Office of Information Technology (OIT)

Breach Response Plan

November 10, 2022

Table of Contents

1.0 Overview

1.1 Purpose

The purpose of the U.S. International Development Finance Corporation (DFC) breach response plan is to provide procedures for effectively and efficiently responding to a breach. This plan includes information on:

- Reporting a suspected or confirmed breach
- Breach response team
- Identifying applicable privacy compliance documentation
- Information sharing to respond to a breach
- Reporting requirements
- Assessing the risk of harm to individuals potentially affected by a breach
- Mitigating the risk of harm to individuals potentially affected by a breach
- Notifying individuals potentially affected by a breach[1]

1.2 Background

The Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, requires agencies to develop a breach response plan to ensure that the agency is prepared to respond to a breach. The breach response plan is a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach. It is specifically tailored to the agency and addresses the agency's mission, size, structure, and functions. The breach response plan is part of the agency's formal incident response plan.[2]

1.3 Agency Mission

DFC is America's development finance institution. The Better Utilization of Investments Leading to Development (BUILD) Act of 2018 established DFC to "facilitate the participation of private sector capital and skills in the economic development of countries

[1] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 15.
[2] NIST Special Publication 800-61, *Computer Security Incident Handling Guide* (Aug. 6, 2012), 8.

with low- or lower-middle-income economies and countries transitioning from nonmarket to market economies in order to complement U.S. assistance and foreign policy objectives." DFC partners with the private sector to finance solutions to the most critical challenges facing the developing world today. DFC invests across sectors including energy, healthcare, critical infrastructure, and technology. DFC also provides financing for small businesses and women entrepreneurs in order to create jobs in emerging markets. DFC investments adhere to high standards and respect the environment, human rights, and worker rights.

DFC makes America a stronger and more competitive leader on the global development stage with greater ability to partner with allies on transformative projects. Further, DFC provides the developing world with financially sound alternatives to unsustainable and irresponsible state-directed initiatives.

1.4 Agency Functions

DFC's financial tools help mobilize investment across the developing world. DFC offers loans, loan guarantees, equity investments, political risk insurance, technical assistance, and feasibility studies to drive significant amounts of private capital into challenging developing markets to address local needs. DFC's offerings mobilize government and private resources to support key sectors such as infrastructure, energy, water, and health.

DFC's equity authority allows it to play a new and catalytic role in mobilizing private sector capital to achieve developmental and strategic outcomes. Equity investing in funds makes DFC a more attractive partner to other development finance institutions and expands impact. DFC's technical assistance program also mobilizes private capital by providing grant funding to develop projects and help make them bankable.[3]

1.5 Agency Size and Structure

DFC is considered a medium independent agency[4] with a workforce size of over 400 employees. DFC is led by its Chief Executive Officer (CEO), with oversight from its Board of Directors, Development Advisory Council, Office of Accountability, and Office of Inspector General.

[3] DFC, *U.S. International Development Finance Corporation Strategic Plan FY 2022-2026* (https://www.dfc.gov/sites/default/files/media/documents/20220923%20DFC%20Strategic%20Plan.pdf) (n.d.), 4.
[4] OPM, *Open Government Data* (https://www.opm.gov/about-us/open-government/Data/Apps/Agencies/index.aspx) (n.d.). Medium independent agencies contain 100-999 employees.

The DFC organizational chart is shown in Figure 1.

