Office of Information Technology (OIT)

Privacy Program Plan

November 10, 2022

Table of Contents

1.0 Overview

1.1 Purpose

The purpose of the U.S. International Development Finance Corporation (DFC) privacy program plan is to provide an overview of the agency's privacy program and communicate how DFC implements and integrates privacy into the work of the agency. This plan includes:

- 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 and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks[1]

1.2 Privacy Program Mission

The DFC privacy program's mission is to establish a strong culture of privacy awareness and protection that ensures transparency and accountability for agency activities involving the use of personally identifiable information (PII). The proper handling of PII is critical to building the trust of DFC's stakeholders – including employees, contractors, other federal agencies, and members of the public. The privacy program works toward achieving its goals by promoting the consistent application of privacy laws, policy, and standards. This includes the Privacy Act of 1974, as amended (Privacy Act), E-Government Act of 2002, Federal Information Security Modernization Act of 2014 (FISMA), Office of Management and Budget (OMB) guidance, and standards issued by the National Institute of Standards and Technology (NIST).

1.3 Personally Identifiable Information

The concept of protecting PII is central to any privacy program. PII is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. It is important to

[1] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), Appendix I - 5.

recognize that information that is not PII can become PII when additional information becomes available that would make it possible to identify an individual.[2]

Examples of PII include but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as Social Security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographic indicators, employment information, medical information, education information, financial information)[3]

Sensitive PII (SPII) is PII that if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII requires stricter handling because of the increased risk of harm if the information is improperly disclosed.[4] In determining whether information is PII or SPII, agencies should use a best judgment standard based on the context of the information in relation to the risk of harm. For example, a list of employee names is generally considered PII, but the name of an employee who works in an intelligence position might be considered SPII because revealing their identity could result in substantial harm to the individual (e.g., blackmail, physical harm, etc.) due to the employee's access to classified information and the potential to compromise national security.

1.4 Fair Information Practice Principles

[2] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), Appendix II - 1.
[3] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (Apr. 6, 2010), ES-1.
[4] GAO-08-343, *Information Security: Protecting Personally Identifiable Information* (Jan. 25, 2008), 5.

The privacy program adheres to the Fair Information Practice Principles (FIPPs) as the policy framework for accomplishing its mission. The FIPPs are a collection of widely accepted principles that agencies should use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs are not OMB requirements; rather, they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements.[5]

DFC incorporates the FIPPs into numerous agency-wide processes as described below:

- Access and Amendment – DFC provides individuals with appropriate access to PII and appropriate opportunity to correct or amend PII. Privacy Act requests for access or amendment may be sent to the DFC Office of Human Resources or the appropriate system manager.
- Accountability – DFC monitors, audits, and documents compliance with the FIPPs through several processes, including but not limited to the completion of Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs), where appropriate. Additionally, DFC incorporates key privacy requirements into the agency's Information System User Rules of Behavior and provides appropriate privacy training to all employees and contractors who have access to PII.
- Authority – DFC only creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII if it has authority to do so, and identifies this authority in the appropriate notice. If the information is maintained in a system of records, DFC provides a Privacy Act Statement to the individual that contains the appropriate statute or executive order for collecting the information.
- Minimization – DFC only creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII that is directly relevant and necessary to accomplish a legally authorized purpose, and only maintains PII for as long as is necessary to accomplish the purpose. DFC does not process information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.

[5] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), Appendix II - 2.

- Quality and Integrity – DFC creates, collects, uses, processes, stores, maintains, disseminates, and discloses PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- Individual Participation – DFC involves the individual in the process of using PII and, to the extent practicable, seeks individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to the DFC privacy program or SAOP.
- Purpose Specification and Use – DFC provides notice of the specific purpose for which PII is collected and only uses, processes, stores, maintains, disseminates, and discloses PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
- Security – DFC has established physical, technical, and administrative safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- Transparency – DFC is transparent about information policies and practices with respect to PII, and provides clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

1.5 Privacy Threshold Analysis

The PTA is a questionnaire that is used to determine whether an information system, program, project, or collection (hereinafter, collectively referred to as "system") involving PII has privacy implications that trigger other privacy requirements. Although not statutorily required, the PTA is useful in initiating the communication and collaboration between program officials and the privacy program at the earliest stages of the information life cycle. Completing the PTA is the first step that DFC program officials should take in the privacy compliance process.

