United States Department of State

Washington, D.C. 20520

July 7, 2017

The Honorable
Elisebeth B. Collins, Board Member
Privacy and Civil Liberties Oversight Board
MS2 – 2C104
Washington, DC 20511

Dear Ms. Collins:

Pursuant to Section 803(f) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, codified at 42 U.S.C.A. § 2000ee-1, the Department of State hereby submits the attached report, which includes information on reviews, advice, and compliance management across the privacy spectrum for July 1, 2016 through December 31, 2016.

We hope this information is useful to you. Please do not hesitate to contact us if we can be of further assistance on this or any other matter.

Sincerely,

William E. Todd

William Todd
(M) Director General, Acting

Enclosures:
As stated.

Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period July 1, 2016 – December 31, 2016

I. Introduction

In accordance with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. 2000ee-1 (hereinafter "Section 803"), the Department of State ("Department") is herein reporting for the period of July 1, 2016 to December 31, 2016. Section 803 requires periodic reports on the discharge of the functions of the Department's Privacy and Civil Liberties Officer ("PCLO"), including information on: (1) the number and types of reviews undertaken; (2) the type of advice provided and response given to such advice; (3) the number and nature of complaints received by the Department, agency, or element concerned for alleged violations; and (4) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of the PCLO. *See* 42 U.S.C. 2000ee-1(f).

During this review period, the Under Secretary for Management served as the Department's PCLO. The PCLO is the principal advisor to the Secretary of State on the privacy and civil liberties implications of Department policies and regulations. In November 2016, as part of the Office of Management and Budget (OMB) guidance to assess the Senior Agency Official for Privacy (SAOP) appointment and to re-designate as necessary, the Department designated the Deputy Assistant Secretary for Global Information Services to serve as the Department's SAOP. The Deputy Assistant Secretary for the Bureau of Administration, Global Information Services, and the Office of the Legal Adviser share responsibility for advising and supporting the PCLO in the administration of the PCLO's responsibilities to ensure, inter alia, that the Department is appropriately considering privacy and civil liberties in its actions. The SAOP has overall responsibility and accountability for ensuring that privacy protections are integrated into all Department programs, policies, and procedures. Many of the day-to-day privacy compliance activities are handled by the Department's Privacy Office, which reports to the SAOP. The Privacy Office is comprised of full-time program analysts who are responsible for conducting privacy compliance reviews, training Department personnel, assisting with reporting functions, and managing privacy breaches. The Office of the Legal Adviser advises the SAOP, the Privacy Office, and other Department personnel on compliance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a, and other applicable laws and policies, including those pertaining to civil liberties.

II. Privacy Reviews

The Department of State conducts reviews of information technology systems and programs to assess potential privacy risks. The types of reviews conducted during this reporting period include the following:

1. **Privacy Impact Assessments ("PIAs")** are a requirement of Section 208 of the eGovernment Act of 2002. The PIA is used to identify and assess privacy risks throughout the development lifecycle of a system or program.

2. **Systems of Records Notices ("SORNs")** are required by the Privacy Act of 1974. *See* 5 U.S.C. 552a(e)(4). A SORN describes the existence and character of a system of records, including the categories of individuals whose records are in the system; the categories of records; and the routine uses of the records.
3. **Privacy Act Statements ("PASs")** are required by the Privacy Act of 1974. *See* 5 U.S.C. 552a(e)(3). The PAS, which must be on the form used to collect the information or on a separate form that the individual can retain, includes the authority for collecting the information; the principal purpose for which the information is intended to be used; the routine uses of the information; and the effects on the individual, if any, of not providing all or any part of the requested information.
4. **Data Loss Prevention ("DLP")** is a tool used by the Department to assess and mitigate actual or suspected breaches. A breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations in which persons other-than-authorized users or authorized persons for an other-than-authorized purpose, have access or potential access to PII, whether non-cyber or cyber.

