

Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period January 1, 2019 – June 30, 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 January 1, 2019 – June 30, 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 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 current BRP was developed in 2018 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 is conducting 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 14 PIAs and reviewed 28 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. **INR/AO FAN** – The Bureau of Intelligence and Research’s Office of Analytic Outreach (INR/AO) organizes and funds analytic exchanges with outside experts to inform the thinking of U.S. Government policymakers and intelligence analysts. By using the Foreign Affairs Network (FAN), INR/AO can collaborate with contractors working outside of the Department to identify and assess potential participants in INR-sponsored analytic exchanges. The INR/AO FAN-Use PIA was the pilot for a new process of engagement with enterprise cloud services. The aim of the ‘use template’ is to make it clear and easy for FAN users to report and get approval to process PII on FAN.
2. **Passport Information Electronic Records System (PIERS)** – One of the primary responsibilities of the Bureau of Consular Affairs is the issuance of passports and other documents to citizens and nationals. The passport screening and issuance process requires the collection, authentication and review of various documents. The Passport Information Electronic Records System (PIERS) is a web based application that manages all of the various passport records including Consular Reports of Birth Abroad (CRBAs), Certificates of Witness to Marriage (CWM), Records of Death (ROD), Advance Finder (AF) and Diplomatic and Official Tracking System (DOTS) records, and Panama Canal Zone (PCZ) records data. PIERS provides structured query capabilities to the data maintained within its environment.

3. **The Office of Foreign Missions Information System (TOMIS)** – The Office of Foreign Missions (OFM) and the Office of the Chief of Protocol (S/CPR) both use TOMIS to electronically process foreign mission notifications and requests for services and to manage a wide range of benefits and services for the foreign diplomatic community. S/CPR uses TOMIS to accredit and manage information for Foreign Missions and Personnel that work for the Department of State. Once S/CPR accredits a foreign national in TOMIS, OFM uses the system to manage a range of benefits and services including the issuance of vehicle titles, registrations, driver licenses, and license plates; processing tax exemption and duty-free customs requests; and facilitating property acquisitions within local zoning law restrictions.
4. **ServiceNow** – The Bureau of Information Resource Management (IRM) provides the Department with modern, secure, and resilient information technology and services. ServiceNow is an enterprise-wide cloud-based service (SaaS) offered by IRM to facilitate and enhance collaboration, process management, and approvals of documents, forms, or requested services. ServiceNow offers a variety of suites and modules that offices, bureaus, and posts may use to meet mission goals and manage information workflows.

During the reporting period, the Department published one Notice of Proposed Rule Making (NPRM) summarized below; and reviewed eight SORNs, which are pending completion. All published SORNs are available on the Privacy Office website, <http://www.state.gov/privacy/>

1. **Notice of Proposed Rule-Making for State-01, Email Archive Management Records** – The records covered by the SORN State-01 include emails and attachments to those emails. The Email Archive Management Records system allows for search, retrieval, and view of emails. The Department intends to amend 22 C.F.R. 171.26 to exempt portions of the Email Archive Management Records system of records from certain provisions of the Privacy Act. The Email Archive Management Records can include all email messages and attachments in a specific employee’s inbox. Any exemptions that the Department has claimed in connection with other systems of records could apply to records in the Email Archive Management Records, because similar records could be included in or attached to emails that were sent or received by a Department employee.

During this reporting period, the Department completed the review and approval of 12 PASs and Confidentiality Statements. Included below are three key PASs for this reporting period.

1. **DS-5525 Statement of Exigent/Special Family Circumstances for Issuance of a U.S. Passport to a Child Under Age 16** – In accordance with Public Law 106-113, Section 236 this form assists the U.S. Department of State in administering the regulations in 22 C.F.R. 51.28 requiring that both parents and/or any guardians’ consent to the issuance of a passport to a minor under age 16. This form is used when the written consent of the non-applying parent or guardian cannot be obtained. The

form details the non-applying parent or guardian's unavailability, and recent efforts made to contact the non-applying parent/guardian. The Privacy Office worked with the Bureau of Consular Affairs to review and renew approval of the Privacy Act Statement included in the instructions of the DS-5525 form.

2. **DS-4282 Discrimination Complaint Form** – The Department is obligated to provide a standardized way for employees and members of the public to bring complaints of discrimination under Sections 504 and 508, and Title VI, to the attention of Department human resource officials. The Privacy Office worked with the Office of Civil Rights (S/OCR) to review and renew approval of the Privacy Act Statement included in the instructions of the DS-4282 form.
3. **DS-82 US Passport Renewal Application for Eligible Individuals** – One of the primary roles of the Bureau of Consular Affairs is to adjudicate U.S. passport applications. To facilitate this function, eligible citizens and non-citizen nationals of the United States use form DS-82 to renew their current or recently expired passport. The Privacy Office worked with the Bureau of Consular Affairs to review and renew approval of the Privacy Act Statement included in the instructions of the DS-82 form.

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

- **1,108** 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 who handle PII.
- **59,538** 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 FY 2021 IT Business Case Training for IT system designers and

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

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 mis-handling 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.