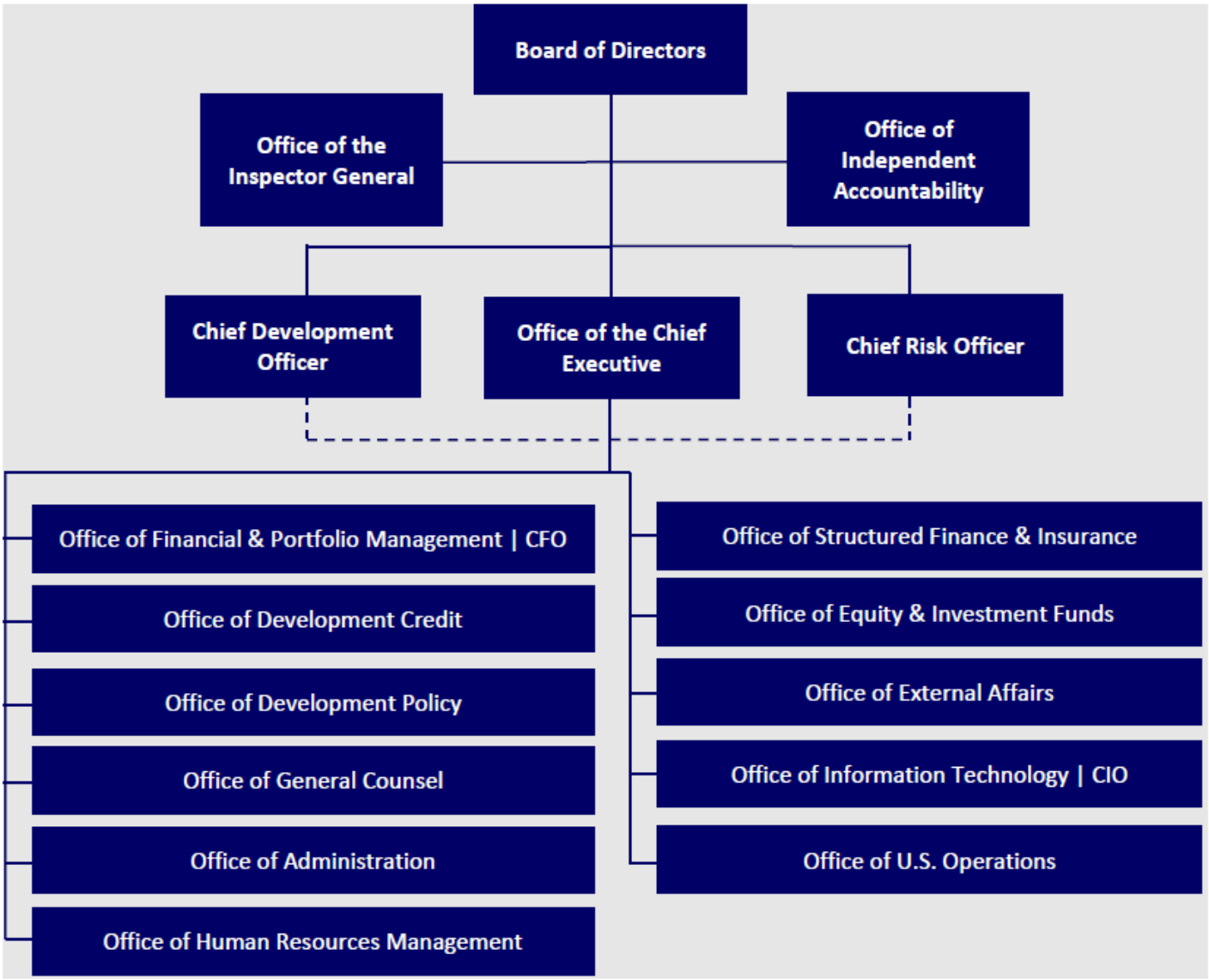

Figure 1: DFC Organization Chart[5]

2.0 Reporting a Suspected or Confirmed Breach

2.1 Definition of a Breach

[5] *DFC Annual Management Report Fiscal Year 2021* (https://www.dfc.gov/sites/default/files/media/documents/DFC%20Annual%20Management%20Report%20FY%202021.pdf) (Sept. 30, 2021), 2.

The guidance set forth in this breach response plan applies to a "breach," which is a type of "incident."

- **Definition of an Incident:** *An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*
- **Definition of a Breach:** *The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.*

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses personally identifiable information (PII)[6] by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for an other than authorized purpose. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen
- An email containing PII is inadvertently sent to the wrong person
- A box of documents with PII is lost or stolen during shipping

[6] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 8. The term PII refers to 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.

- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or federal benefits
- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual
- An IT system that maintains PII is accessed by a malicious actor
- PII that should not be widely disseminated is posted inadvertently on a public[7]

2.2 Reporting a Breach

Any DFC employee or contractor who becomes aware of a suspected or confirmed breach must report it as soon as possible and without unreasonable delay to the security operations center (SOC) at ServiceDesk@dfc.gov or (202) 336-8600. This includes a breach in any medium or form, including paper, oral, and electronic.[8] The DFC Privacy Breach Reporting Form (Appendix I) provides a template for the information that should be included, if possible, when reporting a breach. If a DFC employee or contractor is uncertain of whether a breach occurred, he or she should still notify the SOC as soon as possible so that the incident may be investigated. If a breach has occurred, the SOC may be able to prevent PII from being further compromised and, in some cases, reduce the risk of harm to potentially affected individuals.

There shall be no negative consequences or penalties associated with an individual's good faith reporting of a suspected or confirmed breach. Therefore, all suspected breaches should be reported to the SOC without condition or delay, even if the suspected breach is unable to be confirmed at the time of discovery.

2.3 Determination of Whether a Breach Has Occurred

To determine if PII has been compromised, the agency will take the following measures, if applicable:

1. Consult with the Chief Information Security Officer (CISO) team to review information technology (IT) system logs to determine access history for records containing PII

[7] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 9.
[8] *See id.* at 14.

2. Contact any potentially unauthorized viewer of PII and the individual who notified DFC of the suspected or confirmed breach to obtain additional information regarding the breach or potential breach

3. Conduct a review of the records in question to determine if PII was contained in those records and, if so, the types of PII contained

In determining whether a breach has or may have occurred, the SOC and/or privacy lead shall gather information from various sources, including information from: 1) any affected DFC staff, 2) paper and electronic documentation, and 3) external parties outside of DFC. The SOC and/or privacy lead shall make the determination by analyzing whether there was a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an unauthorized user accesses or potentially accesses PII for an other than authorized purpose.

2.4 Tracking and Documenting the Response to a Breach

The SOC maintains a formal process to track and document each breach reported to the agency. As part of the agency's formal process for internally tracking and documenting a response to a breach, the agency shall complete the DFC Privacy Breach Reporting Form (Appendix I) and maintain it as part of their internal documentation for each privacy breach. The form may be completed by the person who reported the breach, the SOC, the privacy lead, or any other person who is able to accurately describe the breach. The form includes examples of data elements and information types that can be used to distinguish or trace an individual's identity, either alone or when combined with any other information that is linked or linkable to a specific individual.

The process for internally tracking each reported breach shall allow the agency to track and monitor the following:

- The total number of breaches reported over a given period of time
- The status for each reported breach, including whether the agency's response to a breach is ongoing or has concluded
- The number of individuals potentially affected by each reported breach
- The types of information potentially compromised by each reported breach

- Whether the agency, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach
- Whether the agency, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach
- Whether a breach was reported to U.S. Computer Emergency Readiness Team (US-CERT) and/or Congress[9]

At the end of each quarter of the fiscal year, the SOC will provide a report to the SAOP detailing the status of each breach reported to the SOC during the fiscal year. The SAOP shall review the report and validate that the report accurately reflects the status of each reported breach.[10]

3.0 Breach Response Team

OMB Memorandum M-17-12 instructs the head of the agency to designate a group of officials that may be convened to respond to a breach. The DFC 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.[11] 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.

DFC 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

[9] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 34.
[10] *See id.* at 35.
[11] *See id.* at 16.

conclude that a major incident has occurred. The specific Congressional Committees include:

- House of Representatives:
    - Committee on Oversight and Government Reform
    - Committee on Homeland Security
    - Committee on Science, Space, and Technology
    - Committee on the Judiciary
- Senate:
    - Committee on Homeland Security and Governmental Affairs
    - Committee on Commerce, Science, and Transportation
    - Committee on the Judiciary
- Appropriate authorization and appropriation committees of Congress[12]

When an agency reports a breach to Congress, the breach response team shall formally review the agency's response to the breach and identify any lessons learned. The agency shall use lessons learned to implement specific, preventative actions. The agency shall document any changes to its breach response plan, policies, training, or other documentation resulting from lessons learned. If there are specific challenges preventing DFC from instituting remedial measures, the agency shall also document those challenges. [13]

3.1 Breach Response Team Designation

The CEO has designated the following DFC officials, or their designees, to comprise the DFC breach response team:

- Senior Agency Official for Privacy (SAOP)
- Chief Information Officer (CIO)
- Chief Information Security Officer

[12] OMB Memorandum M-22-05, *Fiscal Year 2021 – 2022 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 6, 2021), 11.
[13] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 35.

