COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

AND

CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
CONSUMER FEDERATION OF AMERICA
COUNCIL ON AMERICAN-ISLAMIC RELATIONS
DEMAND PROGRESS
JUSTHEALTH
LIBERTY COALITION
THE NATIONAL WORKRIGHTS INSTITUTE
OPENTHEGOVERNMENT.ORG
PATIENT PRIVACY RIGHTS
PRIVACYACTIVISM
PRIVACY RIGHTS CLEARINGHOUSE
PRIVACY TIMES
VIR-SEC MEDICAL SERVICES

to the

OFFICE OF THE SECRETARY of the DEPARTMENT OF DEFENSE

DoD Privacy Program
32 CFR Part 310
Docket ID: DOD-2013-OS-0023
RIN 0790-AJ03

October 21, 2013

By notice published August 22, 2013, the Department of Defense ("DoD") proposes to amend its Privacy Program implementing the Privacy Act of 1974.[1] 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

[1] DoD Privacy Program Proposed Rule; Amendment, 78 Fed. Reg. 52,117 (proposed Aug. 22, 2013) (hereinafter "NRPM").

of and compliance with the DoD Privacy Program; and delegat[e] authorities and responsibilities for the effective administrative of the DoD Privacy Program."[2]

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."[3] The National Security Agency ("NSA") is an organizational entity and agency component within the DoD.[4] 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

[2] NPRM, 78 Fed. Reg. at 52,117.
[3] *Id*. at 52,118-19.
[4] *Frequently Asked Questions Oversight*, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, http://www.nsa.gov/about/faqs/oversight.shtml (last visited Oct. 21, 2013).

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.[5] 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[.][6]

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 [.][7]

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.[8] 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

[5] DoD NPRM, 78 Fed. Reg. at 52,121.
[6] 5 U.S.C. § 552a(a)(4).
[7] 5 U.S.C. § 552a(a)(5).
[8] S. Rep. No. 93-1183 at 1 (1974).

systems data of the Federal Government [.]"[9] 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."[10] 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.[11] 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;[12]
- may amend a record about him or her;[13] and
- must be informed whom the agency asks to supply information;[14]

Importantly, the Privacy Act grants individuals a private right of action and individuals may sue federal agencies for violating the Privacy Act.[15]

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";[16]

[9] S. Rep. No. 93-1183 at 1.
[10] Pub. L. No. 93-579 (1974).
[11] *Id.*
[12] 5 U.S.C. § 552a(d)(1).
[13] 5 U.S.C. § 552a(d)(2).
[14] 5 U.S.C. § 552a(e)(3).
[15] 5 U.S.C. § 552a(g).
[16] 5 U.S.C. § 552a(e)(11).

- 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";[17]

- give individuals access to the accounting of disclosure of their records;[18]

- make notes of requested amendments within the records;[19]

- 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";[20]

- "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";[21]

- 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;[22]

- 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;[23]

- 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;[24]

In addition to assessing "reasonable attorney fees and other litigation costs" for noncompliant agencies, courts may order agencies to amend individuals records, as well

[17] 5 U.S.C. § 552a(e)(7).
[18] 5 U.S.C. § 552a(c)(3).
[19] 5 U.S.C. § 552a(d)(4).
[20] 5 U.S.C. § 552a(e)(1).
[21] 5 U.S.C. § 552a(e)(2).
[22] 5 U.S.C. § 552a(e)(5).
[23] 5 U.S.C. § 552a(e)(8).
[24] 5 U.S.C. § 552a(f)(1), (2), (3), (4), (5).

as "enjoin the agency from withholding records."[25] 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.[26]

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.[27] The NSA is also a DoD organizational entity within the DoD.[28] Accordingly, NSA is subject to the Privacy Act, current DoD Privacy Program regulations, and the NPRM.[29] Pursuant to the Privacy Act and DoD Privacy Program regulations, the NSA has published twenty-six systems of records.[30] These are as follows:

IDENTIFIER	NOTICES	EXEMPTIONS CLAIMED
Preamble		
GNSA 02	NSA/CSS Applicants (June 5, 2008, 73 FR 31997)	(k)(1) and (k)(5)
GNSA 03	NSA/CSS Correspondence, Cases, Complaints, Visitors, Requests (February 22, 1993, 58 FR 10531)	(k)(1), (k)(2), (k)(4), (k)(5)
GNSA 05	NSA/CSS Equal Employment Opportunity Data Statistical Data (December 30, 2008, 73 FR 79851)	(k)(1), (k)(2), (k)(4)
GNSA 06	NSA/CSS Health, Medical and Safety Files (March 15, 2012, 77 FR 15360)	(k)(1), (k)(4), (k)(5), (k)(6)
GNSA 07	NSA/CSS Motor Vehicles and Carpools (July 25, 2008, 73 FR 43411)	(k)(1)

[25] 5 U.S.C. § 552a(g)(2)(B); 5 U.S.C. § 552a(g)(3)(A).
[26] 5 U.S.C. § 552a(i).
[27] 5 U.S.C. § 552a(a)(1).
[28] *Frequently Asked Questions Oversight*, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, http://www.nsa.gov/about/faqs/oversight.shtml (last visited Oct. 21, 2013).
[29] 32 C.F.R. § 322.1.
[30] *DPCLO—Privacy—System of Records Notices (SORNs)—DoD Component Notices—NSA/CSS*, DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE, http://dpclo.defense.gov/privacy/SORNs/component/nsa/index.html (last visited Oct. 21, 2013).

