DEPARTMENT OF STATE
PRIVACY PROGRAM PLAN
SEPTEMBER 2021

Department of State
Privacy Program Plan
Table of Contents

Department of State Privacy Program Plan

1 Introduction

1.1 Purpose of the Privacy Program Plan

The purpose of the Department of State (State or the Department) Privacy Program Plan is to provide an overview of the Department's privacy program. This plan highlights:

- A description of the structure of the privacy program;
- The resources dedicated to the privacy program;
- The role of the Senior Agency Official for Privacy (SAOP) and other privacy officials and staff;
- The strategic goals and objectives of the privacy program;
- The program management controls in place to meet applicable privacy requirements and manage privacy risks; and
- Any other information deemed necessary by the Department's privacy program.

1.2 State Privacy Website

The Department's public-facing privacy website contains information on the Senior Agency Official for Privacy (SAOP), system of records notices (SORNs), privacy impact assessments (PIAs), privacy reports, and additional points of contact. Any questions, concerns, or complaints may be addressed by contacting State Privacy Office by email at Privacy-DL@state.gov or by telephone at (202) 453-8751.

2 Overview of the Department of State Privacy Program

2.1 Mission Statement

The Department's Privacy Office safeguards privacy and promotes transparency through compliance, advice, training, and collaboration.

2.2 Strategic Goals and Objectives for Privacy

The Department is committed to safeguarding PII. The Department's Privacy Program intends to use all methods of regulation, policy, guidance, and principles to further this objective across the Department of State. Privacy considerations are a part of all levels of decision-making to continuously build a culture of trust and privacy throughout the Department.

GOAL 1: Build a privacy-aware culture at the Department of State

Objective 1.1: Raise privacy awareness through multiple communications platforms, such as Department Notices, outreach materials, webinars, and events

Objective 1.2: Expand the role of privacy in Department governance through increased partnerships and engagement in Department-wide initiatives and issues with privacy equities

Objective 1.3: Incorporate privacy content in Department role-based training courses to provide targeted training to Department staff relevant to their specific roles

GOAL 2: Strengthen the Privacy Program at State

Objective 2.1: Increase Department of State representation and participation in privacy-related inter-agency communities of practice, committees, working groups and/or councils to capture and share best practices and identify emerging privacy issues

Objective 2.2: Develop and maintain outstanding privacy professionals through continual learning and training opportunities

Objective 2.3: Design and implement a strategic organizational structure for the Privacy Office that facilitates and streamlines compliance and ensures that Department of State privacy policies keep pace with the quickly evolving policy and technology landscape

Objective 2.4: Develop a mechanism to establish Bureau privacy liaisons to disseminate technical expertise across the Department and improve the compliance process

Objective 2.5: Build consensus among Department Stakeholders of their roles and responsibilities in breaches of personally identifiable information to ensure a rapid response to processing and mitigation

GOAL 3: Ensure compliance with federal privacy laws and OMB directives

Objective 3.1: Collaborate effectively with the Bureau of Information Resource Management (IRM) and other stakeholders to ensure privacy controls are in place throughout the Department, including the development of an industry-standard Continuous Monitoring Strategy

Objective 3.2: Improve compliance with mandated privacy requirements under the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Modernization Act of 2014

Objective 3.3: Mitigate breach risk for personally identifiable information held by contracting entities on behalf of the Department

2.3 Privacy Governance in the Department

The SAOP for the Department's privacy program is the Department of State's Deputy Assistant Secretary for Global Information Services. The SAOP is responsible for overseeing, coordinating, and facilitating the Department's compliance with privacy policies, as mandated by Federal legislation, the Office of Management and Budget (OMB), and as described in the Department's Foreign Affairs Manual (5 FAM 460). 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 Chief Privacy Officer (CPO) and Deputy Chief Privacy Officer (DCPO). In addition to the CPO and DCPO, the Privacy Office's organizational structure comprises two Privacy Program Managers, eight full-time program analysts, and an administrative officer. Privacy Office staff is responsible for conducting privacy compliance reviews, training Department personnel, assisting with reporting functions, and managing privacy breaches.

The Department's Office of the Legal Adviser advises the SAOP, the Privacy Office, 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.

