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, 2021 – June 30, 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.

The 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 19 PIAs and reviewed 45 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. **Secretary's Phone Book 2.0 (SPB):** The Executive Secretariat acts as the nerve center of the Office of the Secretary in the Department of State. The Secretary's Phone Book 2.0 (SPB) is a teleconferencing system with a contact database used by the Executive Secretariat and the Operations Center to maintain contact information for foreign and domestic individuals, as well as some Department employees. The contact database and teleconferencing system are used to facilitate communications for the Secretary and senior Department officials in the course of their duties.

2. **Online Passport Renewal (OPR):** The Bureau of Consular Affairs (CA) is the public face of the Department of State for millions of people around the world and is responsible for the issuance of passports to citizens. OPR modernizes a paper-intensive process and provides the capability for U.S. Citizens to apply for passport book/card renewals online. In addition to helping the Department adjudicate and deliver quicker customer services during surges in passport demands, it also provides enhanced services to the applicant.

3. **Student Training Management System (STMS):** The Foreign Service Institute serves the U.S. Department of State and the entire USG foreign affairs community in delivering diplomatic training and providing the learning opportunities that U.S. government foreign affairs professionals need to excel in today's global arena. STMS is an official personnel record management system used to manage students' course registrations, document successful completions, and produce reports for trending and compliance tracking. Additionally, STMS also provides billing services for the Budget

office, and administrative functions (i.e., transcript request, approval of courses, and billings).

4. **Regional Financial Management System (RFMS):** The Bureau of Comptroller and Global Financial Services (CGFS) provides a financial management platform that helps further the U.S. government and Department of State global foreign affairs mission. RFMS is used to account for and control appropriated resources and to maintain accounting and financial information associated with the normal overseas operations of U.S. government organizations. The information in this system is used to make authorized payments for goods and services to companies or individuals doing business with the Department of State, to make authorized reimbursement payments to an employee, to prepare IRS-1099 forms (Miscellaneous Income tax reports) and to account for individual accounts of debts owed to the Department of State or the U.S. Government.

5. **myServices:** The Bureau of Administration provides support to the Department of State and U.S. embassies and consulates. To better facilitate workflow functionality, myServices provides the end-user a centralized platform to submit service requests and have service providers fulfill those requests via online interface. Information is used to support fulfillment of International Cooperative Administrative Support Services (ICASS) services at post.

6. **Virtual Student Federal Service (VSFS):** The Bureau of Information Resource Management (IRM) provides the Department with modern, secure, and resilient information technology and services. VSFS is an application owned by the Department of State (DoS) and used both by DoS and other Federal agencies. VSFS is used to advertise internship opportunities for U.S. Citizens who are active college students. Students view internship opportunities posted on VSFS and apply via USAJobs.

During the reporting period, the Department reviewed 15 SORNs. 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 nine SORNs expected to publish early next reporting period, four 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 28 PASs and Confidentiality Statements. Included below are five key PASs for this reporting period.

1. **DS-64 – Statement Regarding a Valid Lost or Stolen U.S. Passport Book or Card:** The Bureau of Consular Affairs (CA) is responsible for protecting the integrity of the U.S. passport. It is imperative that CA ensure that no one has more than one valid U.S. passport book and card at any one time. To combat misuse and fraud, the

DS-64 form allows citizens the means to detail why a previously valid passport cannot be presented when applying for a new passport.

2. **DS-7699 – Affidavit of Relationship for Minors and Children from El Salvador, Guatemala, or Honduras:** The Bureau of Population, Refugees, and Migration (PRM) is responsible for coordinating and managing the U.S. Refugee Admissions Program (USRAP). PRM coordinates within the Department, as well as with the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS), in carrying out this responsibility. PRM and USCIS are preparing to restart an expanded "in-country" program known as the Central American Minors program to provide a means for certain persons in the United States to claim a relationship with children in Honduras, El Salvador, and Guatemala and to assist the Department in determining whether those children are qualified to seek access to the USRAP for family reunification purposes. The main purpose of the DS-7699 is for the qualifying individuals to provide biographical information about children overseas who may subsequently seek access to the USRAP for verification by the U.S. government.

3. **2021 KidVid Submission Form:** The Overseas Briefing Center at the Foreign Service Institute hosts an annual KidVid Contest (now in its 25th year) in which families from the Foreign Service community voluntarily submit videos to illustrate the lives of Foreign Service children overseas. This is an internal contest, only open to direct-hire employees posted abroad under Chief of Mission authority. Each year the winning videos are posted on the OpenNet site of the Overseas Briefing Center for internal viewing by Foreign Service bidders. The information collected through the submission form will serve for the administration of the KidVid Contest, which requires contact information from Foreign Service members.

4. **DS-1998E - Foreign Service Officer Test:** The Foreign Service Officer Test Registration Form is the form used by all individuals who wish to register for the Foreign Service Officer Test. Individuals registering for the Foreign Service Officer Test are required to provide information that will be used to determine their eligibility to take the Foreign Service Officer Test, to register for the test, to assess qualifications for selection as a Foreign Service Officer, and to ensure the integrity of the examination process. this data may be used to prepare statistical reports and analyses at the Department of State, including to improve future tests and conduct research studies based on the test results.

5. **International Career Advancement Program (ICAP) Application:** The International Career Advancement Program (ICAP) is a professional leadership development program for mid-career professionals in international affairs in the United States. ICAP aids professionals from underrepresented groups and those who are strong advocates of diversity and inclusion to pursue leadership positions in international affairs in the United States and abroad. Using the developed application, and other required documentation, the Bureau of Global Talent Management will select candidates to participate in the program. Those who apply for the program aim to enhance the quality and effectiveness of U.S. participation in global affairs.

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

o   **50,757** Department personnel completed the updated distance learning training course, PA318: Protecting Personally Identifiable Information, between January 1, 2021 and June 30, 2021. The course is required training every two years for all OpenNet users (course launched September 24, 2020).

o   **57,607** Department personnel completed the distance learning training course, PS800: Cybersecurity Awareness, between January 1, 2021 and June 30, 2021. This course includes a dedicated privacy module, and it 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, as part of the FSI Tech Talk series the Privacy Office hosted a session titled "Privacy 102". The session was designed to provide an overview of the foundations of federal privacy policy and the Privacy Office's role in implementing the Federal Risk Management Framework. With over 120 employees in attendance, the session covered creating a culture of privacy awareness, privacy compliance, best practices, and the requirements for responding to a known or suspected breach. This session served as role-based training for IT professionals at the Department.

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.