirements have been revised and incorporated into 32 CFR Part 310.8(j)-(l), and are now applicable to all DoD personnel and DoD contractor personnel, including system mangers. This revision does not eliminate the position/role of system managers.

COMMENT 2: 32 CFR 310.22. This comment is targeted to a part of 32 CFR Part 310 that DoD saw fit to not update, and it is a missed opportunity to clarify current DoD practices. The DoD has gone out of its way to establish that sharing lists of PII with non-DoD requestors is prohibited by FOIA. The DoD has requested that OPM not share DoD personnel information with requestors, and OPM has approved that request. DoD has gone to court (supporting OPM), and won, in its effort to ensure that requests for personnel information of DoD employees is exempt under the FOIA. (see Long vs. OPM (Case 5:05-cv-01522-NAM-DEP)). And while the DPCLD continues to state that “there is no DoD FOIA policy denying the release of names of DoD personnel below the Director, O-7, or SES levels. All such decisions to deny names that do not comprise a list must be made by using the Reporters Committee balancing test.”, in fact DoD has issued a policy memorandum (09 Nov 2001) stating exactly that.

Sidebarring whether it is "actual" DoD policy to withhold or not, I think it is fair to say that DoD will likely discourage or prevent release of personnel information (either in lists per the Nov 2001 memo or not-in-lists via FOIA exemptions). Therefore the contention expressed in 32 CFR 310.22(b)(5)(i)(A) that “…personal information regarding DoD civilian employees that

normally may be released without a clearly unwarranted invasion of personal privacy" is misleading and disingenuous and should be reworded. As presently constituted, this wording gives the impression that this info is normally released, so either some DoD commands may release it without being aware that DoD, in practice, does exactly the opposite, or some citizens wishing to know how their government works may actually think they have a chance of getting that info from DoD without a court fight.

If the policy memo written just after 9/11 is indeed the new permanent policy and not, as Michael Donley declared, that "it was believed that this would only be a temporary policy", please change the CFR to reflect that. 12 years of relying on a scrap of paper touting a 'temporary policy' and not changing Federal Regulations seems to be circumventing the purpose of the CFR.

DoD RESPONSE: This Comment addresses the release of "personal information that is normally releasable" as described in 32 CFR 310.22(b)(5)(i)(A). The commentator objects to the wording "personally information regarding DoD civilian employees that normally may be released without a clear unwarranted invasion of personal privacy," as "misleading and disingenuous." Attention should be drawn to the use of the word "may," as in indicator that it is permissible to release this information, but not required.

COMMENT 3: 32 CFR 310.4(h). The amendment to the definition of DoD Personnel should also include "dependents of members of armed services registered in DEERS." Military dependents receive no protection under both the current and proposed versions of the Privacy Program. Aside from ongoing military operations, military dependents are just as likely to depend upon DoD services requiring the use of PII and/or PHI, but are afforded no protections.

Currently, family members are only required to receive notice of PII spillage, but are not afforded any civil remedies, nor is their information protected by criminal action against its malicious use. See DoD 5400.11-R, sec. C10.6.1.2.2. The Federal Tort Claims Act (FTCA) also severely limits any torts arising out of PII spillage by parties to whom the Privacy Program applies. See 28 U.S.C. 2680 (h). For military dependents stationed overseas, who are more likely to use federal contractor services and in so doing, place their confidential information in someone else's care, the FTCA might preclude any protections at tort law for military families whatsoever. See 28 U.S.C. 2860 (k).

Protecting DEERS dependent information has the added benefits of enhancing national security, providing accountability for dependents' records, and increasing oversight over DoD dependents' data by government contractors. Protecting dependents' privacy enhances national security by preventing another avenue by which malicious actors can exploit service members. During a service member's deployment, DoD dependents on the homefront frequently contact family readiness groups and other on-base agencies for news on their military members, provide information to DoD agencies to qualify for benefits, and join military unit sponsored clubs to relieve the stress of their loved one's absence. While information on the military member would be protected under the Privacy Program, the DoD dependent's information would not be. Thus, a malicious actor could legally request information about a service member's family and use it to exploit a service member's actions in a forward area, or illegally gain it by hacking information that is currently not required to be protected.

