Report to Congress on
Department of State's
Privacy Activities
Reporting Period January 1, 2023 – December 31, 2023
Section 803(f) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, codified at 42 USC 2000ee

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, 2023 – December 31, 2023. 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 in the Bureau of Administration 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.

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.

- **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). 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 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 Breach Response Plan (BRP) was developed in 2018. The BRP was last updated April 2023 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 2023.

During the reporting period, the Department completed 32 PIAs and reviewed 29 additional PIAs that were pending completion. Reviews are designed to ensure that systems possess required privacy controls. Published PIAs are available on the Privacy Office website, https://www.state.gov/privacy-impact-assessments-privacy-office/. Included below is a key example of one of the 32 PIAs completed during the reporting period.

- **Passport Lookout Tracking System (PLOTS)**: The Bureau of Consular Affairs (CA) is responsible for issuing visas to foreign nationals and passports to U.S. citizens and monitoring for potential visa and passport fraud. PLOTS is a Department of State system that supports CA's mission requirements by enabling passport services to manage and track passport cases. PLOTS streamlines the passport lookout tracking process and shortens the duration of investigations by eliminating the need to physically transfer hard copy files.

During the reporting period, the Department published 7 SORNs. An additional 21 are pending completion. All published SORNs are available on the Privacy Office website, https://www.state.gov/system-of-records-notices-privacy-office/. Included below is a key SORN published during this reporting period.

- **Special Presidential Envoy for Hostage Affairs and Related Records, STATE–60**: On April 17, 2023, the *Federal Register* published a new SORN titled "Special Presidential Envoy for Hostage Affairs and Related Records, State-60". Information in Special Presidential Envoy for

Hostage Affairs and Related Records is used to support diplomatic and consular efforts to secure the recovery of and provide assistance and support services to individuals taken hostage or wrongfully detained abroad.

During this reporting period, the Department completed the review and approval of 79 Privacy Act Statements (PAS). Included below is a key PAS for this reporting period.

- **DS-2029-Application for Consular Report of Birth Abroad of a Citizen of the United States of America Form**: The primary purpose for soliciting the information sought in this form is to establish entitlement to issuance of a Consular Report of Birth Abroad and to properly administer and enforce the laws pertaining thereto. The information may also be used in connection with issuing other evidence of citizenship and in furtherance of the Secretary of State's responsibility for the protection of U.S. nationals abroad.

III. Advice, Training, and Awareness

The Privacy Office advised various offices, embassies, and overseas posts throughout the Department in connection with the privacy reviews described above. This advice is reflected in the final versions of the related PIAs and PASs, as well as in the issuance of the Department's artificial intelligence (AI) policy issued in April 2023 and available at https://fam.state.gov/FAM/20FAM/20FAM020101.html.

The Privacy Office developed policy guidance and best practices concerning the use of AI. The Privacy Office further promoted awareness of emerging technology by hosting a Summer Speaker Series on AI, digital privacy rights, and deep fakes, with over 500 Department and interagency attendees across three events.

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 the

related documents. In addition to providing advice and awareness, the Privacy Office conducted the following privacy trainings during the reporting period:

Mandatory Online Training

- **71,309** 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.

- **127,754 foreign affairs 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.

  Note: The numbers cited include both other agency staff and locally employed staff working at our Missions overseas.

Other Training

- **The Privacy Office shares best practices for protecting personally identifiable information (PII) with the Bureau of Global Talent Management (GTM), Office of Accessibility and Accommodations (OAA)**: The Privacy Office was a panelist in a robust discussion on protecting personally identifiable information (PII) and highlighted effective information sharing strategies with contractors who may not have access to government devices. As a result, more than 40 participants were provided best practices on ensuring the confidentiality and integrity of sensitive data when accomplishing their duties as they continue to work towards creating a more accessible Department.

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 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.