Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period January 1, 2018 – June 30, 2018

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, 2018 – June 30, 2018. 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 the form used to collect the 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 first BRP was originally developed 10 years ago and was recently revised in accordance with OMB's Memorandum M-17-12. Most notably, this BRP includes an updated Breach Incident Form, updated procedures for major versus non-major breaches, post-breach evaluations to help identify lessons learned (such as tasks that could have been conducted more effectively and/or efficiently) and to help make improvements as appropriate. Lastly, the Department will also periodically, but not less than annually, conduct a tabletop exercise to test the breach response plan and to help ensure that key members understand their specific roles.

During the reporting period, the Department completed 24 PIAs and reviewed 24 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. **IRM – FAN** – The Bureau of Information Resource Management provides the information technology and services the Department needs to successfully carry out its foreign policy mission. The Foreign Affairs Network (FAN) is a portfolio of secure, cloud-based services that enable Department of State personnel to securely collaborate and share information with other federal government agency personnel, including contracting personnel, in support of the Department of State's mission.

2. **Passport Application Management System (PAMS)** – PAMS is a group of systems that the Bureau of Consular Affairs (CA) uses in connection with passport applications. The systems covered by the PAMS PIA include the Management Information System, Passport Data Information Transfer System, Passport Information Electronic Records System, Passport Lookout Tracking System, and

User Manager Web Security. These systems allow for the verification and validation of PII submitted on passport applications, facilitate interagency cooperation in validating and authorizing movement over U.S. borders, provide streamlined views of application data and adjudication decisions, and facilitate fraud detection. As PAMS is the Department's primary passport application management platform, it processes a vast amount of PII. This PIA helps ensure that privacy risk has been assessed at all levels and that individuals' data is properly protected.

3. **DS - PEGASYS –** The Bureau of Diplomatic Security (DS) acts as the law enforcement and security arm of the U.S. Department of State. Post Emergency Guidance and Authoring System (PEGASYS) is a new, web-based system implemented to support the creation and management of Emergency Action Plans (EAPs) at posts abroad. PEGASYS retains post-specific information on how to plan for and respond to a crisis. PEGASYS supports the Bureau of Diplomatic Security's mission to protect people, property, and information at 275 Department of State missions around the globe

During the reporting period, the Department published 4 SORNs, summarized below, and reviewed 14 SORNs which are pending completion. All published SORNs are available on the Privacy Office website, http://www.state.gov/privacy/

1. **State-40, Employee Contact Records** –Information covered by State-40 is used: (1) to develop the official locator directories for all personnel; (2) to communicate with certain individuals in the event of an emergency in which designated contact information will be used; (3) to communicate with designated emergency contacts or next of kin; (4) for mail forwarding purposes of the employee; and (5) to answer official inquiries. The Department published updates to State-40 to reflect the consolidation of records previously covered by State-12, the Foreign Service Employee Locator/Notification Records system, into a single modified State-40. The updates also included changes to reflect the move to cloud storage and new emergency notification procedures.

2. **State-36, Security Records** - State-36 captures data related to incidents and threats affecting U.S. Government personnel, information, and facilities for a variety of legal purposes including federal and state law enforcement, counterterrorism purposes, and administrative security functions. The Department published updates to reflect the consolidation of records previously covered by State-72, Identity Management System Records, into a modified State-36. The updates also included changes to reflect the move to cloud storage and new routine uses.

3. **State-39, Visa Records** – State-39 covers information used to adjudicate U.S. visas. Recent updates included amendments to the categories of individuals covered by the system, the categories of records covered by the system, and the routine uses section.

4. **State-21, Legal Case Management Records** – Information in State-21 is used to provide or facilitate the provision of legal advice and opinion to the offices of the Department of State and to facilitate defense or representation of the Department in litigation and in other legal proceedings. Information may also be used to reply to requests from federal, state, local, or international courts, agencies, commissions, organizations, or mechanisms. The Department published updates to State-21, including new routine uses.

During this reporting period, the Department completed the review and approval of 21 PASs. Included below are three key PASs for this reporting period.

1. **DS-64, Statement Regarding a Lost or Stolen US Passport Book and/or Card** – The DS-64 form provides a means for U.S. citizens to report a lost or stolen passport. The information collected on the form is used to ensure that an individual does not have more than one valid U.S. passport book and one valid U.S. passport card at any one time, except as authorized by the U.S. Department of State, in an effort to combat passport fraud and misuse. The Privacy Office worked with CA to review and approve this PAS.

2. **DS-3064, Foreign Service Emergency Locator Information** – This form is used to collect family and emergency contact information for Foreign Service employees. While working to incorporate this form into the Department's "MyData" system, the office that owns the form determined that the truncated SSN that was originally collected in the form was no longer necessary. Accordingly, the SSN field was removed from the updated version.

3. **Advanced Notification Form – Tourist and Other Nongovernmental Activities in the Antarctic Treaty Area –** The Department of State uses this form to solicit information used to determine whether an intended tourist or non-governmental activity is organized in or proceeding from a U.S. territory. These activities must comply with Environmental Protection Agency (EPA) regulations, under the Treaty's Protocol on Environmental Protection. The Department works in conjunction with the EPA to ensure that they do. The Privacy Office reviewed this PAS and made recommendations to ensure that the PAS included the required information and was properly formatted.

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, SORNs, 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

- **1,295** Department personnel completed the distance learning training course, PA459, Protecting Personally Identifiable Information. The course is a one-time mandatory training for all employees who handle PII.

- **56,951** 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 the Department's network.

Other Training

- **Privacy Awareness Briefings** - The Privacy Office provided a range of privacy awareness briefings throughout the Department. Most notably, privacy awareness training was provided for over 1,000 contractors in the Bureau of Administration who would have otherwise been unable to receive such training; the Department's online PA459 training is not currently available to contractors. The contractor training session was recorded and made available on an internal Department website to enable contractors who were unable to attend the in-person session to view the training. Having the session recorded ensured that the Privacy Office would be able to reach all 1,087 contractors within the Bureau of Administration.

IV. Privacy Complaints

For purposes of this report, a complaint is a written allegation (excluding complaints filed in litigation with the Department) submitted to the PCLO alleging a violation of privacy or civil liberties concerning the handling of personal information by the Department in the administration of Department programs and operations.

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.