Adding this definition also creates accountability for DEERS dependent records. DoD dependents often become highly involved in on-base activities that require sharing private information. When that DoD dependent changes duty stations with their DoD member, there is

no accounting for the disposition of the records the DEERS member left behind. On-base agencies are often the same from one base to the next. A Privacy Program mandated recordkeeping program would allow for more easier integrations of service members and their families from one duty location to the next, by allowing a standardization of the sharing and safekeeping of records between "franchises" at different bases. This in turn allows service members to more rapidly begin work at a new duty station.

Admittedly, such an amendment possibly triggers an economic impact analysis under E.O. 12866, and an unfunded mandates analysis under the Unfunded Mandates Reform Act, due to the increase in costs in archiving additional data and requiring contractor compliance.

However, the benefit to the welfare of our armed services, the eventual elimination of replication of efforts in data collection at different bases, and the savings to DoD family members' lost time and wages in fighting possible identity theft due to PII spillage, will outweigh the burden of such an amendment.

DoD RESPONSE: This Comment addresses the classification of DoD Personnel in 32 CFR 310.4(h) and suggests the inclusion of "dependents of members of the armed services registered in DEERS" in this classification. Although military dependents do carry many of the same attributes of military service members, they are not DoD employees and therefore cannot be classified as "DoD Personnel." The commentator also suggests that military dependents "are afforded no protections" under the Privacy Program. Information concerning dependents of members of the armed services registered in DEERS is maintained by DoD in accordance with the Privacy Act of 1974, as amended, which does provide protection to military dependents. Within the DoD Privacy Program, "family members" are specifically mentioned in 32 CFR

310.14(a)(1) and 32 CFR 310.50(a)(2)(ii) with respect to breach notification and Privacy Act violations.

COMMENT 4: The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Brennan Center's Liberty and National Security Program works to further national security policies that respect constitutional values and the rule of law while protecting our people. Specifically, the Center seeks to restore the proper flow of information between the government and the people, ensure that domestic counterterrorism policies effectively target the terrorist threat, and secure appropriate mechanisms for oversight and accountability.

The Brennan Center recently published a report, What the Government Does with Americans' Data, that explores the federal government's retention of non-criminal information about Americans. The report recommends specific reforms, including reforms to the Privacy Act and limits on the retention of information reflecting the exercise of rights protected by the First Amendment.

With respect to the DoD proposed regulation, we note that a coalition of organizations is submitting a letter urging the DoD to require the National Security Agency, a component of the DoD, to publish System of Records Notices for three NSA databases: (1) a system containing "telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons," used to distinguish U.S. persons form foreigners in the source of targeting persons for the purpose of surveillance under Section 702 of the Foreign Intelligence Surveillance Act; (2) a database of email address lists and instant messaging "buddy lists" belonging to U.S. citizens and residents; and (3) a database with information about social networks, including data relating to U.S. persons. We endorse this

recommendation, and believe it is critically important that the NSA comply with its obligations to provide the notices required by the Privacy Act regarding searchable databases containing information about Americans and legal residents.

DoD RESPONSE: This Comment addresses System of Records Notices (SORNs) with respect to the DoD, and with the National Security Agency (NSA) in particular. It is DoD policy to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records …" 5 U.S.C. 552a(e)(4). A SORN is required when (1) information about an individual is collected and stored by a DoD Component; and (2) that information is retrievable by a unique personal identifier. 32 CFR 310.10. NSA has twenty-five active SORNS that are publicly available for review. NSA generates SORNs as require by the Privacy Act of 1974 and applicable DoD regulation, 32 CFR 310.10. One NSA SORN, GNSA 18, concerns NSA "collection of operations records." GNSA 18 covers all individuals, as that term is defined within the Privacy Act to encompass citizens of the United States and lawful permanent residents. The purpose of GNSA 18 is to allow NSA to maintain, as that term is defined by the Privacy Act, records on foreign intelligence, counterintelligence, and information systems security matters relating to the missions of NSA. Specifically, GNSA 18 covers all individuals, as that term is defined by the Privacy Act, who are identified in NSA foreign intelligence, counterintelligence, or information system security reports, including supportive materials. As such, the DoD Privacy Program complies with the Privacy Act of 1974, as amended, and as codified at 5 U.S.C. 552a.

