UNDER SECRETARY OF STATE

FOR MANAGEMENT

WASHINGTON

March 13, 2020

The Honorable
Adam I. Klein
Chairman
Privacy and Civil Liberties
Oversight Board
800 N. Capitol St. NW, Suite 565
Washington, DC 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, 2019 through December 31, 2019.

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,

William E. Todd for

Brian Bulatao

Enclosures:
As stated.

Department of State
Report on Privacy Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period July 1, 2019 – December 31, 2019

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, 2019 – December 31, 2019. 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:

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.

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 of State. 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 five PIAs and reviewed 23 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. **The Museum System (TMS)** - The Bureau of Overseas Building Operations (OBO) has the unique responsibility of managing all art exhibits that take place at embassies and consulates around the world. This is truly a detail-oriented role that has many moving parts and requires extensive logistics to successfully accomplish. The Museum System (TMS) supports OBOs mission requirements to manage these over 2000 exhibitions. Art in Embassies office utilizes the TMS database to maintain all aspects of collections management. TMS fully integrates exhibitions, shipments, publication and outreach into one comprehensive database and creates customized reports for any need within the curatorial, registrar, or publications departments.

2. **Document Authentication Review Tracking System (CA DARTS)** - Both domestically and at the hundreds of U.S. embassies, consulates and missions around the world, the Department of State is responsible for authenticating documents that will be used by U.S. citizens, commercial organizations, other government agencies, and foreign nationals. CA DARTS supports the Department of State's mission to authenticate documents by providing individuals with an authenticating certificate that verifies the submitted document(s) adheres to international laws governing trade and other areas.

3. **Diplomatic Security Evidence and Property System Classified (DSEPS-C)** – The Bureau of Diplomatic Security (DS) acts as the law enforcement and security arm of the U.S. Department of State. DSEPS-C is a new system used to support DS investigations by recording the details of seized property items (documents, firearms, currency, etc.). Recorded data about case subjects can be in the form of digital

video/audio files. Most of the activities in the system relate to the management of property items, specifically chain of custody and disposition. DSEPS-C supports the Bureau of Diplomatic Security's mission to protect people, property, and information at 275 State Department missions around the globe.

4. **International Exchange Alumni** - The Bureau of Educational and Cultural Affairs' (ECA) mission is to increase mutual understanding between the people of the United States and the people of other countries by means of educational and cultural exchange that assist in the development of peaceful relations. One of the ways ECA works to achieve its mission is by fostering relationships with students and faculty from around the world. International Exchange Alumni is a dynamic and interactive networking website for past and current participants of U.S. government-sponsored exchange programs to build on their exchange experiences, network with fellow alumni, find grants and funding opportunities, and participate in alumni-only competitions. This platform allows ECA to maintain contact with past participants as well as allow users to continue to build upon their beneficial experiences with the Department of State.

During the reporting period, the Department reviewed seven 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 utilize or will be migrating to secure cloud storage. As a result, 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 19 PASs and Confidentiality Statements. Included below are three key PASs for this reporting period.

1. **Direct Line Participant Registration (webform)** – The Bureau of Economics and Business Affairs, Office of Commercial Business Affairs (EB/CBA) runs the Direct Line for American Business program. This program connects U.S. businesses with American Ambassadors and U.S. mission personnel overseas. Typically, Ambassadors or Principal Officers of U.S. missions overseas host Direct Line webinars or conference calls, often including local government officials, to discuss

emerging sectors or new developments. The registration form collects the information necessary for individuals and businesses to participate in the call.

2. **DS-4079 Request for Determination of Possible Loss of United States Nationality** Section 349(a) of the Immigration and Nationality Act (INA), 8 U.S.C. §1481(a), establishes the statutory bases upon which United States nationals may relinquish their U.S. nationality. U.S. nationals may complete the DS-4079 when they wish to document the voluntary admission of a prior potentially expatriating act with intent to lose U.S. nationality.

3. **DS-5504 The Application for a U.S. Passport: Corrections, Name Change Within 1 Year of Passport Issuance, And Limited Passport Holders** - One of the primary roles of the Bureau of Consular Affairs is the issuance of passports to U.S. Citizens. The DS-5504 is the form used by current passport holders who have identified a discrepancy on their existing passport that requires correction. This service is provided, at no cost, for the situations specified on the form itself.

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

- **1,231** 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.

- **56,595** 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 provided a range of privacy awareness briefings throughout the Department. For example, the Privacy Office conducted training sessions with Information System Security Officers (ISSOs) on how to draft an accurate Privacy Impact Assessment (PIA). These sessions, titled "PIA Boot Camp," were provided both on-site and virtually. Additionally, as part of the Department's Capital Planning Guidance Training for IT system designers and

managers, the Privacy Office discussed the importance of privacy compliance requirements in IT system design.

Tabletop Exercise – In accordance with OMB M-17-12, agencies are required to conduct a breach tabletop exercise at least once annually. The SAOP, in coordination with the Privacy Office, hosted the Department's first tabletop exercise during the reporting period. This exercise walked core response group members through the Breach Response Plan and helped ensure that they understand their specific roles in the event of a breach.

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.