The Privacy Office also interacts with the Department's Chief Information Officer (CIO) and the Office of Cyber Operations within the Information Resources Management Bureau in accordance with the Department's Risk Management Framework to accredit those IT systems which process PII.

2.4 Core Response Group

The Core Response Group (CRG) is convened at the discretion of the Under Secretary for Management (M) based on the recommendation of the SAOP, in the event of an actual or suspected major breach of PII. The CRG members consist of the following organizations' representatives at the Assistant Secretary level or designee, as commensurate with the scope of the breach:

- The Office of the Under Secretary for Management (M), CRG Chair;
- Office of the Legal Adviser (L);
- Senior Agency Official for Privacy (SAOP);
- Bureau of Administration (A);
- Chief Information Officer (CIO) and Chief Information Security Officer (CISO);
- Bureau of Diplomatic Security (DS);
- Bureau of Legislative Affairs (H);
- Bureau of Public Affairs (PA); and
- Stakeholder Bureau

Depending on the nature of the breach, CRG members may also include:

- Bureau of the Comptroller and Global Financial Services (CGFS);
- Bureau of Consular Affairs (CA);
- Medical Director (MED); and
- Director General of the Foreign Service and Director of Human Resources

See Section 8.2 Core Response Group and Breach Rapid Response Task Force, for more information.

3 Privacy Workforce Management

The SAOP, in collaboration with the CPO, assesses and addresses the hiring, training, and professional development needs of the Department with respect to privacy. The SAOP ensures that privacy managers are aware of flexible hiring authorities with which privacy professionals can be brought on board. Additionally, the SAOP coordinates with other Department principals to: 1.) maintain and enhance a current workforce planning process through the annual budget reconciliation process and creation of privacy strategic plans, 2.) maintain workforce skills through the establishment of Department-wide privacy training, 3.) recruit and retain privacy and IT professionals with complementary awareness of both privacy and IT security issues, and 4.) develop competency requirements for Department staff in the area of PII breach response.

4 Budget and Acquisition – Privacy Requirements in IT Solicitations

The Federal Acquisition Regulations (FAR) require that a contracting officer in the Department's Acquisition's Office review solicitation requirements to determine whether the contract will involve the design, development, or operation of a system of records on individuals to accomplish an agency function. If either of these tasks will be required, then the contracting officer ensures that the contract statement of work specifically identifies the system of records on individuals and the design, development, or operation work to be performed; and makes available, in accordance with agency procedures, agency rules and regulations implementing the Privacy Act.

The Department's policies concerning its capital planning and investment control process are included in the Foreign Affairs Manual (FAM), specifically 5 FAM 610. IT investment requests progress through the phases of: Pre-Select, Select, Control, and Evaluate. The Senior Agency Official for Privacy (SAOP) is a functional partner in this process, which reviews all IT investments, ensuring privacy is considered and protected in electronic activities. For IT applications involving cloud services, the SAOP sits on an evaluation board hosted by the Cloud Program Management Office as detailed in 5 FAH-8 H-351.1.

Before the Information Technology Executive Council PMO reviews a request for a new IT system and associated funding, an IT business case must be drafted. The Department offers IT business case training for IT program/project managers and staff, bureau budget officers, and all other Department personnel involved in developing IT business cases. The Privacy Office delivers privacy-related content for this training. Business cases involving IT systems with privacy risk are reviewed by Privacy Office personnel to ensure that privacy risk is adequately identified and remediated. This reinforces 5 FAM 611(o) that specifies that system owners must consult with the Department's Privacy Office when conducting a Privacy Impact Assessment (PIA).

A system owner must draft a PIA for any IT system (new or existing) which collects, processes, stores, forwards, transmits or maintains PII. That PIA is reviewed by the Privacy Office and the SAOP. If the PIA reveals that PII cannot be protected, then the SAOP will so note in a memo to the CIO.