COMMENT 5: The Policy section of the DoD's Privacy Program currently states that "No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the constitution...." There are three enumerated exceptions: when retention is

authorized by statute, where the individual has authorized it, or "when the record is pertinent to and within the scope of an authorized law enforcement activity." Under the proposed rule, the analogous section would expand the third exception to allow information relating to First Amendment-protected speech to be maintained when the records is "pertinent to and within the scope of an authorized intelligence or administrative investigation." (This same change is reflected in the proposed changes to the Privacy Program's Rules of Conduct as well.)

This exception – both as it stands and as revised – is simultaneously overly broad and vague. To begin with, it is not clear what matters are encompassed by "law enforcement activities"; it seems likely that those activities could include more than an authorized investigation, but it is unknown what other actions might qualify as an "activity" and thus trigger the ability to maintain First Amendment-protected information. The new terms are even more ambiguous. "Intelligence activities" are not defined, and the meaning of "administrative activities" is particularly uncertain; it appears susceptible to being used as a catch-all to permit the retention of First Amendment-protected information in almost any circumstances.

Furthermore, the requirement that the record be "pertinent to and within the scope of" one of the above matters is an extremely low standard, as nearly any record could be found to be "pertinent to" a particular activity. This is particularly true in light of the assertions by the NSA and the DOJ that databases containing nearly all American's phone records are "relevant" to the NSA's activities because some minute percentage may be germane in the future. A higher standard would be the "relevant and necessary" standard, which is reflected in a proposed change to the Rules of Conduct requiring all users to "minimize the collection of [personally identifiable information] to that which is relevant and necessary to accomplish a purpose of the DoD."

In short, the exception as proposed would allow First Amendment-related information to remain in an individual's file under almost any circumstances, as long as there is a colorable argument that it is related in some way, or might be related in the future, to some law enforcement, intelligence, or "administrative" matter. Because of the ambiguity of these terms, American citizens are left with little guidance about the actual circumstances under which information about their protected speech or associations may be maintained in DoD files.

Accordingly, we urge the DoD to reject the proposed changes and to significantly narrow this exception. Appropriate steps would include: 1) Adding definitions for "law enforcement activities," "intelligence activities," and "administrative activities to 32 CFR 310.4, Definitions; 2) Limiting the retention of information reflecting the exercise of First Amendment-protected rights to circumstances in which it is relevant and necessary to an authorized investigation; 3) Ensuring that at the close of any investigation, First Amendment-protected information is purged. (All information gathered about U.S. persons should be purged if no reasonable suspicion of criminal activity is developed.) If this information must be retained as part of an investigative file that is reasonably maintained in the ordinary course of business, it should be masked to ensure that it is accessible in the future only if strictly relevant and necessary to another authorized investigation; and 4) Specifying the circumstances under which any PII about Americans, including records reflecting First Amendment-protected activities, may be shared with other local, state, or federal agencies, foreign governments, or private parties or entities.
DoD RESPONSE: This Comment addresses the terms "law enforcement activities," "intelligence activities," and "administrative activities," and raises First Amendment concerns. The proposed revision to the DoD policy includes that "no record will be maintained on how an individual exercises rights guaranteed by the First Amendment …, except (1) when expressly

authorized by statute; (2) when expressly authorized by the individual that the record is about; or (3) when the record is pertinent to and within the scope of an authorized law enforcement activity, including an authorized intelligence or administrative investigation." 32 CFR 310.5(f)(proposed). The Privacy Act of 1974 permits "exception from such requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority." Public Law 93-579, Section 2(b)(5). General and Specific Exemptions are provided in 5 U.S.C. 552a(j) and (k). As such, the DoD Privacy Program complies with the Privacy Act of 1974, as amended, and as codified at 5 U.S.C. 552a.

COMMENT 6: By notice published August 22, 2013, the Department of Defense ("DoD") proposes to amend its Privacy Program implementing the Privacy Act of 1974. Specifically, DoD proposes to change its "policies, guidance, and assigned responsibilities of the DoD Privacy Program…; authoriz[e] the Defense Privacy Board and the Defense Data Integrity Board; prescrib[e] uniform procedures for implementation of and compliance with the DoD Privacy Program; and delegat[e] authorities and responsibilities for the effective administrative of the DoD Privacy Program."

The proposed amendments apply to all organizational entities within the DoD, including the Office of the Secretary of Defense, the Military Departments, and the DoD Office of the Inspector General, which the DoD refers to collectively as the "DoD Components." The National Security Agency ("NSA") is an organizational entity and agency component within the DoD. Therefore, the DoD's proposal applies to the NSA.

