**UNDER SECRETARY OF STATE**

**FOR MANAGEMENT**

**WASHINGTON**

MAR - 9 2021

The Honorable
Adam I. Klein
Chairman
Privacy and Civil Liberties
Oversight Board
800 N. Capitol St. NW, Suite 565
Washington, D.C. 20002

Dear Mr. Klein:

Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, codified at 42 U.S.C. § 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, 2020 through December 31, 2020.

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,

Carol Z. Perez
Under Secretary of State for Management,
Acting

Enclosures:
As stated.

Department of State
Report on Privacy Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period July 1, 2020 – December 31, 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 July 1, 2020 – December 31, 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 led by the Chief Privacy Officer (CPO) and comprises 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, the CPO, 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 included on all forms used to collect information or on a separate form that the individual can retain, describes 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, and updated in 2020, 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 26 PIAs and reviewed 36 additional PIAs, which are pending completion. Reviews are designed to ensure the systems possess required privacy controls. The summaries below are a representative sample of the PIAs completed/reviewed. All published PIAs are available on the Privacy Office website, http://www.state.gov/privacy.**

1. **Diplomatic Security Electronic Records Management System (DS-ERM):** Diplomatic Security (DS) acts as the law enforcement and security arm of the U.S. Department of State. The purpose of DS-ERM is to provide an electronic records management system that will include functionality to support the record life cycle, including: collection, organization, categorization, storage, metadata capture, physical record tracking, retrieval, use and disposition among all DS offices in order to be in compliance with the Office of Management and Budget (OMB) and National Archives and Records Administration (NARA) Transition to Electronic Records Memorandum (M-19-21).

2. **The Office of the Antarctic Advisor in the Office of Ocean and Polar Affairs, Bureau of Oceans, Environment and Science**: The Bureau of Oceans, Environment, and Science (OES) is responsible for formulating and implementing U.S. policy on international issues concerning the ocean, the Arctic, and the Antarctic. U.S. obligations under Article VII(5)(a) of the Antarctic Treaty of 1959, and consistent with Antarctic Treaty Consultative Meeting Recommendation XVIII-1 allows the Department to collect, via form DS-4131, information from all U.S. nationals organizing expeditions to Antarctica. Responses will facilitate a determination of U.S. jurisdiction over the activity and permit timely dissemination of expedition information to Treaty Parties and the Antarctic Treaty Secretariat's public Electronic Information Exchange System.

3. **Diplomatic Security Federal Bureau of Investigations Connectivity (DS-FBIC)**: The Bureau of Diplomatic Security (DS) acts as the law enforcement and security arm of the U.S. Department of State. DS-FBIC contains several biometric software applications to support case investigations activities in support of the Bureau of Diplomatic Security's (DS) various missions. These applications are used by Diplomatic Security to collect Biometric and Identity data, which is then shared with external federal authoritative databases to establish and verify an individual's identity and criminal records in support of vetting and law enforcement efforts.

4. **FSI Cornerstone FSI-Learn (FSICS)**: The Foreign Service Institute is the U.S. Government's foreign affairs training provider. It serves the U.S. Department of State and the entire USG foreign affairs community in its mission to deliver diplomatic training and provide the learning opportunities that U.S. government foreign affairs professionals need in order to excel in today's global arena. FSICS supports FSI's mission by creating a new home for distance learning courses and classroom e-communities at the Department of State. FSiLearn will replace FSI's current platform, LearnCenter. Through FSiLearn, students can access training and materials anytime, anywhere, and on any device.

5. **Visa Request System (VRS)**: The U.S. Department of State leads America's foreign policy through diplomacy, advocacy, and assistance by advancing the interests of the American people, their safety and economic prosperity. Essential to that mission is the need to travel abroad to meet with foreign dignitaries. VRS helps to facilitate this travel by supporting the Bureau of Consular Affairs (CA) in obtaining visas from foreign embassies and/or consulates for official U.S. government travel. VRS generates formal letters to the foreign embassies or consulates requesting the issuance of a diplomatic or government official visa and tracks the visa request letters and visa applications sent to and collected from the respective foreign embassies/consulates.