5 Privacy Risk Management Framework

5.1 Implementation of a Risk Management Framework (RMF)

In the Department, the Bureau of Information Resources Management, Cyber Operations manages the Department's governance, risk, and compliance (GRC) tool, Xacta, to implement the RMF and manage the authorization to operate (ATO) process Department-wide for information systems. The Privacy Office participates in the ATO process by conducting a privacy assessment for each information system undergoing the ATO process that collects, stores, forwards, transmits, processes or disseminates PII. The Bureau of Information Resource Management has developed an RMF Playbook, a reference tool designed to give Department of State employees and contractors step-by-step instructions on how to implement the RMF and manage the authorization to operate (ATO) process in Xacta.

5.2 Review and Approval of Categorization of Information Systems that Involve PII

The Department follows NIST standard SP 800-60 Vol. II to categorize the data types collected by each information system, including PII. Correct categorization of data types allows for selection and implementation of the correct security and privacy controls in the succeeding steps of the RMF. Once categorized, the ISO consults SP 800-60 to identify and judge the level of risk that is associated with each particular category of information and posts it in Xacta. Thereafter, the task is forwarded to the Authorizing Official Designated Representative (AODR) queue for review and approval.

5.3 Privacy Impact Assessments (PIAs)

The Privacy Questionnaire in Xacta serves as a privacy threshold assessment (PTA) and lets the Privacy Office know whether a PIA will be required. The ISO and team then engage the Privacy Office to request assistance. A PIA is included in RMF Step 1 (Categorize Information System).

6 Privacy Control Requirements/Continuous Monitoring Strategy

6.1 Privacy Impact Assessment (PIA)

Section 208 of the E-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment (PIA) for any electronic information collection and information technology (IT) system that contains personally identifiable information (PII).

A PIA is an analysis of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
- Determine the risks and effects of collecting, maintaining and disseminating PII in a system, and;
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Additionally, a PIA demonstrates that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. It also provides the public with information about the Department of State's collection and use of PII.

A PIA must be conducted when:

- Developing or procuring new technologies or systems that handle or collect PII
- Making significant revisions or modifications to an existing system
- Undergoing a system's triennial security reauthorization
- Issuing a new or updated rulemaking involving the collection of PI
- Moving to cloud storage
- Collecting information by a third-party application utilized by the Department

The Department's Privacy Office has developed a PIA Guide and Template document to aid program offices in drafting a PIA; it contains the required templates and other PIA-related resources. The Department posts PIAs on systems which collect PII from members of the public on its public-facing website.

6.2 Contractors and Third Parties

The Department ensures contractors and third parties that:1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of the Department; or 2) operate or use information systems on behalf of the Department, comply with the mandated privacy requirements. The Department's Privacy Program coordinates with the Office of Acquisition Management to ensure that the applicable privacy clauses below are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of information in the possession of the Department:

- FAR Subpart 4.19–Basic Safeguarding of Covered Contractor Information Systems
- FAR Clause 52.204-21
- FAR Subpart 24.1 Protection of Individual Privacy
- FAR Clause 52.224-1 "Privacy Act Notification"
- FAR Clause 52.224-2 "Privacy Act"
- FAR 39.101–Acquisition of Information Technology-General-Policy
- FAR 39.105–Acquisition of Information Technology-General-Privacy
- FAR Clause 52.239-1 "Privacy or Security Safeguards"
- FAR Subpart 27.4–Rights in Data and Copyrights

6.2.1 Ensuring Contracts Incorporate Privacy Requirements

The Privacy Office periodically reviews contracts to verify inclusion of mandatory Federal Acquisition Regulation (FAR) clauses that cover the design, development, or operation of a system of records on individuals (FAR clauses 52.224-1 and 52.224-2), as well as breach language specified in OMB M-17-12. Additionally, the Privacy Office issues instruction on when to insert contract clauses into contracts which are contained in the relevant FAR sections.

6.3 System of Records Notice (SORN)

The Department meets Privacy Act requirements for publishing SORNs in the Federal Register. A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

A SORN is intended to inform the public about what kinds of personal information federal agencies maintain; to limit the uses and disclosures of the information to those compatible with the law permitting its collection; and to describe how an individual might request access to their information or to seek redress otherwise.

6.3.1 SORN Reviews and Updates

The Department ensures that SORNs remain accurate, up-to-date, and appropriately scoped during PIA reviews and through a structured multi-year SORN review process. The Department ensures that with respect to SORNs:

- No system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order; and
- Each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary.