GNSA 08	NSA/CSS Payroll Processing File (October 3, 2012, 77 FR 60401)	(k)(1) and (k)(2)
GNSA 09	NSA/CSS Personnel File (December 30, 2011, 76 FR 82283)	(k)(1), (k)(4), (k)(5), (k)(6)
GNSA 10	NSA/CSS Personnel Security File (June 16, 2009, 74 FR 28483)	(k)(1), (k)(2), (k)(5), (k)(6)
GNSA 11	NSA/CSS Key Accountability Records (June 28, 2010, 75 FR 36642)	(k)(2)
GNSA 12	NSA/CSS Education, Training and Workforce Development (March 24, 2009, 74 FR 12116)	(k)(1), (k)(2), (k)(5), (k)(6)
GNSA 14	NSA/CSS Library Patron File Control System (July 30, 2013, 78 FR 45913)	(k)(1) and (k)(4)
GNSA 15	NSA/CSS Computer Users Control System (February 5, 2010, 75 FR 6000)	(k)(1) and (k)(2)
GNSA 16	NSA/CSS Drug Testing Program (September 22, 2011, 76 FR 58787)	
GNSA 17	NSA/CSS Employee Assistance Service Case Records (November 14, 2011, 76 FR 70427)	(j)(2), (k)(1), (k)(2), (k)(4), and (k)(5)
GNSA 18	Operations Records (November 30, 2010, 75 FR 74019).	(k)(1), (k)(2), and (k)(5)
GNSA 19	NSA/CSS Child Development Services (December 4, 2009, 74 FR 63732)	
GNSA 20	NSA Police Operational Files (April 23, 2010, 75 FR 21250)	(k)(2), (k)(4), and (k)(5)
GNSA 21	NSA/CSS Morale, Welfare, and Recreation (MWR) and Non-appropriated Fund Instrumentality (NAFI) Files (May 7, 2010, 75 FR 25215)	

GNSA 22	Garnishment Processing Files, (October 25, 2010, 75 FR 65457)	
GNSA 24	NSA/CSS Pre-Publication Review Records (September 15, 2010, 75 FR 56079)	
GNSA 25	NSA/CSS Travel Records (September 13, 2012, 77 FR 56626)	(k)(2), (k)(4)
GNSA 26	NSA/CSS Accounts Receivable, Indebtedness and Claims (August 19, 2009, 74 FR 41872)	(k)(4)
GNSA 27	Information Assurance Scholarship Program (October 5, 2011, 76 FR 61679)	
GNSA 28	Freedom of Information Act, Privacy Act and Mandatory Declassification Review Records (January 19, 2011, 76 FR 3098)	(k)(1) through (k)(7)
GNSA 29	NSA/CSS Office of Inspector General Investigations and Complaints (May 3, 2012, 77 FR 26254)	(j)(2),(k)(2), (k)(5)
GNSA 30	Congressional, Executive, and Political Inquiry Records (September 13, 2012, 77 FR 56628)	

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]."[31] 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."[32] 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.[33]

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." [34] In this system of records, the NSA gathers email contact lists and instant message buddy lists that traverse global data links.[35] The contact lists and buddy lists include those belonging to US citizens.[36] The lists are maintained within a searchable contact list database that permits the NSA to retrieve information by an "identifying number, symbol, or other

[31] 5 U.S.C. § 552a(a)(5).
[32] Eric H. Holder, Jr., Attorney General of the United States, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, 3 (July 28, 2009).
[33] 5 U.S.C. § 552a(a)(5). Eric H. Holder, Jr., Attorney General of the United States, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, 3 (July 28, 2009).
[34] NSA Special Source Operations, *PowerPoint: Content Acquisition Optimization*, slides 3-4; *See also* Barton Gellman and Ashkhan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASHINGTON POST, Oct. 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.
[35] Barton Gellman and Ashkhan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASHINGTON POST, Oct. 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.
[36] *Id.*

identifying particular,"—*i.e.*, email addresses and instant message accounts. [37] 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.[38] The NSA retrieves information in this system of records to perform social network analysis.[39] 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."[40] General Alexander confirmed that the 2009 Supplemental Procedures are still being used.[41]

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

[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Continued Oversight of the Foreign Intelligence Surveillance Act Before the Sen. Judiciary Comm.* (2013) (oral response of Gen. Keith Alexander).
[41] *Id.*

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."[42] 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.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Jeramie Scott
National Security Fellow

Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue NW, Suite 200

[42] 5 U.S.C. § 552a(e)(7).

Washington, D.C. 20009
(tel) 202 – 483 – 1140
(fax) 202 – 483 –1248

Center for Financial Privacy and Human Rights
Consumer Federation of America
Council on American-Islamic Relations
Demand Progress
JustHealth
Liberty Coalition
The National Workrights Institute
OpenTheGovernment.org
Patient Privacy Rights
Privacyactivism
Privacy Rights Clearinghouse
Privacy Times
Vir-Sec Medical Services