The purpose of the PTA is to:

1) Identify systems that are privacy-sensitive
2) Demonstrate DFC's consideration and inclusion of privacy during the review of a system

3) Provide a record of the system and its privacy requirements to the DFC privacy program

4) Demonstrate DFC's compliance with privacy laws, regulations, and government-wide guidance

After completing its review, the privacy program will return the PTA to the program official with recommendations on next steps, if any.

1.6 Privacy Impact Assessment

A PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[6]

In accordance with Section 208 of the E-Government Act of 2002, a PIA must be conducted before:

a. Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

b. Initiating a new collection of information that–

   i. Will be collected, maintained, or disseminated using information technology; and

   ii. Includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, further clarifies that part (a) applies to developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form *from or about members of the public*. No PIA is required where

[6] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), Sec. II.A.f. "Privacy Impact Assessment: Definitions."

information relates to internal government operations, has previously been assessed under an evaluation similar to a PIA, or where privacy issues are unchanged.[7]

1.7 Adapted Privacy Impact Assessment

OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, requires federal agencies to take specific steps to protect individual privacy whenever they use third-party websites or applications to engage with the public. Among other requirements, the memorandum asks agencies to prepare an adapted PIA that is tailored to address the specific functions of a third-party website or application that is being used.

The adapted PIA should describe:

i. The specific purpose or the agency's use of the third-party website or application

ii. Any PII that is likely to become available to the agency through public use of the third-party website or application

iii. The agency's intended or expected use of PII

iv. With whom the agency will share PII

v. Whether and how the agency will maintain PII, and for how long

vi. How the agency will secure PII that is uses or maintains

vii. What other privacy risks exist and how the agency will mitigate those risks

viii. Whether the agency's activities will create or modify a "system of records" under the Privacy Act

1.8 System of Records Notice

The Privacy Act applies to records about individuals in a system of records. Under the Privacy Act's definitions, the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence. The term "record" means any item, collection, or grouping of information about an individual that is maintained by the agency, including, but not limited to, his education, financial transactions, medical history, and

[7] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), Sec. II.B.a. "Privacy Impact Assessment: When to conduct a PIA."

criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. The term "system of records" means 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 identifying particular assigned to the individual.[8] The Privacy Act does not apply to deceased persons, corporations and organizations, and non-citizens or non-lawful permanent residents.[9]

A record is considered a Privacy Act record when all of the following apply:

1) The record must be about the individual
2) The record must identify the individual
3) The record must be maintained by the agency

A system of records exists if:

1) There is an indexing or retrieval capability using identifying particulars built into the system, and
2) The agency does, in fact, retrieve records about individuals by reference to some personal identifier.[10]

The Privacy Act requires each agency to publish notice of its systems of records in the *Federal Register*. The purpose of this notice, called a System of Records Notice (SORN), is to provide information to the public on the purpose of a system of records and how the records will be maintained and used by the agency.[11] If there is no established system of records, retrieval by personal identifiers is prohibited.

1.9 Privacy Act Statement/Privacy Notice

Under the Privacy Act, agencies are required to provide a Privacy Act Statement, also known as an (e)(3) statement, to all persons asked to provide personal information about

[8] 5 U.S.C. § 552a, *The Privacy Act of 1974, as amended* (Dec. 31, 1974, amended in 1988 and 1990), Subsect. (a). "Definitions."
[9] Moncada, Kirsten J. *The Privacy Act of 1974: An Overview 5 U.S.C. §552a* [Slideshow] (https://www.accesspro.org/AccessPro/assets/File/training/ntc-2018/docs/1%2004%20Privacy%20Act%20Overview%20(Moncada).pdf) (Jul. 18, 2018), 7.
[10] *See id.* at 11-12.
[11] OMB Circular No. A-108, *Federal Agency Responsibilities for Reviewing, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016), 5.

themselves that will go into a system of records. The statement shall provide sufficient information about the request to allow the individual to make an informed decision about whether to respond.