6.3.2 Reporting SORNs to OMB and Congress

The SAOP reports all significant changes to existing SORNs and new SORNs to OMB and Congress following requirements identified in OMB Circular A-108. Reports, under cover of a letter signed by the SAOP, include:

- A description of the purpose(s) for which the Department is establishing or modifying the system of records and an explanation of how the scope of the system is commensurate with the purpose(s) of the system;
- The specific authorities (statutes or executive orders) under which the system of records will be maintained. The Department cites the specific programmatic authorities for collecting, maintaining, using, and disseminating the information;
- An evaluation of the probable or potential effect of the proposal on the privacy of individuals whose information will be maintained in the system of records; the assessment may be derived from applicable PIAs;
- An explanation of how each new or modified routine use satisfies the compatibility requirement of the Privacy Act; and
- Any information collections approved by OMB or submitted to OMB for approval that will be used to collect information that will be maintained in the system of records, along with the relevant names, OMB control numbers, and expiration dates.

6.3.3 Systems of Records Notices (SORNs) for Contractors

Where the Department employs contractors in the design or implementation of system of records containing Privacy Act information or PII, the System of Record Notice (SORN) for that system of records makes explicit references to contractors in the listing of routine uses.

6.4 Privacy Act Statements

The DOS ensures that a Privacy Act compliant statement is provided or available when collecting PII. The Privacy Act Statement is provided on the collection instrument, on a poster that is visible to the individual, or on a separate form that can be retained by the individual prior to the actual collection. A Privacy Act Statement provides an individual with:

- The Agency's legal authority to collect the information, such as a statute, executive order, and/or regulation;
- The purpose(s) for collecting the information and how it will be used;
- The routine uses of the information, which describes to whom the Department may disclose information outside of the Department and for what purposes1; and
- Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual of not providing all or any part of the information requested.

6.5 Privacy Controls

Currently, the Department uses the privacy controls contained in Appendix J of NIST's 800-53, version 4, as the designated privacy control set. The Department is transitioning to implementing NIST's 800-53, version 5 control set. It is anticipated that the Department's privacy control baseline will be a tailored version of NIST's Privacy Baseline found in 800-53B. The Department's current index for inventory of privacy controls can be found in the Privacy Office's Continuous Monitoring Strategy.

6.5.1 Privacy Control Selection Process

The Privacy Control Selection Process is based on *NIST Special Publication SP 800-122*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. Based on the answers provided in the Privacy Questionnaire, the type and number of PII elements are evaluated and used to determine the sensitivity level (low, moderate, or high) and the privacy and security controls that are identified in the security control baseline.

6.5.2 Continuous Monitoring Strategy and Program

The Privacy Office has developed a Continuous Monitoring Strategy (based on Appendix J controls in NIST's 800-53, rev. 4). The Privacy Continuous Monitoring Strategy and Program will be revised to reflect the new security and privacy baseline once the Department migrates to NIST's SP 800-53, version 5, controls.

6.5.3 Review Authorization Packages for Information Systems that Involve PII

A Privacy Impact Assessment (PIA) is created by the system owner for any system that involves PII. Once the Privacy Office reviews and approves the PIA, then the SAOP formally informs the CIO, via memorandum, that any privacy risk has been identified and remediated and is considered acceptable for the Department to carry.

7 Requirements for Handling and Protecting Personally Identifiable Information (PII)

7.1 Recognizing Personally Identifiable Information

Personally Identifiable Information (PII) refers to information which can be used to distinguish or trace an individual's identity. PII includes, name, social security number, biometric records, etc. which alone, or combined with other personal or identifying information, such as date and place of birth, mother's maiden name, etc. can be linked to a specific individual.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. The following types of PII are considered sensitive when associated with an individual:

- Social Security Number (including in truncated form);
- Place of birth;
- Date of birth;
- Mother's maiden name;
- Biometric information;
- Medical information (excluding brief references to absences from work);
- Personal financial information;
- Credit card/purchase card account numbers;
- Passport numbers;
- Potentially sensitive employment information (e.g., performance ratings, disciplinary actions, results of background investigations);
- Criminal history; or
- Information that may stigmatize or adversely affect an individual.

