Department of State
Report on Privacy Activities
Section 803(f) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, codified at 42 USC 2000ee
Reporting Period January 1, 2024 – December 31, 2024

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 (the "Department") is herein reporting for the period of January 1, 2024 – December 31, 2024. Section 803 mandates periodic reports on the activities 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, responsible for advising the Secretary of State on privacy and civil liberties implications of Department policies and regulations. The Deputy Assistant Secretary for Shared Knowledge Services is the Department's Senior Agency Official for Privacy ("SAOP"), responsible for integrating privacy protections 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 incidents and 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.

II. Privacy Reviews

The Department conducts reviews of information technology systems, privacy 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. PIAs identify and assess 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. The creation of a new SORN or modification or recission of an existing SORN must be published in the Federal Register.

- **Privacy Act Statements ("PASs")** are required by the Privacy Act of 1974 when information about individuals is collected and will be stored in a system of records. *See* 5 U.S.C. § 552a(e)(3). A PAS is included on all forms that collect personal information directly from an individual 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.

- The Department's **Breach Response Plan ("BRP")** establishes 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. The BRP was last updated **November 2024** during this reporting period. The Department also conducts an annual tabletop exercise to test the breach response plan and help ensure that key stakeholders understand their specific roles. The most recent tabletop exercise was held in September 2024.

During the reporting period, the Department completed 83 PIAs. PIA reviews are designed to ensure that systems possess required privacy controls. The bullet point below provides a summary of one PIA completed during the reporting period, as an example of the types of systems covered by Department PIAs. All published PIAs are available on the Privacy Office website, https://www.state.gov/privacy-impact-assessments-privacy-office/.

- **Center for Analytics Palantir Federal Cloud Services (CfA PFCS)**: Palantir Technologies created the Center for Analytics (CfA) Palantir Federal Cloud Service (PFCS) system which enables customers to integrate, manage, and secure enterprise data, forming a single data asset that powers operations and decision making. Department users of varying technical ability collaborate in the CfA PFCS to accelerate analysis and compound their data asset, while keeping data secure. CfA PFCS includes two modules: StateChat, which enables users to ingest, manage, search, transform, analyze, and present data in a variety of ways depending on their needs and technical proficiency, and SUMMIT module, a scheduling tool used for United Nations General Assembly (UNGA) High Level Week.

During the reporting period, the Department published 3 SORN recissions: Post Capabilities Database (State-71), Communications Personnel Training Records (State-57), and Central Foreign Policy Records (State-29).

- The records contained in State-71 were consolidated with Medical Records (State-24), into a single modified State-24 because the records and system purposes were substantially similar. The

records contained in State-57 were consolidated with Foreign Service Institute Records (State-14), into a single modified State-14 for the same reasons. The records contained in State-29 no longer exist following the decommissioning of the associated system of records, State Archiving System (SAS), in May 2020. As a result, maintenance of State-29 is no longer required.

An additional 26 notifications of SORN creation, modification, or recission are pending completion. All published SORNs are available on the Privacy Office website, https://www.state.gov/system-of-records-notices-privacy-office/.

During this reporting period, the Department completed the review and approval of 37 Privacy Act Statements (PAS).

III. Advice, Training, and Awareness

The Privacy Office advised various offices throughout the Department in connection with the privacy reviews described above. The Office of the Legal Adviser also advised in connection with PIAs, SORNs, and PASs during the reporting period, as reflected in the related documents. In addition to providing advice, the Privacy Office conducted the following privacy trainings during the reporting period:

Mandatory Online Training

- **67,747** 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.

- The PS800 "Cybersecurity Awareness" distance learning course was completed **132,898** times by Department personnel (domestic and overseas) This course includes a dedicated privacy module. This

course is required annually for all personnel who access Department IT networks.

Other Training

The Privacy Office shares best practices for protecting PII with the Bureau of Administration, Office of Technology and Innovation (A/PRI/TI): The Privacy Office conducted two comprehensive training sessions for the Office of Technology and Innovation (A/PRI/TI), focusing on best practices for protecting PII and the resources available to staff at the Department. The training emphasized the importance of maintaining the confidentiality and integrity of sensitive data, ensuring that all attendees are well-equipped to handle PII in their daily operations, and strengthening the overall security posture of the Bureau. As a result, over 40 participants gained a deeper understanding of the critical role of privacy within their office.

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 external complaints and litigation against 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.