Report to Congress 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-1
Reporting Period January 1, 2025 – December 31, 2025

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, 2025 – December 31, 2025. 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**. The Department also conducts an annual tabletop exercise to test the breach response plan and help ensure that key stakeholders understand their specific roles. A Department-wide reorganization in 2025 deferred the planned tabletop exercise from FY25 to FY26.

- **During the reporting period, the Department completed 59 PIAs. PIA reviews are designed to ensure that systems possess required privacy controls. The bullet point below provides a summary of a system that underwent a PIA during the reporting period, serving 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/.**

    - **Operations Response Interagency Online Network (ORION) 2.0:** ORION 2.0 serves as a central repository to inform shift-to-shift guidance of key functions within the Office of Executive Secretariat (S/ES) Operations Center (OPS) and centralizes reporting in a consolidated repository that can be queried. ORION 2.0 provides a centralized data platform for S/ES OPS that enhances monitoring of world events, and proactively detects, flags, alerts, creates and disseminates reports on key events that may impact U.S. Government (USG) interests overseas.

- **During the reporting period, the Department published 1 SORN recission:**

    - **Information Access Programs Records (State-35):** State-35 was rescinded because the system's characteristics and practical use did not qualify it as a system of records as defined in 5 U.S.C. 552a(a)(5). The request letters and Department responses, copies of responsive records (if applicable) and any other correspondence, memoranda, interrogatories, and declarations related to the processing of information access requests from the initial receipt stage through to completion, amendment, appeal, and litigation were not "records" as defined by § 552a(a)(4), as they were not "about" the individuals incidentally mentioned in the files.

- **An additional 29 notifications of SORN creation, modification, or recission are pending completion.** These pending SORNs cover categories including employment records, financial systems, diplomatic operations, law enforcement matters, medical records, and passport services, with a portion being revised to comply with Executive Order 14249, Protecting America's Bank Account Against Fraud, Waste, and Abuse; and M-25-32 Preventing Improper Payments and Protecting Privacy Through Do Not Pay. 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 27 PASs,** primarily for forms covering areas such as visa, employment, personnel processing and program participation, and medical clearance.

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

- **61,564** Department OpenNet users completed the updated distance learning training course, PA318 "Protecting Personally Identifiable Information." This course is required every two years for all OpenNet users.

- **121,763** Department OpenNet users 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

Regional Post Training for Europe and Eurasia (July 2025): The Privacy Office conducted a comprehensive, half-day training session for posts abroad in Europe and Eurasia (EUR) covering the entire range of Privacy responsibilities and best practices including PIAs, SORNs, PASs, breach/incident response, and artificial intelligence. As a result, over 100 participants gained a deeper understanding of the critical role of privacy within their post/unit.

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.