Context of information is important. The same types of information can be sensitive or non-sensitive depending upon the context. For example, a list of names and phone numbers for the Department's softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease.

7.2 Minimizing the Collection of PII

The Privacy Act of 1974 requires that Federal agencies maintain only relevant and necessary information about individuals. In addition, the Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, directs Federal agencies to eliminate unnecessary collections, maintenance, and uses of Social Security Numbers (SSN).

The Department maintains an agency-wide inventory of PII holdings and uses the PAS, PIA, and SORN certification and re-certification process to identify reduction opportunities and to ensure, to the maximum extent practicable, that such holding is accurate, relevant, timely, and complete. In addition, the Department has established process requirements for justifying the collection, maintenance, and uses of SSNs as directed in the Department's Guide to Eliminating Unnecessary SSNs.

7.3 Handling and Transmitting PII

PII requires strict handling guidelines due to the nature of the data and the increased risk to an individual if data were to be compromised. The Department's best practices for handling PII include:

- Encrypt sensitive PII on computers, media, and other devices;
- Lock or log off unattended computer systems;
- Destroy sensitive paper PII by shredding or using burn bags;
- Delete sensitive electronic PII by emptying computer recycle bin;
- Store sensitive PII on secure Federal Government systems only;
- Secure sensitive paper PII data by locking in desks and filing cabinets.

Sensitive PII may be distributed or released to other individuals if it is within the scope of their official duties and they have a need to know. If sensitive PII is electronically transmitted, it must be protected by secure methodologies, such as encryption, Public Key Infrastructure, or secure sockets layer. When in doubt, the Department treats PII as sensitive. The transmission of sensitive PII must be kept to a minimum, even if it is protected by secure means.
Other ways for communicating, sending, and receiving sensitive PII include:

- Facsimile – When faxing information, include an advisory statement about the contents on the cover sheet and notify the recipient before and after transmission. Exception: According to State Acquisition Manual 1313.301, Department purchase card holders shall not transmit purchase card information over a facsimile machine.
- Mail – Physically secure sensitive PII when in transit by sealing it in an opaque envelope or container, and mail using First Class or Priority Mail, or a commercial delivery service. Do not mail, or send by courier sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, or other removable media unless the data is encrypted.
- Hard Copy – Hand-deliver documents containing sensitive PII if needed. Do not leave sensitive PII unattended on printers, facsimile machines, or copiers.

8 Breach Incident Response and Management

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence (i.e. the loss of confidentiality, integrity, or availability of PII) where:

- A person other than an authorized user accesses or potentially accesses sensitive PII, or
- An authorized user accesses or potentially accesses sensitive PII for other than an authorized purpose.

8.1 Reporting Breaches

In the event of an actual or suspected breach, employees, contractors and relevant stakeholders must immediately report the breach using a Breach Incident Form. The form, once completed, will automatically send a report to the Cyber Incident Response Team at Diplomatic Security and to the Privacy Office as well as to the reporting office's supervisor in accordance with the Department's Breach Response Plan and any published bureau or post procedures.

8.2 Breach Response Plan

The Breach Response Plan ("BRP" or "Plan") establishes governing policies and procedures for handling breaches of PII at the Department of State. 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 Plan incorporates the policies and procedures, roles and responsibilities, collaboration and coordination, transparency and timeliness requisite to successful response to, and management of, a breach involving PII and the safeguarding of individuals' privacy. Additionally, the Plan ensures that processes are in place to verify corrective actions. The Department tests its Breach Response Plan through an annual Table Top Exercise.

8.3 Breach Reporting

The Department reports breach incidents in accordance with OMB and DHS guidance. Government-wide statistics on breach incidents can be found in the annual Federal Information Security Modernization Act (FISMA) Report to Congress and the latest Department statistics are reported annually to DHS via the SAOP FISMA Reporting Metrics report.