- General Counsel
- Vice President, Office of External Affairs
- Vice President, Office of Administration

3.2 Roles and Responsibilities

The DFC breach response team's roles and responsibilities when responding to a breach are described below:

- **Senior Agency Official for Privacy***
    - Determine whether the response to a breach can be conducted at the staff level or whether to convene the breach response team
    - Identify the applicable privacy documentation for the potentially impacted information and information system
    - *Note: The SAOP may delegate any responsibility assigned to the role of SAOP in this breach response plan to the privacy lead or others as appropriate
- **Chief Information Officer**
    - Determine the technical support required to respond to a breach
    - Determine whether outside assistance is required to respond to a breach
- **Chief Information Security Officer**
    - Lead the SOC in handling and reporting computer security incidents
    - Coordinate with the privacy lead on incidents that involve PII
    - Assess the implementation and effectiveness of security safeguards in protecting agency data
- **General Counsel**
    - Determine the legal support required to respond to a breach
    - Review privacy breach notification letters when assistance is requested by the SAOP
- **Vice President, Office of External Affairs**

- Notify appropriate Congressional Committees of a major incident no later than seven days after the agency has determined that it has a reasonable basis to conclude that a major incident has occurred
- Coordinate agency responses to media inquiries regarding a breach

- **Vice President, Office of Administration**
  - Determine whether the breach involved physical security
  - Provide adequate physical security for DFC facilities and office space

3.3 Tabletop Exercises

The SAOP shall periodically, but not less than annually, convene the agency's breach response team to hold a tabletop exercise. The purpose of the tabletop exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing breach response plans is an essential part of risk management and breach response preparation. Tabletop exercises will be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in an agency's response capabilities.[14]

4.0 Identifying Applicable Privacy Compliance Documentation

When responding to a breach, the SAOP lead shall identify all applicable privacy compliance documentation for the potentially impacted information or information system. This includes identifying which System of Records Notice (SORN), Privacy Impact Assessment (PIA), and privacy notices apply to the potentially compromised information. In order to do this, the privacy lead should determine what information and information system(s) were affected and review the privacy compliance documentation relevant to those information and information system(s) for the following:

- The information that was potentially compromised
- The purpose of the information
- The permitted uses and disclosures of the information

[14] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 35.

- Any other relevant information to assist in developing a breach response

When reviewing privacy compliance documentation in response to a breach, the SAOP shall additionally consider:

- If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how will the agency account for the disclosure?
- If additional PII is necessary to contact or verify the identity of the individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?
- Are the relevant SORNs, PIAs, and privacy notices accurate and up-to-date?[15]

4.1 Privacy Threshold Analysis

The PTA is a questionnaire that is used to determine whether a program, project, information collection, or information system (hereinafter, referred to as "system") 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

[15] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 18.

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

4.2 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.[16]

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 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 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 information relates to internal government operations, has previously been assessed under an evaluation similar to a PIA, or where privacy issues are unchanged.[17]

4.3 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

[16] 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."
[17] *See id.* at Sec. II.B. "Privacy Impact Assessment: When to conduct a PIA."

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

4.4 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 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.[18] The Privacy Act does not apply to deceased persons, corporations and organizations, and non-citizens or non-lawful permanent residents.[19]

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.[20]

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.[21] If there is no established system of records, retrieval by personal identifiers is prohibited.

4.5 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 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:

[18] 5 U.S.C. § 552a, *The Privacy Act of 1974, as amended* (Dec. 31, 1974, amended in 1988 and 1990), Subsect. (a). "Definitions."
[19] 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.
[20] *See id.* at 11-12.
[21] OMB Circular No. A-108, *Federal Agency Responsibilities for Reviewing, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016), 5.

