**Department of State**
**Report on Privacy Activities**
**Section 803 of 9/11 Commission Act of 2007**
**Reporting Period January 1, 2022 – June 30, 2022**

## 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, 2022 – June 30, 2022. 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 is 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 is 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, notices, forms, and breach response procedures. The types of reviews conducted during this reporting period include the following:

- **Privacy Impact Assessments (PIAs)** are required by Section 208 of the eGovernment Act of 2002. The PIA identifies and assesses privacy risks throughout the lifecycle of a system or collection.
- **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 is included on all forms used to collect information or on a separate form that the individual can retain. It 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 first BRP was developed in 2018, and subsequently updated in 2020. The 2020 version is currently undergoing another revision in accordance with OMB's Memorandum M-17-12. Lastly, the Department conducts an annual tabletop exercise to test the breach response plan and help ensure that key stakeholders understand their specific roles.

**During the reporting period, the Department completed 39 PIAs and reviewed 16 additional PIAs, which were pending completion. Reviews are designed to ensure the systems possess required privacy controls. The summaries below are a representative sample of the PIAs completed. All published PIAs are available on the Privacy Office website, http://www.state.gov/privacy.**

- **Integrated Personnel Management System (IPMS):** The Bureau of Human Resources Integrated Personnel Management System (IPMS) is the underlying technical architecture for all OpenNet applications managed by the GTM Executive Office (GTM/EX). It is comprised of five major components: Global Employment Management System (GEMS), HROnline, Overseas Personnel System (OPS), Executive Agency Personnel Support (EAPS), and the HR Knowledge Center (KC) that together reduce transaction processing overhead, enhance enterprise-wide data sharing, improve data integrity and quality, and empower employees and supervisors with the ability to independently manage their personal information through seamless online workflow processes.

- **Salesforce Enterprise (SF-DOS):** The Bureau of Global Public Affairs (GPA) manages the Salesforce platform both for its own offices and for other bureaus and offices in the Department, which offers a shared service model resulting in greater efficiency than if each organization managed its own separate Salesforce instance. The Department of State uses Salesforce GovCloud Plus, known within the Department as Salesforce Enterprise, to serve as its centralized contact management database. Salesforce Enterprise enables Department staff to engage with members of the public domestically and abroad and maintain a robust history of those relationships. It provides the core contact relationship management module (CRM) and interrelated applications that capture personally identifiable information through contact records and a webform.

- **Windows Time and Attendance System (WINT&A):** The Bureau of Comptroller and Global Financial Services (CGFS) provides a financial management platform for domestic

and overseas employees. WinT&A is a major component of the Department of State (Department) payroll system because it provides those employees time and attendance (T&A) reporting at each post for payroll generation and leave accounting. This system ensures the disbursement of the payroll to the appropriate individual.

- **MyGrants**: The Bureau of Administration (A) provides world-class administrative services in support of America's global foreign affairs. The MyGrants System is a centralized and integrated solution for federal assistance issued by domestic bureaus and allows Bureaus to carry out specified grants work by assisting in the issuance and monitoring of federal assistance to the award recipients. The information collected and maintained in this system is necessary to support the end-to-end federal assistance planning, pre-award, award, post-award, and closeout processes for the Department, alongside Integrated Logistics Management System (ILMS).

**During the reporting period, the Department reviewed 14 SORNs and completed 3. Included below are two key SORNs for this reporting period. All published SORNs are available on the Privacy Office website, http://www.state.gov/privacy.**

- **Integrated Logistics Management Records, STATE-70:** On January 25, 2022, the *Federal Register* published a modified Department SORN titled "Integrated Logistics Management Records, STATE-70". The information contained in this SORN is collected and maintained by the Office of Logistics Management, Office of Program Management and Policy (A/LM/PMP) in the administration of its responsibility for providing worldwide logistics services and integrated support.

- **Risk Analysis and Management Records, STATE-78:** On March 23, 2022, the Federal Register published a modified Department SORN titled, "Risk Analysis and Management Records, STATE-78". Information in the system supports the vetting of directors, officers, or other employees of organizations who apply for Department of State contracts, grants, cooperative agreements, or other funding; and individuals who may benefit from such funding. The information collected from these organizations and individuals is specifically used to conduct screening to ensure that Department funds are not used to provide support to entities or individuals deemed to be a risk to U.S. national security interests.

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

- **ASET Global Virtual TechSprint 2022 Registration Form:** The form is used to track the demographics of the Bureau of International Narcotics and Law Enforcement Affairs' ASET Global Virtual TechSprint 2022 event participants. The form is used to confirm identity as well as balance and diversify teams.

- **Access Records Form:** In compliance with OMB Memorandum "Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act" (M-21-04), the Information Programs and Services Office (A/GIS/IPS) created a Privacy Act Statement to be published on the FOIA website for Access Records.

- **MED Feedback Tool Form:** The information solicited on this form is used to survey Department of State employees on the services they receive at their respective posts' Health Unit or MED's Exam clinics in order to improve their service delivery.

## 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

- **13,973** Department personnel (domestic and overseas) completed the updated distance learning training course, PA318 "Protecting Personally Identifiable Information." The course is required training every two years for all OpenNet users

- **59,927** 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 Office's Data Privacy Day Webinar**: The Privacy Office hosted a webinar on Data Privacy Day, which focused on the Privacy Office as a resource, how the office assists the workforce, why privacy matters, and the future of privacy. The virtual webinar educated the workforce on what the Privacy Office does to protect privacy and encouraged the Department's workforce to further engage with the Privacy Office.
- **Privacy Office Advises the Bureau of Medical Services on Email Labeling and Encryption of Personally Identifiable Information (PII):** At the request of the Bureau of Medical Services (MED), Privacy Office staff met with MED to provide direction regarding the appropriate sensitivity label markings for medical information and tools for encrypting PII. The virtual meeting provided best practices for safeguarding PII.

## 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 the 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.