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-1Reporting Period July 1, 2022 – December 31, 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 July 1, 2022 – December 31, 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.

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 2022 during this reporting period. 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 34 PIAs and reviewed 26 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 (direct link to PIAs is https://www.state.gov/privacy-impact-assessments-privacy-office/).

- **Consular Affairs Crisis Management System (CACMS)**: The Bureau of Consular Affairs (CA) is responsible for the welfare and protection of U.S. citizens abroad. CA Crisis Management System (CACMS) is used by the Department of State to provide assistance and information to U.S. persons and non-U.S. persons overseas when a crisis occurs. CACMS gives the Department of State user the capability to create and maintain a running log of events associated with the crisis at hand. The Department of State can leverage this capability to provide more detailed updates on the status of a crisis situation and the welfare and whereabouts of particular individuals. CACMS also provides reporting and analytics to support Department logistics and data driven decision-making.

- **Gateway to State (GTS)**: The Bureau of Global Talent Management (GTM) is the personnel management arm of the Department of State and responsible for onboarding and retaining personnel. Gateway to State (GTS) is a web-based job candidate assessment tool that is accessible via the internet from USAJobs. GTS interfaces with the U.S. Office of Personnel Management's (OPM) USAJobs recruitment tool and serves as the automated mechanism for applicants to apply for all Department Civil Service and most Foreign Service jobs. GTS provides email correspondence functionality so that once enrolled, employment candidates can be notified of the respective hiring decisions and interested parties can be notified of future job vacancies. GTS's primary function is to improve and streamline hiring management processes/efforts by automating recruitment activities.

- **Security Incident Management and Analysis System (SIMAS II)**: The mission of the Bureau of Diplomatic Security (DS) is to lead worldwide security and law enforcement

efforts to advance U.S. foreign policy and safeguard national security interests. DS investigates passport and visa fraud, conducts personnel security investigations, and protects the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States. The Security Incident Management and Analysis System (SIMAS) II is a worldwide DS web-based application, which serves as a repository for all suspicious activity, crime, and incident reporting from U.S. Diplomatic Missions abroad (all U.S. embassies and consulates) and Department of State domestic facilities. Department of State personnel, including Diplomatic Security personnel, regional security officers, and cleared foreign nationals, enter incident records into SIMAS II as a central repository for all physical security incidents affecting Department of State interests.

During the reporting period, the Department reviewed 17 SORNs, which are pending completion. All published SORNs are available on the Privacy Office website, http://www.state.gov/privacy (direct link to SORNs is https://www.state.gov/system-of-records-notices-privacy-office/).

In striving to comply with E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the Department has seen an increase in the number of both new and existing IT systems which either use or will be migrating to secure cloud storage. This has resulted in an increase in the number of SORNs which must be updated to reflect cloud storage. Although no new or modified Department SORNs have been published in the Federal Register during the reporting period, of the six SORNs expected to publish early next reporting period, three of those modifications are a result of the Department's migration to cloud storage. The Department expects this trend to continue over the coming years.

During this reporting period, the Department completed the review and approval of 27 Privacy Act Statements (PAS). Included below are four key PAS for this reporting period.

- **DS-4317: Coordination for Afghanistan Relocation Efforts Family Reunification Form:** The information solicited on this form will be used to collect information on Afghans who may be eligible to enter the Operation Allies Welcome (OAW) pipeline for relocation to the U.S. and their family members already in the U.S. with whom they would be reunited. The information furnished may also be used to manifest them for travel and refer them for U.S. Refugee Admissions Program (USRAP) cases.

- **DS-5111-H: Certification of Foster Child Status under the Federal Employees Health Benefits (FEHB) Program:** This form is used to certify a foster child's status as required for coverage under an individual's Federal Employees Health Benefits (FEHB) Program.

- **U.S. Speaker Form:** The purpose of the U.S. Speaker Form is to gather information to enable U.S. citizen recruitment for, and participation in, the Bureau of Educational and Cultural Affairs' U.S. Speaker Program. The information collected and maintained in this form will be used to facilitate and plan exchanges in which U.S. Speakers share expertise with international audiences on topics of strategic importance.

- **Diplomatic Security Memorial Database (DSMDb) Form:** This form collects information to be used by the Department of State to nominate deceased Bureau of Diplomatic Security (DS) personnel for inclusion in the Diplomatic Security Service memorial.

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

Mandatory Online Training

- **43,640** 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.

- **58,116** 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 Advises the Foreign Service Institute (FSI) Office of the Historian on privacy compliance items for the Enterprise Dataset:** At the request of FSI, the Privacy Office staff met with FSI's Office of the Historian to provide privacy guidance on the Enterprise Dataset, which will keep account of the Department's Senior Officials. The virtual meeting provided clear guidance on the required privacy compliance documentation, the implications for managing the collection, and how to best collaborate with other Bureaus on the required privacy compliance.

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.