1) Authority: The legal authority to collect the information as provided by a federal statute or executive order

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[22]

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.[23]

5.0 Information Sharing to Respond to a Breach

When responding to a breach, the agency may need additional information to reconcile or de-duplicate records, identify potentially affected individuals, or obtain contact information in order to provide notification. Accordingly, the agency may need to combine information maintained in different information systems within the agency, share information between agencies, or share information with a non-federal agency.

When contemplating the potential information sharing that may be required in response to a breach, the SAOP shall consider the following:

- Would the information sharing be consistent with existing or require new data use agreements, information exchange agreements, or memoranda of understanding?
- How will PII be transmitted and protected when in transmission, for how long will it be retained, and may it be shared with third parties?[24]

To facilitate DFC's response to a breach of its own records, the following routine use will be included in each of the agency's SORNs:

---

[22] OMB Circular No. A-108, *Federal Agency Responsibilities for Reviewing, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016), 13.
[23] NIST Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept 23, 2020), 233.
[24] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 18.

> *To appropriate agencies, entities, and persons when (1) DFC suspects or has confirmed that there has been a breach of the system of records; (2) DFC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DFC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DFC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.*

Additionally, DFC may have records in its systems of records that could assist another agency in its efforts to respond to a breach. This may include information that would assist the other agency in locating or contacting individuals potentially affected by a breach, or information that is related to the other agency's programs or information. To ensure that DFC is able to disclose records in its systems of records that may reasonably be needed by another agency in responding to a breach, the following routine use will be included in each of DFC's SORNs:

> *To another Federal agency or Federal entity, when DFC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.*[25]

6.0 Reporting Requirements

OMB Memorandum M-16-03 requires each federal agency to designate a principal SOC to be accountable for all incident response activities for the respective agency.[26] The SOC is led by the CISO and is comprised of members from the CISO team.

6.1 Reporting to US-CERT

[25] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 11.
[26] OMB Memorandum 16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements* (Oct. 30, 2015), 11.

The SOC shall notify the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) of a breach consistent with the agency's incident management policy and US-CERT notification guidelines. In accordance with US-CERT notification guidelines, agencies must report information security incidents where the confidentiality, integrity, or availability of a federal information system is potentially compromised within one hour of being identified by the SOC.[27] OMB Memorandum M-15-01 requires federal agencies to notify US-CERT of all cyber-related (electronic) incidents with confirmed loss of confidentiality, integrity, or availability within one hour of reaching the SOC or IT department.[28] In some cases, it may not be feasible to have complete and validated information prior to reporting, but agencies should provide their best estimate at the time of notification and report updated information as it becomes available. Events that have been found by the reporting agency not to impact confidentiality, integrity, or availability may be reported voluntarily to US-CERT but may not be included in the Federal Information Security Modernization Act (FISMA) annual report to Congress.[29]

6.2 Reporting to Law Enforcement, the Inspector General, and General Counsel

When responding to a breach, the SAOP shall ensure that law enforcement, the Office of the Inspector General, and/or General Counsel receive timely notification when notification is appropriate. The SAOP shall also consider and advise appropriate officials on whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.

When a breach warrants a report to law enforcement, the agency shall ensure that the report occurs promptly, even if the breach is unconfirmed or the circumstances are still unclear. Prompt referral to law enforcement can prevent PII from being further compromised[30]

6.3 Reporting to Congress

[27] Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines* (https://www.cisa.gov/uscert/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf) (Apr. 1, 2017), 1.
[28] OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (Oct. 3, 2014), 12.
[29] Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines* (https://www.cisa.gov/uscert/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf) (Apr. 1, 2017), 1.
[30] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 19.

The agency shall notify the appropriate Congressional Committee pursuant to FISMA no later than seven days after the date on which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. In addition, the agency shall also supplement its initial seven-day notification to Congress with a report no later than 30 days after the agency discovers the breach. This notification shall be consistent with FISMA and OMB guidance on reporting a breach to Congress. The SAOP and/or Office of External Affairs shall be responsible for notifying Congress.