A. **During the reporting period, the Department completed 37 PIAs and reviewed 22 additional PIAs which are pending completion. Included below is a summary of key PIAs, which are considered to be significant undertakings for the Department and/or involve substantial collections of PII, for this reporting period. All published PIAs are available on the Privacy Office website, http://www.state.gov/privacy.**

1. **Integrated Logistics Management System (ILMS)** The Office of Logistics Management provides global logistics support for the people and programs of America's diplomacy by supporting domestic customers, government agencies involved in foreign affairs and operations, and their employees and families. The PIA for ILMS was updated March 2016 to reflect the creation and usage of three mobile applications that are intended to further improve worldwide logistics services and integrated support.
2. **myServices** The Bureau of Administration provides support to the Department of State and U.S. embassies and consulates. To better facilitate workflow functionality, the Bureau introduced myServices, an entirely cloud-based enterprise service management system, to allow Department employees, eligible family members, and other government agency employees at overseas posts to request administrative support services.
3. **Integrated Personnel Management System (IPMS)** The Bureau of Human Resources handles recruitment, assignment evaluation, promotion, discipline, career development, and retirement policies and programs for the Department's Foreign and Civil Service employees. HR IPMS has improved the way it shares information with the Transportation Security Administration, to improve enterprise-wide data sharing and data integrity and quality, and to enable personnel to independently manage their personal information through online seamless workflow processes.
4. **RPC-GSS (aka WRAPS)** The Refugee Processing Center-General Support System (RPC-GSS) consists of the RPC computing and network infrastructure for the Worldwide Refugee Admissions Processing System (WRAPS) application and the WRAPSnet.org website. WRAPS is an electronic refugee resettlement case management system that links the Department of State Bureau of Population, Refugees and Migration (PRM) and its worldwide

partners to facilitate the refugee resettlement process. The revised WRAPS PIA indicates that WRAPS and WRAPSnet.org are subsystems of the RPC-GSS system.

B. During the reporting period, the Department completed one SORN and reviewed 10 additional SORNs which are pending completion. Included below is a summary of the published SORN for this reporting period. All published SORNs are available on the Privacy Office website, www.state.gov/privacy.

1. **State-05, Overseas Citizens Services Records and Other Overseas Records** The Department published a notice that proposes to consolidate two existing systems of records, Overseas Citizens Services Records, State-05 and Overseas Records, State-25. The consolidated State-05 includes records covering the adjudication of claims relating to acquisition or loss of U.S. citizenship; the protection and assistance of individuals abroad; arrest cases; assistance to minors, including children who may be victims of abuse, neglect, or who are abandoned or runaways; assistance to individuals involved in child support enforcement proceedings; persons collecting federal benefits overseas; the resolution of property, estate, and benefits claims arising under the pertinent statutes; assistance to individuals involved in international adoption cases and in possible or actual international child custody disputes and/or international parental child abduction cases; and oversight of accredited and approved adoption service providers and the designated accrediting entities of adoption service providers. The revision included modifications and updates to all sections, including a new exemption under (k)(4).

C. During this reporting period, the Department completed the review and approval of 15 PASs. Included below is a list of two key PASs, which are considered to be to have been significant undertakings for the Department and/or involve substantial collections of PII, for this reporting period.

1. **Democracy, Human Rights, and Labor Registration Web Form** The Department of State and the Institute for Human Rights and Business used this form to collect participant information for an event hosted at a Department venue. The Privacy Office made recommendations to ensure that the PAS was properly formatted and included relevant SORN usage, so as to be as accurate as possible.
2. **Affidavit of Relationship (AOR) for Minors Who are Nationals of El Salvador, Guatemala, or Honduras** The AOR provides a means for certain persons in the United States to claim a relationship with a child/children in El Salvador, Guatemala, and Honduras and to assist the Department of State in determining whether that child/those children should be granted access to the U.S. Refugee Admissions Process for family reunification purposes. The Privacy Office worked with the relevant post to review and approve this PAS.

D. During this reporting period, the Department's Data Loss Prevention capacity expanded from only monitoring email to prompting senders when it appears data loss is imminent. Technical faults resulted in inconsistent reporting from some portions of the system, and are being addressed. 14 data loss events have been confirmed, and all events have been remediated.

