

Department of State
Report on Privacy Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period January 1, 2020 – June 30, 2020

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, 2020 – June 30, 2020. 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 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:

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 life-cycle of a system or program.

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.

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 a form used to collect 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.

Breach Response Plan (“BRP”) establishes governing policies and procedures for handling breaches of personally identifiable information (PII) at the Department. These policies and procedures are driven by Office of Management and Budget (OMB) directives and based on applicable laws, Presidential Directives, best practices, and lessons learned. The Department’s current BRP was developed in 2018 in accordance with OMB’s Memorandum M-17-12. Lastly, the Department conducts an annual tabletop exercise to test the breach response plan and to help ensure that key stakeholders understand their specific roles.

During the reporting period, the Department completed 14 PIAs and reviewed 35 additional PIAs, which are pending completion. Reviews are designed to ensure the systems possess required privacy controls. The below summary is a representative sample of the PIAs completed/reviewed. All published PIAs are available on the Privacy Office website, <http://www.state.gov/privacy>.

1. **Department of State SharePoint Services - OpenNet (DoSSS-O)**: The Bureau of Information Resource Management (IRM) provides the Department with modern, secure, and resilient information technology and services. DoSSS-O provides an enterprise platform for knowledge sharing, collaboration, and governance of data presentation. DoSSS-O is used as the primary collaboration and document repository vehicle by many Bureaus and Posts throughout the world.
2. **Worldwide Refugee Admissions Processing System (WRAPS)**: The Bureau of Population, Refugees, and Migration (PRM) manages the United States Refugee Admissions Program (USRAP) through WRAPS. WRAPS provides a standardized, globally linked case tracking system to efficiently and effectively process the admission of refugees to the U.S. The system interfaces with governmental and non-governmental stakeholders including U.S. government (USG) vetting partners, U.S. Citizenship and Immigration Services (USCIS), United Nations (UN) organizations and Non-governmental Organizations (NGOs), and provides statistical analysis and reporting required to ensure the program’s success.
3. **Document Imaging System (DIS)**: The Bureau of the Comptroller and Global Financial Services (CGFS) is responsible for the financial management of the Department and seeks to provide an accountable, efficient and transparent financial management platform. DIS converts paper records to digital records and electronically files and stores data collected for CGFS compensation or financial transaction service

activities. This electronic filing enables account managers and technicians to accomplish tasks faster without the need to access paper files from physical storage.

4. **Employee Labor Relation Tracking System (ELRTS)**: The Bureau of Overseas Building Operations (OBO) manages all Department of State buildings and facilities worldwide. This is a substantial responsibility that requires the inter-workings of various offices and personnel so that each post functions in a safe and efficient manner while supporting the individual missions of the post. The Human Resources Employee and Labor Relations Branch within OBO is vital to the achievement of this goal. ELRTS is a valuable tool for the branch in accomplishing its mission as it tracks and manages employee and labor relations cases.

5. **Online Passport Status Services (OPSS)**: One of the primary responsibilities of the Bureau of Consular Affairs (CA) is the screening and issuance of passports and other official documentation to citizens and nationals. In order to facilitate such a vast and vitally important task, multiple IT systems are utilized simultaneously to identify, screen, and ultimately approve and issue a United States Passport. OPSS supports CA's mission requirement to permit U.S. citizens who have applied for a passport, but not yet received it, to utilize the Internet and a standard browser to check the status of the passport application via the travel.state.gov website. The OPSS application provides U.S. citizens with quick and easy 24 hour access to their application status.

During the reporting period, the Department reviewed ten SORNs, which are pending completion. All published SORNs are available on the Privacy Office website, <http://www.state.gov/privacy>.