A Privacy Act Statement shall include a plain-language description of:

1) Authority: The legal authority to collect the information as provided by a federal statute, executive order, or regulation
2) Purpose: The purpose for collecting the information and how it will be used
3) Routine Uses: To whom the agency may disclose information outside of the agency and for what purpose (and, if practicable, a link to the SORN)
4) Disclosure: Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual for not providing all or part of the information requested[12]

For systems that do not collect information as part of a system of records, a Privacy Notice is recommended. The Privacy Notice contains the same elements as a Privacy Act Statement but does not reference a SORN.[13]

1.10 Risk Management Framework

The privacy program utilizes the Risk Management Framework (RMF) as a technology neutral method for managing privacy risks in the agency. The RMF serves as the basis for evaluating the privacy and security risks in systems. It provides a disciplined, structured, and flexible process for managing risk in seven steps: a preparatory step to ensure that the organization is ready to execute the process, and six main steps.

The RMF steps are:

- Prepare to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk
- Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss

[12] OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016), 13.
[13] NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept 23, 2020), 233.

- Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk
- Implement the controls and describe how the controls are employed within the system and its environment of operation
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements
- Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable
- Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system[14]

The RMF steps are illustrated in Figure 1:

[14] NIST Special Publication 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Dec. 20, 2018), 8.

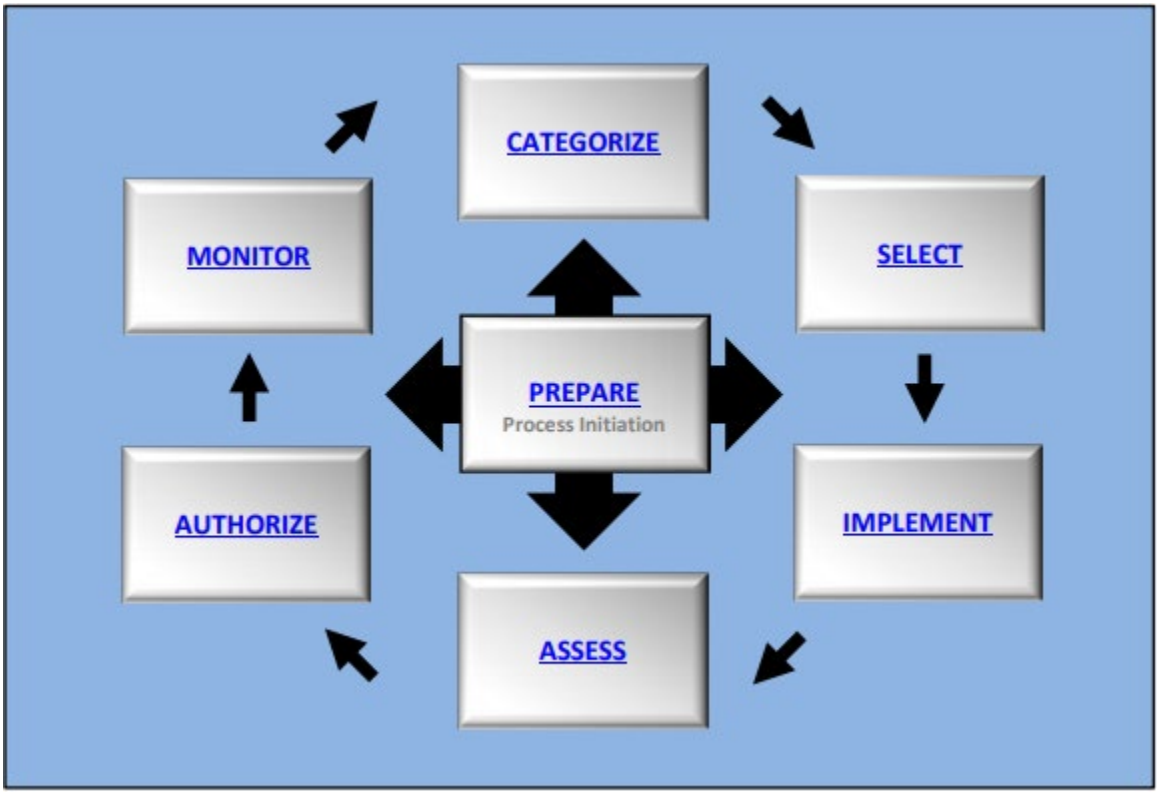

Figure 1 - Risk Management Framework[15]