The Data Loss Prevention (DLP) tool has undergone phased upgrade and expansion efforts. The scope of the DLP deployment was still limited within two pilot sites. Originally only able to observe in instances of data loss in email, portions of the system are now capable of intervening to prevent sensitive data from exiting Department networks. In the course of this upgrade, certain portions of the system have been temporarily unable to report on email transmissions that met the capture criteria. Affected offices are in discussions with the site engineer and software developer to restore data reporting.

The portion of the DLP system with fully functional reporting and intervention indicated that 80.99% of events (7700 events) were either false positives or were not found to be policy violations. 1807 recorded events contained sensitive data. Of those 1807 events, 99.23% of them (1793 events) were cancelled by the user after DLP intervened and prompted the user. Of the user-cancelled events (meaning data loss that was prevented), 29,749 social security numbers, 244 bank account numbers, and 4,679 credit card numbers were protected. The remaining14 events that resulted in data loss have been remediated. Of those remediated events, data loss includes 391 social security numbers and two credit card numbers. DLP also prevented the loss of any bank account numbers. The portion of the system suffering from technical faults was only configured for reporting, not intervention. It appears that this portion of the system experienced 61 events. Review of these events indicated that the majority contained no personally identifiable information (PII). The reason reported events are so much lower on this second portion of the system is because the Department's financial systems operate on the first portion of the system, which has been fully functional during this period.

Of the 1807 events believed to include sensitive data, prompting the user that sensitive data was present stopped 99.2% of those events, protecting 98.9% of the sensitive data that would have otherwise been shared. Due to this incredible success, the Department is presently reviewing the intervention portion of DLP for enterprise-wide usage.

III. Advice, Training, and Awareness

The Privacy Office advised various offices throughout the Department in connection with the privacy reviews described above. This advice is reflected in the final versions of these PIAs, SORNs, and PASs. The Office of the Legal Adviser also advised in connection with PIAs, SORNs, and PASs during the reporting period and its advice is also reflected in these documents. In addition to providing this advice, during the reporting period, the Privacy Office conducted the following privacy training:

Mandatory On-line Training:

1. **3,080** Department personnel completed the distance learning training course, PA459, Protecting Personally Identifiable Information. The course is a one-time mandatory training for all employees who handle PII.

2. **56,790** Department personnel (domestic and overseas) completed the distance learning training course, PS800, Cybersecurity Awareness, which includes a dedicated privacy module. This course is required annually for all personnel who access the Department's network.

Classroom Training (includes ad-hoc instructor-led):
Privacy Awareness Briefings The Privacy Office provided customized privacy awareness briefings to employees and contractors in offices and bureaus throughout the Department. During this reporting period, personnel were trained on the privacy protections that relate to their day-to-day operations and the rules of behavior for safeguarding PII. In addition, the Privacy Office developed a new briefing on privacy compliance and implementation for the Bureau of Diplomatic Security (DS) Cybersecurity Online Learning (COL) Program. These briefings, one of which was recorded, were offered online and attended by personnel both domestic and abroad.

IV. Privacy Complaints

For purposes of this report, a complaint is a written allegation (excluding complaints filed in litigation with the Department) submitted to the PCLO alleging a violation of privacy or civil liberties concerning the handling of personal information by the Department in the administration of Department programs and operations.

The Department has no complaints to report.

V. Summary of Disposition of Complaints, Reviews, and Inquiries Conducted, and Impact of the Activities of Privacy and Civil Liberties Officer

The Department has no additional information to report.

(c) This order is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by a party against the United States, or any of its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any other person.

GEORGE W. BUSH.

§ 2000ee–1. Privacy and civil liberties officers

(a) Designation and functions

The Attorney General, the Secretary of Defense, the Secretary of State, the Secretary of the Treasury, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the head of any other department, agency, or element of the executive branch designated by the Privacy and Civil Liberties Oversight Board under section 2000ee of this title to be appropriate for coverage under this section shall designate not less than 1 senior officer to serve as the principal advisor to—

(1) assist the head of such department, agency, or element and other officials of such department, agency, or element in appropriately considering privacy and civil liberties concerns when such officials are proposing, developing, or implementing laws, regulations, policies, procedures, or guidelines related to efforts to protect the Nation against terrorism;

(2) periodically investigate and review department, agency, or element actions, policies, procedures, guidelines, and related laws and their implementation to ensure that such department, agency, or element is adequately considering privacy and civil liberties in its actions;

(3) ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties; and

(4) in providing advice on proposals to retain or enhance a particular governmental power the officer shall consider whether such department, agency, or element has established—

(A) that the need for the power is balanced with the need to protect privacy and civil liberties;

(B) that there is adequate supervision of the use by such department, agency, or element of the power to ensure protection of privacy and civil liberties; and

(C) that there are adequate guidelines and oversight to properly confine its use.