As discussed below, NSA currently maintains at least three unlawful Privacy Act systems of records pertaining to US citizens and permanent residents. These systems of records violate

both the Privacy Act and current DoD Privacy Program regulations. Accordingly, pursuant to DoD's notice of proposed rulemaking ("NPRM"), the undersigned privacy, consumer rights, and civil rights organizations [hereinafter "Privacy Commentators"] hereby submit these comments to urge DoD to enjoin the NSA—a DoD component subject to the DoD Privacy Program—from violating the Privacy Act and current DoD Privacy Program regulations.

Although the DoD's Privacy Program NPRM is generally favorable to individual privacy and First Amendment rights and adheres to the Privacy Act, the NSA's current collection, maintenance, and disclosure of records violate the Privacy Act and current DoD Privacy Program regulations. The NSA's activity would also violate DoD's proposal.

Because the NSA is under the purview of the DoD Privacy Program, the DoD must ensure NSA implements "information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy" before issuing a final rule. Specifically, the DoD must ensure that the NSA complies with the Privacy Act by publishing additional system of records notices and otherwise adhering to the Privacy Act.

I. The Privacy Act Grants Individuals Judicially Enforceable Rights and Imposes Obligations on Federal Agencies

The Privacy Act of 1974 governs federal agency maintenance, collection, use, and dissemination of U.S. citizen and lawful permanent resident "records" contained in a "system of records." The Act broadly defines "record" to include: any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph[.]

A "system of records" is: a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual [.]

When it enacted the Privacy Act of 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required transparency in agency information practices. Privacy Act legislative history reveals that the Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems data of the Federal Government [.]" The Act is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right to protected by the Constitution of the United States." Congress thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights These rights, for example, guarantee that individuals:

- may request access to records an agency maintains about him or her, as well as have copies made;
- may amend a record about him or her; and
- must be informed whom the agency asks to supply information;

Importantly, the Privacy Act grants individuals a private right of action and individuals may sue federal agencies for violating the Privacy Act.

In addition to granting individual rights, the Privacy Act also imposes several obligations on federal agencies, including obligations that agencies must:

- at least 30 days prior to publication of each record routine, "publish in the Federal Register notice of

any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency";

- not maintain records "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity";
- give individuals access to the accounting of disclosure of their records;
- make notes of requested amendments within the records;
- collect records "about an individual as is relevant and necessary to accomplish
- a purpose of the agency required to be accomplished by statute or by
- executive order of the President";
- "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs";
- assure that all records used by the agency in making determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;
- make a reasonable effort to notify an individual when a record about him or her is made available to another individual when it is a matter of public record;
- promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", institute disclosure procedures for medical and psychological records, create procedures to review amendment requests, as well as determine the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;

In addition to assessing "reasonable attorney fees and other litigation costs" for noncompliant agencies, courts may order agencies to amend individuals records, as well as "enjoin the agency from withholding records." The Act also imposes criminal penalties for officers and agency employees who willfully disclose agency records in violation of the Privacy Act or Privacy Act regulations.

II. NSA Record Maintenance, Collection, Use, and Dissemination are Subject to the Privacy Act and DoD Privacy Program Regulations

The NSA is an "agency" as defined in the Privacy Act. The NSA is also a DoD organizational entity within the DoD. Accordingly, NSA is subject to the Privacy Act, current DoD Privacy Program regulations, and the NPRM. Pursuant to the Privacy Act and DoD Privacy Program regulations, the NSA has published twenty-six systems ofrecords. These are as follows:

IDENTIFIER	NOTICES	EXEMPTIONS CLAIMED
Preamble		
GNSA 02	NSA/CSS Applicants (June	(k)(1) and (k)(5)
GNSA 03	NSA/CSS Correspondence, Cases, Complaints, Visitors,	(k)(1), (k)(2), (k)(4), (k)(5)
GNSA 05	NSA/CSS Equal Employment Opportunity Data Statistical Data	(k)(1), (k)(2), (k)(4)
GNSA 06	NSA/CSS Health, Medical and Safety Files (March 15,	(k)(1), (k)(4), (k)(5), (k)(6)
GNSA 07	NSA/CSS Motor Vehicles and Carpools (July 25,	(k)(1)