1.11 Privacy Continuous Monitoring Strategy

The DFC privacy continuous monitoring strategy establishes ongoing review requirements for the agency's privacy systems. The continuous monitoring strategy is a part of the "Monitor" phase of the RMF and assesses the implementation of the NIST Special Publication 800-53 controls that have privacy implications.[16] The SAOP has assigned organization-defined frequencies to the privacy controls where appropriate. To ensure an ongoing awareness of threats and vulnerabilities to the agency's privacy systems, DFC program officials and the privacy program must review and assess the privacy control implementation statements for FISMA reportable IT systems on an ongoing basis as defined in the information system security plan. For non-FISMA reportable IT systems for which a PIA is conducted, the privacy program uses the PIA as the principal tool to satisfy the requirement to assess the system's privacy controls.[17]

1.12 Privacy Training

[15] *See id.* at 9.
[16] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), 81.
[17] *See id.* at Appendix II - 17.

DFC provides annual privacy awareness training and role-based privacy training to promote privacy education and ensure that personnel understand their responsibilities to safeguard PII. Privacy awareness training provides foundational privacy training to all DFC staff and educates them on the responsibility to protect PII and comply with federal privacy law and policy in the performance of their official duties. Role-based privacy training is offered to specific employees and contractors with significant privacy roles and responsibilities, including managers, and contains privacy content that is targeted toward those roles.[18]

Annual privacy awareness and role-based privacy training are assigned to staff and tracked through FedTalent, DFC's online learning and talent management system. Each training contains a knowledge test at the end of the course that must be passed with a minimum score as well as a self-certification requirement that users must acknowledge attesting that they understand their responsibilities to protect PII. With approval from the Privacy Data Officer, individuals may also receive role-based privacy training credit for taking privacy training outside of FedTalent.

1.13 Contractors and Third Parties

In addition to employees, the Privacy Act applies to contractors who operate a system of records on behalf of the agency to accomplish an agency function.[19] DFC ensures that contractors and third parties that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of agency PII and/or operate or use agency systems containing PII comply with the mandated privacy requirements. The privacy program coordinates with the DFC Office of Administration to see that agency contracts involving contractor access to PII include the applicable Federal Acquisition Regulation (FAR) privacy clauses and other privacy provisions, as appropriate, that outline roles, responsibilities, training, incident reporting, and other privacy requirements.

The following FAR sections contain privacy conditions and may be included in DFC contracts:

- FAR Subpart 4.19: Basic Safeguarding of Covered Contractor Information Systems
- FAR Subpart 24.1: Protection of Individual Privacy

[18] *See id.* at 48.
[19] 5 U.S.C. § 552a, *The Privacy Act of 1974, as amended* (Dec. 31, 1974, amended in 1988 and 1990), Subsect. (m). "Government contractors."

- FAR Subpart 24.3: Privacy Training
- FAR Subpart 27.4: Rights in Data and Copyrights
- FAR Subpart 39.1: General
- FAR Clause 52.204-21: Basic Safeguarding of Covered Contractor Information Systems Contract Clause
- FAR Clause 52.224-1: "Privacy Act Notification"
- FAR Clause 52.224-2: "Privacy Act"
- FAR Clause 52.224-3: "Privacy Training"
- FAR Clause 52.239-1: "Privacy or Security Safeguards"

1.14 Social Security Number Reduction Plan

DFC is taking steps to eliminate the unnecessary collection, maintenance, and use of SSNs. In the past, SSNs have been widely used to identify and authenticate individuals in federal government systems. However, the threat of identity theft has rendered this practice unacceptable, resulting in government-wide requirements for agencies to evaluate and eliminate the unnecessary use of SSNs. DFC requires that program offices only collect SSNs as required by law or when no other identifier can be used to accomplish an agency function. In all other cases, the agency must replace SSNs with an alternative identifier.[20]

1.15 Privacy Breach Response

DFC has an obligation to protect the privacy of agency stakeholders. The DFC privacy breach response plan outlines roles, responsibilities, and requirements for responding to privacy incidents. All DFC staff must report a suspected or confirmed breach involving PII to the agency as soon as possible and without unreasonable delay. Staff may report incidents to the Service Desk by phone or email. Incidents can constitute any medium or form, including paper, oral, or electronic.

