UNDER SECRETARY OF STATE

FOR MANAGEMENT

WASHINGTON

AUG 24 2016

Dear Mr. Chairman:

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 January 1, 2016 through June 30, 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,

Patrick F. Kennedy

Enclosure
As stated.

Mr. Chairman
David Medine,
Privacy and Civil Liberties Oversight Board,
2100 K Street, NW,
Washington, DC 20427.

UNDER SECRETARY OF STATE

FOR MANAGEMENT

WASHINGTON

SEC. 6. *Administration.* Consistent with applicable law and subject to the availability of appropriations, the Department of Justice shall provide the funding and administrative support for the Board necessary to implement this order.

SEC. 7. *General Provisions.* (a) This order shall not be construed to impair or otherwise affect the authorities of any department, agency, instrumentality, officer, or employee of the United States under applicable law, including the functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented in a manner consistent with applicable laws and Executive Orders concerning protection of information, including those for the protection of intelligence sources and methods, law enforcement information, and classified national security information, and the Privacy Act of 1974, as amended (5 U.S.C. 552a).

(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 offioer 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 quarterly, 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.)

AMENDMENTS

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

[1] So in original.

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

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

Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period January 1, 2016 – June 30, 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 January 1, 2016 to June 30, 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).

The Under Secretary for Management serves 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. On behalf of the PCLO, the Assistant Secretary for the Bureau of Administration (Senior Agency Official for Privacy, "SAOP") and the Legal Adviser share responsibility for the Department's privacy and civil liberties programs. 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 Division, which reports to the SAOP. The Privacy Division 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 Division, and other Department personnel on compliance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a, other applicable laws and policies, including 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 of 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 31 PIAs and reviewed 28 additional PIAs which are pending completion. Included below is a summary of key PIAs for this reporting period. All published PIAs are available on the Privacy Division website, http://www.state.gov/privacy/

1. **IIP Cloud** The Bureau of International Information Programs (IIP) conducts the State Department's outreach for public diplomacy by partnering with policy experts and missions abroad to advance U.S. foreign policy. The IIP Cloud PIA was updated to provide posts with a modern, mobile-first contact management platform that allows interested individuals to subscribe to receive content from the U.S. government and provide them opportunities to participate in American public diplomacy. The new platform also manages the individuals' preferences such as those who wish to unsubscribe from future communications.
2. **Passport Application Management System (PAMS)** The Department of State Bureau of Consular Affairs' (CA) Passport Application Management System was developed to consolidate all passport applications under one umbrella. This new system allows for efficient management of the passport application process and related issues.
3. **CVENT** To assist its registration and announcement capabilities for Department of State conferences and events, the Department obtained CVENT, an application that stores personal or contact information about individuals applying or invited to, attending, or supporting these events. The system utilizes cloud storage, so the Office of Major Events and Conferences Staff (M/MECS) worked with the Privacy Division to thoroughly analyze potential privacy risks through the publication of a PIA, as well as an updated system of records notice (SORN), State-33, Protocol Records.

B. During the reporting period, the Department completed 5 SORNs and reviewed 8 additional SORNs which are pending completion. Included below is a summary of key SORNs for this reporting period. All published SORNs are available on the Privacy Division website, http://www.state.gov/privacy/

1. **State-21, Legal Case Management Records** The Department published a notice in the *Federal Register* about updates to State-21, Legal Case Management Records SORN. This system of records is used to provide or facilitate the provision of legal advice and opinion to the offices of the

Department of State and to facilitate defense or representation of the Department in litigation and in other legal proceedings. Information may also be used to reply to requests from courts or agencies.

2. **State-81, Office of Foreign Missions Records Final Rule** The Department's Privacy Division published a final rule for the State-81, the Office of Foreign Missions Records SORN, in the *Federal Register*. The Office of Foreign Missions removed its records from State-36 (Security Records) to include them in their own SORN.

C. During this reporting period, the Department completed 29 PASs and reviewed 4 additional PASs which are pending completion. Included below is a list of key PASs for this reporting period.

1. **Foreign Service Family Reserve Corps (FSFRC)** The Bureau of Human Resources created this new program to establish and maintain a registry of Foreign Service personnel's family members who are eligible for hire at overseas posts. This will allow the Department to meet its need to more quickly fill vacancies with a workforce-ready reserve.
2. **Population, Refugees, and Migration (PRM)** The Department's Privacy Division worked with PRM to draft a PAS in support of a World Refugee Day Program where the bureau asked employees to share their refugee stories. The Privacy Division drafted the PAS to ensure that it accurately reflected the collection and was provided at the point of collection.

D. During this reporting period, the Department's Data Loss Prevention (DLP) tool flagged 3,538 events for potential loss or misuse of sensitive PII. Included below is a summary of DLP events for this reporting period.

Of the 3,538 events flagged by DLP and reviewed by the Privacy Division, 57% were the result of an individual sending his or her own PII from his or her Department email account. For these, the Privacy Division provided

guidance on the risk of sending PII out of the Department's network before closing the event report. Another 14% of events were false positives and were, therefore, closed. The majority of these false positives were foreign phone numbers, website template IDs, zip codes with the optional extra four digits, and DUNS IDs (data universal number system IDs to identify businesses).

24% of flagged events were closed upon initial review by the DLP working group, as they related to law enforcement information or assistance requests from the individual him or herself. Of the rest of the events, around 4% were closed after discussing the event with the individual's supervisor, and only 1% were reported to the United States Computer Emergency Readiness Team (US-CERT) as a privacy incident. As an additional note, the major spike in events from the previous reporting period to the current one can be largely explained by the high volume of individuals who sent their own tax information to external email addresses in preparation of filing with the IRS.

III. Training and Awareness

During the reporting period, the Department of State conducted the following privacy training:

Mandatory On-line Training

1. **1,837** Department personnel completed the distance learning training course, PA459-Protecting Personally Identifiable Information. The course is a one-time mandatory course for all employees who handle PII.
2. **59,311** 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 require access to the Department's network.

Classroom Training (includes ad-hoc instructor-led)

Privacy Awareness Briefings The Privacy Division provided customized privacy awareness briefings to employees and contractors in offices and bureaus throughout the Department. During this reporting period, over 900 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 Division developed a subsequent session on privacy compliance for the Bureau of the Comptroller and Global Financial Services (CGFS) which it offered twice during four days of privacy awareness briefings in Charleston, SC.

E-Gov PMO Budget Year 2018 IT Business Case Training The Privacy Division attended and provided training as part of a one-day training session on the Electronic Capital Planning and Investment Control ("eCPIC") system. The goal of eCPIC training is to streamline business case and scoring criteria to illustrate the value of all Department of State information technology ("IT") investments. The Privacy Division briefed on a multitude of privacy compliance obligations system owners face when bringing IT assets online. Approximately 100 IT project managers were in attendance.

Privacy Briefing to A/OPR The Privacy Division provided a briefing on privacy practices at the Department to seven Directors of the Bureau of Administration's Office of Operations (A/OPR) at their staff meeting. The briefing focused on the SAOP's responsibilities, privacy compliance documents, and activities that put PII at risk.

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 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.