GNSA 08	NSA/CSS Payroll Processing File (October 3,	(k)(1) and (k)(2)
GNSA 09	NSA/CSS Personnel File (December 30, 2011, 76 FR	(k)(1), (k)(4), (k)(5), (k)(6)
GNSA 10	NSA/CSS Personnel Security File (June 16,	(k)(1), (k)(2), (k)(5), (k)(6)
GNSA 11	NSA/CSS Key Accountability Records	(k)(2)
GNSA 12	NSA/CSS Education, Training and Workforce	(k)(1), (k)(2), (k)(5), (k)(6)
GNSA 14	NSA/CSS Library Patron File Control System (July	(k)(1) and (k)(4)
GNSA 15	NSA/CSS Computer Users Control System (February	(k)(1) and (k)(2)
GNSA 16	NSA/CSS Drug Testing Program (September 22,	
GNSA 17	NSA/CSS Employee Assistance Service Case	(j)(2), (k)(1), (k)(2), (k)(4), and (k)(5)
GNSA 18	Operations Records (November 30, 2010, 75 FR	(k)(1), (k)(2), and (k)(5)
GNSA 19	NSA/CSS Child Development Services	
GNSA 20	NSA Police Operational Files (April 23, 2010, 75 FR	(k)(2), (k)(4), and (k)(5)
GNSA 21	NSA/CSS Morale, Welfare, and Recreation (MWR) and Non-appropriated Fund	

GNSA 22	Garnishment Processing Files, (October 25, 2010, 75	
GNSA 24	NSA/CSS Pre-Publication Review Records	
GNSA 25	NSA/CSS Travel Records (September 13, 2012, 77 FR	(k)(2), (k)(4)
GNSA 26	NSA/CSS Accounts Receivable, Indebtedness and	(k)(4)
GNSA 27	Information Assurance Scholarship Program	
GNSA 28	Freedom of Information Act, Privacy Act and Mandatory Declassification	(k)(1) through (k)(7)
GNSA 29	NSA/CSS Office of Inspector General Investigations and Complaints	(j)(2),(k)(2), (k)(5)
GNSA 30	Congressional, Executive, and Political Inquiry	

III. NSA's Maintenance, Collection, Use, and Dissemination of Records from Unpublished System of Records Violate the Privacy Act and DoD Privacy Program Regulations

Recent Administration admissions and NSA documents reveal that over the last several years, NSA has maintained at least three unpublished system of records that allow the agency to retrieve information by "identifying number[s], symbol[s], or other identifying particular[s] assigned to . . . individual[s]." These groups of records violate the Privacy Act and DoD Privacy

Program regulations because they were collected without individual consent, public notice, and other Privacy Act procedural requirements.

The first unlawful NSA system of records contains "telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons." The NSA uses these "identifying numbers, symbols, and other particulars" to retrieve information to identify if an individual whom the NSA intends to monitor is a US person.

The second unlawful NSA system of records is comprised of contact lists that the NSA retrieves from email address books and instant message "buddy lists." In this system of records, the NSA gathers email contact lists and instant message buddy lists that traverse global data links. The contact lists and buddy lists include those belonging to US citizens. The lists are maintained within a searchable contact list database that permits the NSA to retrieve information by an "identifying number, symbol, or other identifying particular,"—*i.e.*, email addresses and instant message accounts.

Furthermore, email contact lists, in particular, can contain other identifying information beyond the email address of the contact, such as name, address, business association, and relationship to the contact.

The third unlawful NSA system of records is a database containing information relating to social networks. Within this system of records, the NSA maintains information on social connections (*e.g.* associates or travel companions), location information, email addresses, phone numbers, and publicly available information from commercial entities, as well as location at certain times among other personal information. The NSA retrieves information in this system of records to perform social network analysis. General Keith Alexander confirmed the social

networking analysis, stating that the Supplemental Procedures allow the NSA "to use metadata that [it has] acquired under Executive Order 12-333 and chain, whether it's phone records or emails, it through U.S. selectors to figure out social networks abroad." General Alexander confirmed that the 2009 Supplemental Procedures are still being used.