Once a privacy incident is reported, the agency security operations center (SOC) will coordinate with the Privacy Data Officer to conduct a preliminary investigation into the incident. If the response can be conducted at the staff level, as determined by the SAOP, then the Privacy Data Officer and/or SOC shall handle the response – including containing

[20] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), 17.

and documenting the breach, sending privacy breach notifications when necessary, and closing out the breach. If the SAOP determines that escalation is required, then details of the breach shall be sent to the breach response team for handling.

The breach response team is the group of agency officials designated by the head of the agency that may be convened to respond to a breach. The breach response team is responsible for advising the head of the agency on effectively and efficiently responding to a breach. The SAOP shall review the nature and extent of a breach to determine whether to convene the breach response team. Once convened, the SAOP is responsible for leading the breach response team.[21] At a minimum, the SAOP shall convene the breach response team when a "major incident" occurs. A breach constitutes a major incident when it involves PII that, if exfiltrated, modified, deleted, or compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification, deletion, exfiltration, or access to 100,000 or more individuals' PII always constitutes a major incident. Agencies must notify appropriate Congressional Committees of a major incident no later than seven days after the date on which the agency determined that it has reasonable basis to conclude that a major incident has occurred.[22]

The agency's breach response team includes the following DFC officials or their designees:

- SAOP
- Chief Information Officer
- Chief Information Security Officer (CISO)
- General Counsel
- Vice President, Office of External Affairs
- Vice President, Office of Administration[23]

[21] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 16.
[22] OMB Memorandum M-17-05, *Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements* (Nov. 4, 2016), 7.
[23] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 17.

1.16 SAOP FISMA Report

Each year, OMB issues guidance instructing each SAOP to review the administration of the agency's privacy program and report compliance to OMB. The SAOP FISMA report documents findings from privacy program reviews and compliance activities. It allows the agency to see what was accomplished during the fiscal year and what areas need more attention in the coming year. The privacy reporting categories that are typically included in the SAOP FISMA report are:

- General Privacy Reporting Requirements
- Information Systems
- Information Technology Systems and Privacy Impact Assessments
- Systems of Records
- Considerations for Managing PII
- Social Security Numbers
- Digital Services
- Budget and Acquisition
- Contractors and Third Parties
- Privacy Workforce Management
- Training and Accountability
- Incident Response
- Risk Management Framework
- Privacy Program Website[24]

1.17 Plans of Action and Milestones

The SAOP FISMA report serves as an annual self-assessment for the privacy program. Any metric that has not been satisfied in the report is documented in a Plan of Action and Milestones (POA&M) if not corrected after 30 days of the report due date. A POA&M is a

[24] Department of Homeland Security, *Fiscal Year 2022 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics* (Dec. 6, 2021), 3.

document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.[25] Agency POA&Ms are made available to OMB, the Department of Homeland Security, inspectors general, and the U.S. Government Accountability Office (GAO), upon request, to record and manage the mitigation and remediation of identified weaknesses and deficiencies, not associated with accepted risks, in the agency.

1.18 Independent Audits

The agency enlists the services of the DFC Office of Inspector General and/or independent, third-party auditors to conduct annual reviews of its privacy and security programs. The audit is a formal process for examining the agency's processes, records, and controls to verify compliance with laws and policy. Government auditors require evidence that controls are in place to meet key privacy requirements. The privacy program documents its operational privacy activities to provide sufficient evidence to an auditor that there are procedures in place for satisfying privacy controls and that the privacy program is following those procedures.