As the Department strives to comply with E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the Department has seen an increase in the number of both new and existing IT systems which either use or will be migrating to secure cloud storage. This has resulted in an increase in the number of SORNs which must be updated to reflect cloud storage. Although no new or modified Department SORNs have been published in the Federal Register during the reporting period, of the seven SORNs expected to publish early next reporting period, five of those modifications are a result of the Department's migration to cloud storage. The Department expects this trend to continue over the coming years.

During this reporting period, the Department completed the review and approval of 43 PASs and Confidentiality Statements. Included below are five key PASs for this reporting period.

1. **The Office of Western Hemisphere and European Affairs (WHA-EUR), Bureau of Conflict and Stabilization Operations Survey**: The Bureau of Conflict and Stabilization Operations formulates and implements policies and proposals, and provides policy counsel at decision-making levels on conflict prevention, response, and stabilization policies and programs under the overall direction of and in coordination

with the Under Secretary for Civilian Security, Democracy and Human Rights. The information solicited on this survey will be used to inform a major program initiative tracking Chinese influence in the Balkans and analyzing the foreign policy implications.

2. **Division for Counter Threat Finance and Sanctions' (TFS) Web Page:** The Bureau of Economic & Business Affairs (EB) is the Department's lead negotiator of international economic agreements, which shapes the global rules of trade and investment and enables the United States to maintain a high rate of growth while fostering global prosperity, security and opportunity. The information solicited on the TFS web page will be used to facilitate registration for the Sanctions@state.gov mailing list. The collected information may be used to track client participation in events and services offered by the Division for Counter Threat Finance and Sanctions.
3. **DS-3026 - Medical History and Physical Exam Worksheet:** One of the primary roles of the Bureau of Consular Affairs (CA) is the issuance of Visas to travelers and immigrants to the United States. This form documents information pertinent to an applicant's eligibility for a visa or refugee status under the INA's medical grounds of inadmissibility at INA § 212(a)(1) by recording the results of the medical examination required by INA § 221(d), 8 U.S.C. § 1201(d).
4. **DS-86 – Statement of Non-Receipt of a U.S. Passport:** A vital role of the Bureau of Consular Affairs (CA) is the issuance of Passports to citizens of the United States. The Statement of Non-receipt of a U.S. Passport, form DS-86, is used by the U.S. Department of State to collect information for the purpose of issuing a replacement passport to applicants whose passport applications have been approved but who have not received their passport documents in the mail. The Secretary of State is authorized to issue U.S. passports under 22 U.S.C. § 211a et seq, 8 U.S.C. § 1104, and Executive Order 11295 (August 5, 1966).
5. **DS-7789 – Statement of Material Changes:** The Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs, U.S. Department of State, in accordance with the Arms Export Control Act (AECA), 22 U.S.C. 2751 *et seq.*, and the International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120-130, has the principal mission of controlling the export and temporary import of defense articles and services. This mission is primarily accomplished through the review and issuance of export and temporary import authorization requests, maintenance of the U.S. Munitions List, the registration of manufacturers, exporters, and brokers of defense articles and services, and enforcement of ITAR requirements. The collection and storage of various types of data are integral to DDTC's mission and responsibilities. DS-7789 allows for pertinent changes to this required information to be made to keep the information current and accurate which is vital to fulfillment of this mission.

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 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

- **1,227** Department personnel completed the distance learning training course, PA459 “Protecting Personally Identifiable Information.” The course satisfies a one-time mandatory training requirement for all employees.
- **54,401** 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 Department IT networks.

Other Training

Privacy Awareness Briefings: The Privacy Office provides a range of privacy awareness briefings as needed throughout the Department. For example, the Privacy Office trained over 50 employees (both direct-hires and contractors) on how to identify the PII they work with, best practices to safeguard this important PII, and the steps and procedures to handle a breach of PII should one occur.

IV. Privacy Complaints

A complaint is a written allegation, submitted to the PCLO, alleging a violation of privacy or civil liberties occurring as a result of mishandling of personal information by the Department. For purposes of this report, privacy complaints exclude complaints filed in litigation with the Department. 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.