All three of the aforementioned NSA systems of records violate the Privacy Act and DoD Privacy Program regulations because the NSA has failed to publish system of records notices for each of the system of records. None of the NSA's twenty-six published SORNs listed above describes the type of data collection or dissemination that the NSA is conducting with these systems of records. Moreover, they violate the Privacy Act and DoD Privacy Program regulations because the records were collected without individual notice, consent, or other Privacy Act rights.

Finally, each of the three unpublished systems of records maintains records describing how individuals exercise their First Amendment rights, including press freedoms, and the rights to freely associate and assemble. The Privacy Act forbids agencies from maintaining these types of records "unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." In addition to the aforementioned Privacy Act violations, the NSA has violated and continues to violate the Privacy Act by maintaining records describing how individuals exercise their First Amendment rights.

Conclusion. The NSA is currently in violation of the Privacy Act and DoD Privacy Program regulations. The DoD must ensure that the NSA complies with the Privacy Act by publishing additional system of records notices and otherwise adhering to the Privacy Act before it can adopt its current proposal.

DoD RESPONSE: This Comment addresses System of Records Notices (SORNs) with respect to the DoD, and with the National Security Agency (NSA) in particular. It is DoD policy to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records …" 5 U.S.C. 552a(e)(4). A SORN is required when (1) information about an individual is collected and stored by a DoD Component; and (2) that information is retrievable by a unique personal identifier. 32 CFR 310.10 NSA has twenty-five active SORNS that are publicly available for review. NSA generates SORNs as require by the Privacy Act of 1974 and applicable DoD regulation, 32 CFR 310.10. One NSA SORN, GNSA 18, concerns NSA "collection of operations records." GNSA 18 covers all individuals, as that term is defined within the Privacy Act to encompass citizens of the United States and lawful permanent residents. The purpose of GNSA 18 is to allow NSA to maintain, as that term is defined by the Privacy Act, records on foreign intelligence, counterintelligence, and information systems security matters relating to the missions of NSA. Specifically, GNSA 18 covers all individuals, as that term is defined by the Privacy Act, who are identified in NSA foreign intelligence, counterintelligence, or information system security reports, including supportive materials. As such, the DoD Privacy Program complies with the Privacy Act of 1974, as amended, and as codified at 5 U.S.C. 552a.

Regulatory Procedures

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

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety

effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "substantive non-significant regulatory action."

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

It has been determined 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 determined 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 determined 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 amended 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.

Subpart A—[Amended]

2. Section 310.2 is revised to read as follows:

§310.2 Purpose.

This part:

(a) Updates the established policies 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.

The following definitions apply to this part:

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

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.

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.

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.

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.

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.

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.

DoD personnel. Service members and federal civilian employees.

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.

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).

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).

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

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

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.

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

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

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.

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.

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.[3]

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.

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.

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).

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.

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.

[3] See footnote 1 to §310.1

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

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.

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.

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.

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.

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 individuals' 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, Volume 1 of DoD Manual 8910.01, “DoD Information Collections Manual: Procedures for DoD Internal Information Collections” (available at

http://www.dtic.mil/whs/directives/corres/pdf/891001m_vol1.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 Deputy Chief Management Officer of the Department of Defense (DCMO):

(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, DoD Directive 5105.53, "Director of Administration and Management (DA&M)" (available at http://www.dtic.mil/whs/directives/corres/pdf/510553p.pdf), and Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer."

(b) Under the authority, direction, and control of the DCMO, through the Director for Oversight and Compliance, the Chief, Defense Privacy and Civil Liberties Division (DPCLD):

(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 DCMO in performing the responsibilities in paragraphs (a)(1)-(a)(6) of this section.

(4) Reviews DoD legislative, regulatory, and other policy proposals that contain information on 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 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 semiannual 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 Chief, DPCLD.

(e) In addition to the responsibilities in paragraph (d), 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 and/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 Chief, DPCLD, for coordination and submission for publication in the 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 and/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 to revise 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 DCMO, who serves as the chair.

(B) The Chief, DPCLD, who serves as the Executive Secretary and as a member.

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

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

(E) The DoD CIO.

(F) The Director, Defense Manpower Data Center.

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

(H) The GC DoD.

(I) 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 DCMO, who serves as the chair.

(ii) The Chief, DPCLD, who serves as the Executive Secretary.

(iii) 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.

* * * * * *

Dated: January 21, 2015.

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

[FR Doc. 2015-01262 Filed 01/26/2015 at 8:45 am; Publication Date: 01/27/2015]