2.0 Structure of the Privacy Program

The privacy program is located within the Office of Information Technology (OIT) under the leadership of the CIO, who also serves as the SAOP. OIT's mission is to advance DFC's ability in driving global development impacts by providing reliable, innovative IT solutions. Its vision is to become an agile IT enterprise that adapts quickly to new technology and industry standards, enabling secure, innovative, cost-efficient support to DFC customers. The Privacy Data Officer reports to the SAOP on all privacy program matters. Within OIT, the privacy program works closely with collateral offices, notably the CISO team, to address all areas specific to the implementation and compliance of NIST privacy and security controls.

3.0 Resources Dedicated to the Privacy Program

The SAOP is responsible for assigning and allocating sufficient resources to implement and operate the DFC privacy program. In addition to the SAOP, DFC employs a full-time

[25] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (Oct. 17, 2001), "What is a POA&M?"

Privacy Data Officer who is responsible for managing daily privacy program functions and facilitating privacy compliance activities. The Privacy Data Officer works collaterally with other DFC personnel as needed to satisfy statutory and policy requirements associated with managing privacy for the agency. To that end, the SAOP identifies and plans for the resources needed to operate the privacy program and engages with members of DFC's executive leadership team to review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. This includes planning and budgeting to upgrade, replace, or retire any information systems that maintain PII for which protections commensurate with risk cannot be effectively implemented.[26]

4.0 Role of the SAOP and Privacy Data Officer

The head of the agency is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the agency. To ensure that agencies effectively carry out the privacy-related functions described in law and OMB policies, Executive Order 13719 requires the head of each agency to designate an SAOP who has agency-wide responsibility and accountability for the agency's privacy program.[27] The SAOP delegates daily DFC privacy program management functions to the Privacy Data Officer.

4.1 Senior Agency Official for Privacy

The SAOP has agency-wide responsibility and accountability for the agency's privacy program, including implementation of privacy protections; compliance with federal privacy laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. The SAOP's responsibilities include:

- Policy Making: The SAOP has a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals that have privacy implications. In this role, the SAOP ensures that the agency considers

[26] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), Appendix I - 4.
[27] Executive Order 13719, *Establishment of the Federal Privacy Council* (Feb. 9, 2016), Sec. 3. "Responsibilities of Agency Heads."

and addresses the privacy implications of all agency regulations and policies, and leads the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular No. A-19.

- Compliance: The SAOP has a central role in overseeing, coordinating, and facilitating the agency's privacy compliance efforts. In this role, the SAOP ensures that the agency complies with applicable privacy requirements in law, regulation, and policy.
- Risk Management: The SAOP manages privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. The SAOP's review of privacy risks begins at the earliest planning and development stages of agency actions and policies that involve PII, and continues throughout the life cycle of the programs or information systems.[28]

4.2 Privacy Data Officer

The Privacy Data Officer manages daily privacy program functions and possesses the requisite subject matter expertise to oversee privacy compliance activities and ensure the implementation of privacy policy and requirements. The Privacy Data Officer's responsibilities include:

- Leading the day-to-day operations of implementing the privacy program
- Identifying and assessing privacy risks in agency programs, systems, and initiatives by reviewing or conducting PTAs and PIAs
- Maintaining the agency's inventory of SORNs and developing, approving, and submitting privacy notices for OMB approval and publication in the *Federal Register*
- Overseeing agency privacy incident/breach reporting, response, notification, and remediation activities
- Managing agency-wide privacy awareness training and role-based privacy training
- Assessing metrics and submitting privacy reports to appropriate federal entities, such as the annual SAOP FISMA report to OMB

[28] OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016), 3.

- Addressing all privacy areas specific to the implementation of the NIST SP 800-53 privacy controls for ATO systems
- Serving as the DFC point of contact for privacy matters that require coordination within OIT, agency stakeholders, as well as the external community. This includes coordinating all privacy matters across departmental boundaries with physical security, legal counsel, auditors, business units, and external agencies, as appropriate
- Developing, implementing, managing, and executing all information security projects associated with managing and protecting DFC privacy information within DFC's primary network (DFCNet), to include on-premise and cloud-based systems/applications

5.0 Strategic Goals and Objectives of the Privacy Program

DFC has established five strategic goals and created specific and measurable objectives for achieving those goals:

Goal 1. Foster a culture of privacy compliance through governance, policy, and partnerships.