8.4 Core Response Group and Breach Rapid Response Task Force

The Data Breach Core Response Group (CRG) serves as a mechanism for the Department to respond promptly and appropriately in the event of a data breach involving PII. The CRG, comprised of representatives from various bureaus and offices throughout the Department involved in privacy issues, determines whether the data breach poses risks related to identity theft or other harms to those potentially affected and, if necessary, assists the relevant bureau or office within the Department in making an appropriate response to the data breach.

8.5 Cyber-Incident Response Team (CIRT)

The CIRT conducts security monitoring of unclassified and classified networks within the Department of State to ensure the integrity, availability and confidentiality of the IT infrastructure. CIRT operations provide near real-time detection, collection, analysis, correlation and reporting of cyber security events that pose a threat to the Department's networks, to include potential breaches of PII. If a breach involves electronic PII, then the CIRT must be involved. The CIRT coordinates with numerous components within the Department to remediate security

events upon detection and reports the overall status of Department cyber security to senior management each business day. The CIRT also serves as the central reporting point for cyber security incidents within the Department of State. The Department of Homeland Security has designated the CIRT as the official conduit for reporting cybersecurity incidents to US-CERT on behalf of the Department of State. Additionally, CIRT shares security information with law enforcement entities as appropriate.

8.6 Security Incident Adjudication

The Bureau of Diplomatic Security Program Applications Division is responsible for administering the Department's Security Incident programs, which enhance the protection of Department information and information systems by identifying, assessing, and assigning responsibility for failures to safeguard Department information and information systems in accordance with applicable laws and Department policies. When the CRG has determined that a data breach has occurred, it will be referred to the Diplomatic Security Program Applications Division for consideration.

9 Awareness and Training

9.1 Privacy Training

All Department workforce members, including contractors, are required to complete the Cyber Security Awareness course (PS800) annually through the Foreign Service Institute (FSI). This course contains a privacy awareness section to assist employees in properly safeguarding PII. In addition, all Department staff and contractors must complete the course, Protecting Personally Identifiable Information (PII) (PA318), also through FSI. This is a mandatory biennial requirement for all contractors and staff that access the Department of State network.

9.2 Privacy Resources

The Department's Privacy Program apprises agency employees of available privacy resources, including internal and external websites, Department Notices, and cables. Examples include:

- The Privacy Program Intranet site – This is an information-rich site with privacy FAQs, contextual information about PIAs, SORNs, PII breach reporting, Privacy Act Statements, and requesting custom-tailored privacy training,
- Privacy Program Public-Facing website - This site contains all the Department's SORNs, PIAs covering systems collecting PII from members of the public, privacy-related reporting and links to the Department's Senior Agency Official for Privacy (SAOP).
- ALDACs – These "All Diplomatic and Consular Posts" cables reach Foreign Service posts world-wide to announce privacy topics.
- Department Notices – These notices are used to announce training and provide privacy-related information and guidance.
- Foreign Service Institute (FSI) – FSI serves as the Department's official training venue and hosts the mandatory on-line PA318 "Protecting PII" course.
- PIA Templates and Guides
- SORN Templates and Guides
- PAS Templates and Guides

9.3 Foundational and Advanced Privacy Training

9.3.1 Foundational

The Department offers multiple types of privacy foundational training and modes of raising privacy awareness. In addition to the two mandatory courses mentioned earlier (PS800 and PA318), the Privacy Office contributes to the Department's "Tip of the Day" series, maintains substantial FAQs on the Privacy intranet site, and hosts privacy awareness events such as "Data Privacy Day" and guest Library speakers.

9.3.2 Advanced privacy training

The Department also offers advanced specialized privacy training for those employees performing PII intensive activities or building IT systems which may capture PII. For instance, the Bureau of Consular Affairs offers a course through FSI titled "Passport Data Security Awareness (PC441)". The IRM Bureau sponsors training for IT system designers (IT Business Case Training) which includes a module on how to build appropriate privacy protections into IT system design. Additionally, the Privacy Office offers custom-tailored training sessions based on customer needs.