(b) Exception to designation authority

(1) Privacy officers

In any department, agency, or element referred to in subsection (a) or designated by the Privacy and Civil Liberties Oversight Board, which has a statutorily created privacy officer, such officer shall perform the functions specified in subsection (a) with respect to privacy.

(2) Civil liberties officers

In any department, agency, or element referred to in subsection (a) or designated by the Board, which has a statutorily created civil liberties officer, such officer shall perform the functions specified in subsection (a) with respect to civil liberties.

(c) Supervision and coordination

Each privacy officer or civil liberties officer described in subsection (a) or (b) shall—

(1) report directly to the head of the department, agency, or element concerned; and

(2) coordinate their activities with the Inspector General of such department, agency, or element to avoid duplication of effort.

(d) Agency cooperation

The head of each department, agency, or element shall ensure that each privacy officer and civil liberties officer—

(1) has the information, material, and resources necessary to fulfill the functions of such officer;

(2) is advised of proposed policy changes;

(3) is consulted by decision makers; and

(4) is given access to material and personnel the officer determines to be necessary to carry out the functions of such officer.

(e) Reprisal for making complaint

No action constituting a reprisal, or threat of reprisal, for making a complaint or for disclosing information to a privacy officer or civil liberties officer described in subsection (a) or (b), or to the Privacy and Civil Liberties Oversight Board, that indicates a possible violation of privacy protections or civil liberties in the administration of the programs and operations of the Federal Government relating to efforts to protect the Nation from terrorism shall be taken by any Federal employee in a position to take such action, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

(f) Periodic reports

(1) In general

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents

Each report submitted under paragraph (1) shall include information on the discharge of

each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer.

(g) Informing the public

Each privacy officer and civil liberties officer shall—

(1) make the reports of such officer, including reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and

(2) otherwise inform the public of the activities of such officer, as appropriate and in a manner consistent with the protection of classified information and applicable law.

(h) Savings clause

Nothing in this section shall be construed to limit or otherwise supplant any other authorities or responsibilities provided by law to privacy officers or civil liberties officers.

(Pub. L. 108–458, title I, §1062, Dec. 17, 2004, 118 Stat. 3688; Pub. L. 110–53, title VIII, §803(a), Aug. 3, 2007, 121 Stat. 360; Pub. L. 113–126, title III, §329(b)(4), July 7, 2014, 128 Stat. 1406.)

AMENDMENTS

2014—Subsec. (f)(1). Pub. L. 113–126 substituted "semi-annually" for "quarterly" in introductory provisions.

2007—Pub. L. 110–53 amended section generally. Prior to amendment, text of section read as follows: "It is the sense of Congress that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer."

§ 2000ee–2. Privacy and data protection policies and procedures

(a) Privacy Officer

Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form;

(2) assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program;

(3) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974 [5 U.S.C. 552a];

(4) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(5) conducting a privacy impact assessment of proposed rules of the Department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected;

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 552a of title 5, 11[1] internal controls, and other relevant matters;

(7) ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

(8) training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies; and

(9) ensuring compliance with the Departments[2] established privacy and data protection policies.

(b) Establishing privacy and data protection procedures and policies

(1)[3] In general

Within 12 months of December 8, 2004, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974 [5 U.S.C. 552a], and section 208 of the E-Government Act of 2002.

(c) Recording

Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report.

(d) Inspector General review

The Inspector General of each agency shall periodically conduct a review of the agency's implementation of this section and shall report the results of its review to the Committees on Appropriations of the House of Representatives and the Senate, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs. The report required by this review may be incorporated into a related report to Con-

[1] So in original.

[2] So in original. Probably should be "Department's".

[3] So in original. No par. (2) has been enacted.