- Objective 1.1 – Develop policy and issue guidance related to privacy laws, policy, and standards
- Objective 1.2 – Develop templates, forms, and tools to meet requirements under federal privacy laws, the FIPPs, and DFC privacy policy
- Objective 1.3 – Implement and maintain agency-wide processes, standards, and policies to ensure appropriate safeguards are in place to protect privacy and the confidentiality, integrity, and availability of federal information and information systems
- Objective 1.4 – Cultivate and maintain a privacy leadership role

Goal 2. Provide outreach, education, and training to promote privacy and transparency.

- Objective 2.1 – Provide policy and compliance leadership to DFC privacy officials, Privacy Act system managers, information system owners, information owners,

information system security officers, and other information management or technology officials

- Objective 2.2 – Develop and deliver annual privacy awareness training and role-based privacy training
- Objective 2.3 – Maintain a DFC privacy program website to promote transparency, provide DFC SORNs and PIAs, and disseminate information about DFC programs, operations, systems, and policies in a manner that is easily accessible to the public
- Objective 2.4 – Report to OMB and other oversight bodies to further the DFC privacy program mission

Goal 3. Manage an agency-wide compliance and oversight program to ensure compliance with Federal privacy laws and policies that promotes and adheres to the FIPPs.

- Objective 3.1 – Conduct compliance reviews on existing DFC programs, systems, projects, information sharing arrangements, and other initiatives to evaluate privacy and provide guidance to reduce impact on privacy and ensure compliance
- Objective 3.2 – Work within DFC governance structures to ensure that general policies, guidance, and templates comply with DFC privacy requirements, and privacy is protected when information is to be shared with the public and private sector
- Objective 3.3 – Ensure that DFC provides the maximum disclosure permitted by law in response to Privacy Act requests
- Objective 3.4 – Coordinate DFC efforts to ensure that privacy complaints are processed efficiently, redress is provided as appropriate, and deficiencies are remedied

Goal 4. Implement and oversee privacy breach response activities and risk mitigation policies.

- Objective 4.1 – Develop and maintain breach response policies and procedures to ensure proper reporting, investigation, and escalation of breaches of PII, and coordinate DFC responses to breaches to ensure appropriate response and mitigation activities are conducted in accordance with federal and DFC policy

- Objective 4.2 – Evaluate office programs, systems, and initiatives to identify potential privacy implications, and work with agency officials to implement controls to manage privacy risk and prevent privacy breaches
- Objective 4.3 – Develop strategies to mitigate privacy risk, including agency-wide efforts to eliminate or reduce the collection and use of SSNs and other PII to reduce potential risk to individuals
- Objective 4.4 – Establish procedures to hold tabletop exercises annually to test breach response policy and procedures, identify gaps or weaknesses, and to ensure breach response teams understand roles and responsibilities for reporting, responding to, and escalating a breach

Goal 5. Develop and maintain a privacy workforce of skilled professionals to build an effective enterprise-wide privacy program

- Objective 5.1 – Develop privacy competencies and identify associated workforce training and career paths
- Objective 5.2 – Support employee development and emphasize the role of training and professional development in performance planning, create opportunities for cross training and learning, and encourage transparent information sharing and collaboration between the DFC privacy program and other teams
- Objective 5.3 – Reward exceptional employee performance and recognize individual contributions to advancing the office mission
- Objective 5.4 – Develop workforce planning and succession strategies to ensure continuity of operations and to ensure that the DFC privacy program is strategically situated to successfully meet the growing challenges of the federal privacy community

6.0 Program Management Controls and Common Controls

DFC employs numerous controls from NIST SP 800-53 for meeting applicable privacy requirements and managing risks. For privacy controls, the SAOP is responsible for designating which controls the agency will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and are essential for

managing the agency's privacy program. Program management controls are distinct from common, information system-specific, and hybrid controls because program management controls are independent of any particular information system.[29]

The following sections list the privacy program management controls and common controls as designated by the SAOP from NIST SP 800-53, Revision 5. For ATO systems, the information system security officer maintains implementation statements for each of the privacy controls in the information system security plan. Although the following controls are currently designated as "privacy" controls, the privacy program may determine that certain controls should be added, removed, transferred, or modified based on the specific system that is being assessed and/or agency resources that can be dedicated toward implementing the control.