**During the reporting period, the Department reviewed 14 SORNs and completed four. All published SORNs are available on the Privacy Office website, http://www.state.gov/privacy.**

1. **Secretariat Contact Records, STATE-84:** On August 24, 2020, the *Federal Register* published a new Department SORN titled "State-84, Secretariat Contact Records". Information in Secretariat Contact Records is used to facilitate Department communication (but principally that of the Secretary of State) with domestic and foreign interlocutors.

2. **Rescindment of Identity Management Systems Records, STATE-72:** On August 3, 2020, the *Federal Register* published a rescindment notice covering a Department system of records called "Identity Management Systems Records, State-72". Records from this system were consolidated under the larger Department SORN umbrella of "STATE-36, Security Records" in 2018. Once the consolidation was completed, the defunct STATE-72 SORN was rescinded.

3. **Rescindment of Skills Catalogue Records, STATE-49:** On September 9, 2020, the *Federal Register* published a rescindment notice covering a Department system of records called "Skills Catalogue Records, State-49". Records from this system were consolidated under the larger Department SORN umbrella of "State-50, Family Liaison Office Records" in 2018. Once the consolidation was completed, the defunct STATE-49 SORN was rescinded.

**During this reporting period, the Department completed the review and approval of 31 PASs and Confidentiality Statements. Included below are five key PASs for this reporting period.**

1. **DS-3077 - Request for Entry Into the Children's Passport Issuance Alert Program**: The Bureau of Consular Affairs (CA) Children's Issues Prevention Branch (OCS/CI) educates parents and legal guardians about the dangers of international child abduction and works with them to protect children from this threat. The Children's Passport Issuance Alert Program (CPIAP) allows CA/OCS/CI to notify a parent or court-designated legal guardian before issuing a passport to his/her child and verifies that the child holds a valid passport. The DS-3077 form is the mechanism by which a parent enters the child's name into the program.

2. **Refugee Biographic Data Sheet**: The Refugee Biographic Data Sheet is used by the Office of Refugee Admissions, Bureau of Population, Refugees, and Migration. It describes a refugee applicant's personal characteristics and is needed to initiate refugee resettlement processing, adjudicate the refugee applicant's application for admission to the United States, to run security checks on refugees by intelligence and federal law enforcement agencies, to conduct medical screenings, and to plan international travel before a refugee applicant can be permitted to travel to the United States. In addition, the information is used to match the refugee with a sponsoring voluntary agency for initial reception and placement in the U.S. under the United States Refugee Admissions Program administered by the Bureau of Population, Refugees, and Migration.

3. **DS-4297 - FLO Professional Development Fellowship (PDF) Application Form**: The Family Liaison Office (FLO) evaluates the information collected in the PDF application to determine who will receive a Professional Development Fellowship. The information will be used by FLO and selection committees to award fellowships. Respondents are spouses and partners of direct-hire U.S. government employees from all agencies serving overseas under Chief of Mission authority who want to maintain, enhance and/or develop professional skills while overseas.

4. **DS-5542 – Request for Vital Records**: The Bureau of Consular Affairs (CA) is responsible for the welfare and protection of U.S. citizens abroad and for issuing documentation to citizens and nationals. The DS-5542 form is used to issue certified or authenticated copies of overseas U.S. citizen vital records such as Consular Reports of Birth/Death Abroad, Certificates of Witness to Marriage, and Panama Canal Zone

documents. U.S. persons may also use the form to request correction, amendment, certification, or replacement of a vital record.

5. **DS-7803- [Title in Development]**: The information collected by the Employee Tracker system via form DS-7803 will be used to provide the Office of the Chief Technology Officer, Bureau of Diplomatic Security, with a locator to track employee work schedules, protective details, and Temporary Duty (TDY) assignments. The information furnished will also be used to produce staffing reports and to provide assistance in ascertaining an individual's whereabouts, identifying or verifying a DS agent detained abroad, found injured/deceased, or seeking assistance via irregular channels.

## 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 Online Training

- **42,846** Department personnel completed the updated distance learning training course, PA318 "Protecting Personally Identifiable Information." The course is required training every two years for all OpenNet users (course launched September 24, 2020).

- **662** Department personnel completed the former distance learning training course, PA459 "Protecting Personally Identifiable Information." The course satisfied the former one-time mandatory training requirement for all employees (PA459 was replaced by PA318 on September 24, 2020).

- **57,724** 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 the Privacy and Civil Liberties Officer

The Department has no additional information to report.