Department of State
Report on Privacy Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period July 1, 2021 – December 31, 2021

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, 2021 – December 31, 2021. 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 25 PIAs and reviewed 32 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. **Human Resources Network (HRNet):** HRNet serves as the Bureau of Global Talent Management's (GTM) main web portal. It provides human resources services to the Department of State community and other agency users, including retired or retiring Foreign Service employees. The HRNet web portal infrastructure does not collect PII directly. Instead, it provides or collects information via its child systems. Some of the information is shared to support staffing changes at U.S. missions abroad and to support employee training, payroll, security clearances, employee travel, logistics, and parking processes.

2. **Museum Website for the Diplomatic Reception Rooms (DRR Website):** The DRR Website, a national museum website for the Diplomatic Reception Rooms, offers visitors a rich and immersive experience in the Department, U.S. history and diplomacy. Visitors who express an interest can sign up for updates and educational programs on the site. They can also sign up for tours or donate by accessing links on the website that will redirect them to other sites that process these requests.

3. **Employee Certification and Proof of Vaccination (ECPV Tool):** The Bureau of Medical Services (MED) manages a worldwide healthcare program providing medical services for Department and other U.S. government employees and their families serving abroad at U.S. diplomatic missions. The ECPV tool is used to validate the vaccine status of all Department employees in order to comply with Executive Order

14043 which required that all Federal employees be fully vaccinated for COVID-19 by November 22, 2021.

4. **Consular Affairs Integrated Biometric System (IBS):** The Bureau of Consular Affairs (CA) is responsible for issuing visas to foreign nationals and passports to U.S. citizens and monitoring for potential visa and passport fraud. CA-IBS is an enterprise-level, facial-recognition matching service. The IBS computerized facial recognition has the potential to recognize several photos of the same person in databases, and the ability to add, delete, and search millions of photographic images for the same person prior to the issuance of travel documents. Facial recognition technology is used to facilitate anti-fraud goals of the Department's existing travel document issuance processes.

5. **Consular Affairs Immigrant Visa Overseas (IVO):** The Bureau of Consular Affairs (CA) is responsible for issuing visas to foreign nationals. CA-IVO provides automated support to the adjudication of an immigrant or diversity immigrant visa applications from individuals wishing to come to the United States with the intent to establish permanent residence. IVO provides for the administration of federal law and regulations that govern the issuance or refusal of either visa type and is a case record and maintenance application used at overseas posts to review and complete the visa adjudication.

6. **Public Key Infrastructure (PKI):** The Bureau of Information Resource Management provides the Department with modern, secure, and resilient information technology and services. The Public Key Infrastructure (PKI) system provides services for the generation, production, distribution, control, and accounting of the Department's Public Key certificates. PKI enhances computer security for the Department, gives users the ability to authenticate to the Department network, and provides options at the desktop such as encryption and digital signatures using the certificates installed on the user's smartcard (e.g., PIV badge or SNAP card). PKI issues certificates to Department non-person entities (NPEs) (network devices, authorized laptops, authorized cell phones, etc.) for secure authentication to Department resources.

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

1. **Visa Records, STATE-39:** On November 8, 2021, the *Federal Register* published a modified Department SORN titled "STATE-39, Visa Records". Information in the Visa Records system is used to assist the Bureau of Consular Affairs and consular officers in the Department and abroad in adjudicating visas and Certificates of Identity. It is also used in dealing with problems of a legal, enforcement, technical, or procedural nature that may arise in connection with a U.S. visa or Certificate of Identity.

2. **Rescindment of Overseas Records, STATE-25:** On October 4, 2021, the *Federal Register* published a rescindment notice covering the Department system of records

"Overseas Records, State-25." Records from this system were consolidated under the broader Department SORN "State-05, Overseas Citizens Services Records and Other Overseas Records" in 2018. Once the consolidation was completed, the obsolete STATE-25 SORN was rescinded.

During this reporting period, the Department completed the review and approval of 25 Privacy Act Statements (PAS) and Confidentiality Statements. Included below are eight key PAS for this reporting period.

1. **Tour Site Application:** The Diplomatic Reception Rooms at the Department house a magnificent collection of art and objects that showcase American heritage and support the nation's diplomacy. The purpose for collecting personal information on this form is to notify the Bureau of Diplomatic Security of visitors to Department facilities to schedule tours for the Diplomatic Reception Rooms.

2. **Authorization For Release of Protected Health Information Form:** The Bureau of Medical Services (MED) promotes and safeguards the health and well-being of America's diplomatic community and facilitates the diplomatic efforts of the Department. This authorization allows the Department's Bureau of Medical Services Health Information Management to release an employee's protected health information to a person or organization of the employee's choosing in compliance with federal and state privacy laws. The information solicited on this form is used to provide all written and electronic medical records requested.

3. **Bureau of Conflict and Stabilization Operations Database:** The Bureau of Conflict and Stabilization Operations (CSO) Database is used to store and track information related to overseas travel conducted in support of CSO's mission to anticipate, prevent, and respond to conflict that undermines U.S. national interests. The database includes biographical information for CSO employees that will be used to track individual personnel readiness.

4. **Office of the Chief of Protocol Event Registrant Form:** The Secretary of State's Office of the Chief of Protocol (S/CPR) supports official summits and conferences hosted by S, VPOTUS and POTUS. To support events, S/CPR created the Event Registrant Form to collect registration data from each invited participant.

5. **MyTravelGov:** The Bureau of Consular Affairs (CA) is responsible for numerous consular affairs services for citizens. MyTravelGov is a portal to the online services that CA provides to the public. Individuals can create an account and choose the service that they need, such as online passport renewal. The information collected on the site will allow CA to adequately fulfill requests.

6. **DS-11- Application for a U.S. Passport:** The Bureau of Consular Affairs (CA) is responsible for the issuance of passports to citizens. CA updated the DS-11 to reflect the new policy that provides customers the option of selecting a non-binary "X" as their gender marker in their U.S. passport.

7. **DS-4194 - Request for Authentications Service:** The Request for Authentication Service form is used by individuals, institutions, and government agencies to request authentication services for documents to be used for legal and administrative purposes abroad under the seal of the Department. The Bureau of Consular Affairs (CA) uses the information collected on the form to establish that the documentation submitted is the same as the documentation received and processed by the Office of Authentications, and to issue certificates in accordance with policies outlined in 22 CFR Part 131.

8. **Embassy Addis Ababa, RSO Security Brief Registration Collection on FAN:** The Bureau of African Affairs is focused on the development of U.S. policy concerning the African continent. The purpose of this collection is to support Embassy Addis Ababa's mission by efficiently managing the mandatory security brief registration process for newly arrived U.S. Direct Hires and adult Eligible Family Members.

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 trainings:

Mandatory Online Training

- **20,842** 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).

- **59,873** 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

System of Record Notice (SORN) Training: At the request of the Foreign Service Institute ("FSI"), Privacy Office staff met with FSI to explain the public notice function of SORNs, identify which FSI SORNs need to be updated and for what purpose, and identify potential stakeholders that will be involved in the SORN update process. The virtual meeting provided FSI information about required privacy compliance documentation and related resources.

Privacy Act Statement (PAS) Training: The Privacy Office also provided an in-depth PAS training to 50 Department personnel. The training included a discussion and instruction on the background, creation, and use of PASs and their place within the privacy controls infrastructure. The aim of the training was to clarify the purpose of the PAS as well as its requirements. Attendees represented Department contacts from multiple bureaus and offices.

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.