6.1 Program Management Controls

FISMA, the Privacy Act, and OMB Circular No. A-130 require federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal information systems and to protect individual privacy. The Program Management (PM) controls have been designed to facilitate organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards.[30]

Within the PM control family, DFC's privacy program management controls are:

- PM-3: Information Security and Privacy Resources
- PM-4: Plan of Action and Milestones Process
- PM-5: System Inventory
    - PM-5.1: Inventory of Personally Identifiable Information
- PM-6: Measures of Performance
- PM-7: Enterprise Architecture

[29] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (Jul. 28, 2016), Appendix II - 15.
[30] NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 23, 2020), 203.

- PM-8: Critical Infrastructure Plan
- PM-9: Risk Management Strategy
- PM-10: Authorization Process
- PM-11: Mission and Business Process Definition
- PM-13: Security and Privacy Workforce
- PM-14: Testing, Training, and Monitoring
- PM-17: Protecting Controlled Unclassified Information on External Systems
- PM-18: Privacy Program Plan
- PM-19: Privacy Program Leadership Role
- PM-20: Dissemination of Privacy Program Information
    - PM-20.1: Privacy Policies on Websites, Applications, and Digital Services
- PM-21: Accounting of Disclosures
- PM-22: Personally Identifiable Information Quality Management
- PM-24: Data Integrity Board
- PM-25: Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- PM-26: Complaint Management
- PM-27: Privacy Reporting
- PM-28: Risk Framing
- PM-31: Continuous Monitoring Strategy

6.2 Common Controls

The privacy program identifies which controls from NIST SP 800-53 will be designated as "common" privacy controls. Common controls are "inherited" by information systems or applications during the Assessment and Authorization process for ATO systems. This

means that the controls are implemented by entities other than those responsible for the system or application.[31]

DFC's privacy common controls are:

- Access Control (AC)
    - AC-1: Policy and Procedures
- Awareness and Training (AT)
    - AT-1: Policy and Procedures
    - AT-2: Literacy Training and Awareness
    - AT-3: Role-Based Training
        - AT-3.5: Processing Personally Identifiable Information
- Assessment, Authorization, and Monitoring (CA)
    - CA-1: Policy and Procedures
- Configuration Management (CM)
    - CM-1: Policy and Procedures
- Incident Response (IR)
    - IR-1: Policy and Procedures
    - IR-2: Incident Response Training
        - IR-2.3: Breach
    - IR-3: Incident Response Testing
    - IR-4: Incident Handling
    - IR-5: Incident Monitoring
    - IR-6: Incident Reporting
    - IR-7: Incident Response Assistance

[31] NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 23, 2020), 12.

- IR-8: Incident Response Plan

- Media Protection (MP)
  - MP-1: Policy and Procedures
  - MP-6: Media Sanitization
- Physical and Environmental Protection (PE)
  - PE-8: Visitor Access Records
    - PE 8.3: Limit Personally Identifiable Information Elements
- Planning (PL)
  - PL-1: Policy and Procedures
  - PL-4: Rules of Behavior
    - PL-4.1: Social Media and External Site/Application Usage Restrictions
  - PL-9: Central Management
- Program Management (PM)
  - PM-8: Critical Infrastructure Plan
  - PM-9: Risk Management Strategy
  - PM-13: Security and Privacy Workforce
  - PM-14: Testing, Training, and Monitoring
- Personnel Security (PS)
  - PS-6: Access Agreements
- Personally Identifiable Information Processing and Transparency (PT)
  - PT-1: Policy and Procedures
- Risk Assessment (RA)
  - RA-1: Policy and Procedures
- System and Services Acquisition (SA)

- SA-1: Policy and Procedures
- SA-2: Allocation of Resources
- SA-3: System Development Life Cycle
- SA-4: Acquisition Process
- SA-11: Developer Testing and Evaluation

- System and Information Integrity (SI)
  - SI-1: Policy and Procedures