

Department of State  
Report on Privacy and Civil Liberties Activities  
Section 803 of 9/11 Commission Act of 2007  
Reporting Period July 1, 2017 – December 31, 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, 2017 to December 31, 2017. 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. The Deputy Assistant Secretary for Global Information Services serves as the Department’s Senior Agency Official for Privacy (“SAOP”). 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, under the supervision of 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, or any similar occurrence where (i) a person other than an authorized user accesses or potentially accesses personally identifiable information, or (ii) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. *See* OMB M-17-12.

**A. During the reporting period, the Department completed 21 PIAs and reviewed 3 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-GFMS** – The Bureau of the Comptroller and Global Financial Services (“CGFS”) provides a financial management platform that furthers the Department’s global foreign affairs mission. The global financial management system (“GFMS”) that CGFS employs is a web-based application that helps achieve that mission by providing flexible financial accounting, funds control, management accounting, and financial reporting processes. As GFMS is the primary financial management platform for the Department, it processes sensitive personally identifiable information (PII). Drafting this PIA helps ensure that privacy risk has been assessed at all levels and that employee PII is properly protected.
2. **Skype for Business** – The Bureau of Information Resource Management provides technological support and services across the Department. Skype for Business is part of the cloud-based Microsoft Office O365 suite of products. Skype provides Department users with the ability to communicate with one another via instant messaging, conduct virtual meetings, and collaborate through document sharing.
3. **IIP Cloud** – The Bureau of International Information Programs provides the Department’s worldwide outreach platform for public diplomacy. The IIP Cloud-PD-CRM will provide posts with a modern, mobile-first contact management platform that will help build connections with foreign audiences that further public diplomacy policy goals.

**B. During the reporting period, the Department completed 3 SORNs, summarized below, and reviewed 14 SORNs which are pending completion. All published SORNs are available on the Privacy Office website, <http://www.state.gov/privacy/>**

1. **State-01, Email Archive Management Records** – This SORN covers a Department system that: (i) captures all emails and attachments that interact with a Department email account, and (ii) stores those emails in a secure repository that allows for search, retrieval, and view when necessary..
2. **State-56, Network User Account Records** – This SORN focuses on the Department-wide collection and maintenance of user account administration records.
3. **State-83, Ombudsperson Mechanism Records** – The EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework create a mechanism for companies on both sides of the Atlantic to comply with EU data protection requirements when transferring personal data from the European Union and Switzerland, respectively, to the United States in support of transatlantic commerce. The Frameworks each established an Ombudsperson Mechanism to address appropriate inquiries by individuals relating to U.S. Intelligence Community access to personal data transmitted from the EU or Switzerland to the United States through Privacy Shield and related commercial transfer mechanisms. The information covered by State-83 will be used by the Ombudsperson to ensure that requests are properly investigated and addressed in a timely manner, and that the relevant U.S. laws have been complied with or, if the laws have been violated, that the situation has been remedied.

**C. During this reporting period, the Department completed the review and approval of 25 PASs. Included below are three key PASs for this reporting period.**

1. **2017 Global Entrepreneurship Application** – The Bureau of International Information Programs (IIP) developed a form to register entrepreneurs for participation in the 2017 Global Entrepreneurship Summit (GES). This Summit convened emerging entrepreneurs, investors, and supporters from around the world and was co-hosted by the U.S. and India. The Privacy Office worked with IIP to review and approve a PAS that was included on the form.
2. **DS-11 Web Form, Application for a US Passport** – The DS-11 web form provides a means for U.S. citizens to apply for a U.S. passport online. As the use of technology is ever increasing, this form makes the passport application process accessible to a wider range of individuals. The information collected on the form is used to establish the individual's identity and determine eligibility for a passport. The Privacy Office worked with the Bureau of Consular Affairs to review and approve this PAS.

3. **U.S. National Commission for UNESCO Laura W. Bush Traveling Fellowship** – The Office of Specialized and Technical Agencies (IO/STA) uses this form to administer this privately funded travel grant for college students who propose projects consistent with UNESCO areas of work. The Privacy Office worked with IO/STA to review and approve this PAS.

**D. During this reporting period, the Department’s Data Loss Prevention (DLP) tool reported 0 events for potential loss or misuse of sensitive PII.**

### **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. **1,469** 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. **59,923** 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 series of six privacy awareness briefings on privacy practices at the Department to contractors in the Bureau of Consular Affairs’ Visa Office. The briefings 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.