9.3.3 Role-Based Training

The Privacy Office is a key stakeholder in the Department's Cyber Training Synchronization Working Group. The working group's mission is to share and discuss cybersecurity awareness, training, education, and enhance the effectiveness of Department Cybersecurity and Information Security Training. The goal is to avoid duplication, reinforce messages to maximize user learning and protect Department data and systems. The working group is researching the Department's existing training catalog to identify courses that are role-specific. As roles are identified, the working group will evaluate the content to identify the gaps in the required competencies cybersecurity and update the course material accordingly.

9.4 Advanced Privacy Training for Privacy Personnel

The Privacy Office encourages its personnel to attain privacy certifications and attend as many of these types of events as possible.:

- Federal Privacy Council (FPC) Boot Camp Training: Provided semi-annually by the Federal Privacy Council.
- International Association for Privacy Professionals (IAPP): Annual training conferences and certification courses.
- National Institute of Standards and Technology (NIST): On-line training on the risk management framework

9.5 Rules of Behavior and Accountability

The Department defines rules of behavior as established rules developed to promote a workforce member's understanding of the importance of safeguarding PII, his or her individual role and responsibilities in protecting PII, and the consequences for failed compliance. All Department workforce members with access to PII in the performance of their official duties are required to comply with established rules. The Federal Information Security Modernization Act (FISMA) of 2014 requires system owners to ensure that individuals requiring access to information and information technology (IT) systems, including those containing PII, sign appropriate access agreements prior to being granted access. The access agreement for a system must include rules

of behavior tailored to the requirements of the system. The Department's rules of behavior and responsibilities for enforcing the same can be found in the Foreign Affairs Manual at 5 FAM 469. The Department provides webinars and other training opportunities to provide agency-wide training for contractors and employees.

10 Privacy Reporting

10.1 Annual Report- Federal Information Security Modernization Act (FISMA)

The Federal Information Security Modernization Act (FISMA) of 2014 requires Federal agencies to develop, document, and implement agency-wide information security programs that include plans and procedures to ensure the continuity of operations for information systems that support the operations of the agencies. All Federal agencies are required to submit an annual report to the OMB and U.S. Department of Homeland Security; the Committees on Oversight and Government Reform, Homeland Security, and Science, Space, and Technology of the House of Representatives; the Committees on Homeland Security and Government Affairs; and State, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; and the Comptroller General.

The Department's SAOP completes the SAOP report, which is submitted as part of the Department's annual FISMA report.

10.2 Privacy Activities (Section 803)

Reports as required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee-1(f) (2012). On July 7, 2014, the statute was amended to require semiannual submissions of the periodic reports rather than quarterly submissions.

10.3 Social Security Number Reporting

On September 15, 2017, the President signed into law H.R. 624, the Social Security Number Fraud Prevention Act of 2017, which became Public Law No, 115-59. In addition to an initial implementation plan, the Act requires the Department of State to provide an annual report to Congress every year for five years-concerning actions taken to reduce the use of complete social security account numbers (SSNs) on documents that are mailed.

11 Appendices

Appendix A – Authorities, Memoranda, Policies, and Guidance

Authorities

- Privacy Act of 1974, 5 U.S.C. §552a
- Federal Information Security Modernization Act of 2014
- E-Government Act of 2002
- Freedom of Information Act (FOIA)
- Paperwork Reduction Act of 1995

Office of Management and Budget (OMB) Memoranda

- OMB Memorandum for Privacy Act Officers of Departments and Agencies, *Status of Biennial Reporting Requirements under the Privacy Act and the Computer Matching and Privacy Protection Act (June 21, 2000)*
- OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000)*
- OMB Memorandum M-03-22**,** *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)*
- OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)*
- OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Application, (June 25, 2010)*
- OMB Memorandum for Chief Information Officers, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications, (December 29, 2011)*
- OMB Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset (May 9, 2013)*
- OMB Memorandum M-13-20, *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative (August 16, 2013)*
- OMB Memorandum M 14-06, *Guidance for Providing and Using Administrative Data for Statistical Purposes, (February 14, 2014)*
- OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)*
- OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services (November 8, 2016)*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets, (December 9, 2016)*
- OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)*
- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (November 2, 2020)*

OMB Circulars

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016)*
- OMB Circular A-130, *Managing Information as a Strategic Resource (July 28, 2016)*
- OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016)*

Appendix B Breach Response Flow Chart