Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period January 1, 2017 – June 30, 2017

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).

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. Last year, the Office of Management and Budget (OMB) issued guidance instructing agencies to assess the Senior Agency Official for Privacy (SAOP) appointment and to re-designate as necessary. The Department's assessment resulted in the designation of the Deputy Assistant Secretary for Global Information Services to serve as the Department's SAOP. As the Department's SAOP, the Deputy Assistant Secretary for the Bureau of Administration, Global Information Services, is responsible for the Department's privacy program. 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 34 PIAs and reviewed 13 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 Office website, http://www.state.gov/privacy/

1. **CGFS-GSS** – The Bureau of the Comptroller and Global Financial Services provides a financial management platform that furthers the Department's global foreign affairs mission. The general support system (GSS) that CGFS employs helps achieve that mission by providing a dedicated storage and operating system virtualization infrastructure that hosts major application systems in support of the bureau. The majority of the applications process personally identifiable information (PII). Drafting this PIA underscores the importance of assessing privacy risk at all levels and recognizing the inherent risks of hosting systems containing PII.
2. **DoS – Office 365** – The Bureau of Information Resource Management provides technological support and services across the Department. DOS-O365 is a cloud-

based service solution that provides enterprise business productivity services and software. DOS-O365 will provide users access to the services and software available via Office application integration in the cloud, therefore freeing up critical storage space on Department systems.

3. **DS CAGE** – The Bureau of Diplomatic Security's Consolidated Application Group Environment provides the Department with a software framework for operation of various DS applications. It is responsible for the sending, receiving, storing, and distribution of information internally and externally on behalf of twelve children systems. The information collections for the applications within DS CAGE range from emergency planning purposes to employee tracking and security incident management.
4. **Enterprise Payment Service (EPS)** – The Bureau of Consular Affairs' EPS system provides a standards-based, extensible and reusable payment collection capability for Consular Shared Tables (CST) applications that need to collect fees for services from their consumers. This system facilitates the request of fee-based consular services from individuals across the world. The PIA helps ensure that individuals' information is properly protected while the Department's global mission is being carried out.

B. During the reporting period, the Department completed no SORNs and reviewed 16 SORNs which are pending completion. With the publication of OMB Circular A-108, OMB put forward new requirements for publishing SORNs. To date, the Department has not received approval under this new guidance from OMB for any SORNs. All published SORNs are available on the Privacy Office website, http://www.state.gov/privacy/

C. During this reporting period, the Department completed the review and approval of 11 PASs. Included below are two key PASs for this reporting period.

1. **DS-60, Affidavit Regarding a Change of Name** – The Affidavit Regarding a Change of Name provides a means for certain persons in the United States to apply for a U.S. passport even though the name used by the applicant is substantially different from that shown on the evidence of citizenship. The information collected on the form is used to establish the individual's identity. The Privacy Office worked with the Bureau of Consular Affairs to review and approve this PAS.
2. **Authorization Request for Premium Class Air Travel and Justification Certificate for Using a Noncontract or Indirect Air Carrier** – The Transportation and Travel Management Division (TTM) uses these forms to document, justify and approve use of business/premium air and rail transportation for official Department-

funded travel. The Privacy Office worked with TTM to review and approve a PAS to place on these forms.

D. During this reporting period, the Department's Data Loss Prevention (DLP) tool reported 0 events for potential loss or misuse of sensitive PII. Included below is an explanation of the unusual reporting for this period.

In August 2016, the Symantec Data Loss Prevention (DLP) tool was rebuilt and reinstalled, and all previous event history was lost. Since the system was rebuilt and reinstalled, it has not been functioning properly. Specifically, the DLP has failed to capture data identified by the established criteria for email transmissions when it should not have. While the DLP still captures events, our review of the captured events found that the majority contained no personally identifiable information (PII). No significant information disseminations were captured in the DLP tool during the reporting period. Additionally, there have been a high number of duplicate events, events transmitted to approved recipients, combinations of multiple emails from multiple senders, and other technical glitches. The Privacy Office discussed these issues with the GS engineer and Symantec. Symantec recommended the "End-Point-Prevent" solution and this is currently under review.

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. **1,087** 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. **56,642** 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 a privacy awareness briefing on privacy practices at the Department for over 40 contractors in MED's Medical Informatics Office. The briefing focused on identifying and protecting personally identifiable information (PII) and how to report a suspected or confirmed PII breach.

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.