7.0 Assessing the Risk of Harm to Individuals Potentially Affected by a Breach

In order to properly escalate and tailor breach response activities, the SAOP, in coordination with the breach response team when applicable, shall conduct and document an assessment of the risk of harm to individuals potentially affected by a breach. This assessment shall by documented in the DFC Privacy Breach Reporting Form. The assessment of the risk of harm will include an analysis of: (1) the nature and sensitivity of the PII potentially compromised by the breach, (2) the likelihood of access and use of PII, and (3) the type of breach.

When assessing the risk of harm to individuals potentially affected by a breach, the SAOP shall consider the potential harms that could result from the loss or compromise of PII. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

Additionally, the Privacy Act requires the agency to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

The agency will consider any and all risks relevant to the breach, which may include risks to the agency, agency information systems, agency programs and operations, the federal government, or national security. Those additional risks may properly influence the agency's overall response to a breach and the steps the agency should take to notify individuals.

7.1 Nature and Sensitivity of the PII Compromised by the Breach

The SAOP shall consider the following when assessing the nature and sensitivity of PII potentially compromised by a breach:

7.1.1 Data Elements

When considering the nature and sensitivity of PII involved in a suspected or confirmed breach, the SAOP shall evaluate the sensitivity of each individual data element. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. These data elements include but are not limited to: Social Security number (SSN), passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers.

In addition to evaluating the sensitivity of each data element, the SAOP shall also evaluate the sensitivity of all the data elements together. Sometimes multiple pieces of information, none of which is particularly sensitive in isolation and would not present a risk of harm to the individual, may present an increased risk of harm to the individual when combined. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

When assessing the nature and sensitivity of potentially compromised PII, the SAOP will not limit the scope of the evaluation to the sensitivity of the information involved in the breach. The SAOP will also consider the information that may have been potentially compromised in a previous breach, as well as any other available information that when combined with the information may result in an increased risk of harm to the individuals.

7.1.2 Context

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider the context. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about individuals. For example, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a law enforcement agency is sensitive information. Similarly, the same list of names and associated phone numbers on a list of individuals along with information about a medical condition is also sensitive.

7.1.3 Private Information

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall evaluate the extent to which the PII constitutes information that an individual would generally keep private. Such "private information" may not present a risk of identity theft or criminal conduct but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include: derogatory personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy-related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, and immigration status. Passwords are another example of private information that if involved in a breach may present a risk of harm.

7.1.4 Vulnerable Populations

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider whether the potentially affected individuals are from a particularly vulnerable population that may be at a greater risk of harm than the general population. Potentially vulnerable populations include but are not limited to: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking. This is not a comprehensive list and other populations may also be considered vulnerable.

7.1.5 Permanence

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual's health insurance ID number can be replaced. However, information about an individual's health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as the lives of his or her family members.

Special consideration is warranted when a breach involves biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, the agency may factor

in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.[31]

7.2 Likelihood of Access and Use of PII

The agency shall consider the following when assessing the likelihood of access and use of PII potentially compromised by a breach:

7.2.1 Security Safeguards

When assessing the likelihood of access and use of PII potentially compromised by a breach, the CIO shall evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive. The CIO shall consider each of the employed security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources toward overcoming those safeguards.

When evaluating the likelihood of access and use of encrypted PII potentially compromised by a breach, the CIO, in coordination with the SAOP and CISO, shall confirm:

- Whether encryption was in effect
- The degree of encryption
- At which level the encryption was applied
- Whether decryption keys were controlled, managed, and used

There are many ways to encrypt information and different technologies provide varying degrees of protection. Encryption can be applied at the device-level, file-level, and to information at rest or in transmission.

The protection provided by encryption may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised.

Federal agencies are required to use a National Institute of Standards and Technology (NIST)-validated encryption method. The SAOP shall consult with the agency's CISO and

[31] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 22-23.

other technical experts, as appropriate, to ascertain whether information was properly encrypted.[32]

The PII potentially compromised by a breach may also be rendered partially or completely inaccessible by security safeguards other than encryption. This may include redaction, data masking, and remote wiping[33] of a connected device. Physical security safeguards, such as a locked case securing documents or devices, may also reduce the likelihood of access and use of PII. For example, PII in a briefcase left temporarily unattended is less likely to have been accessed and used if the briefcase were securely locked.

7.2.2 Format and Media

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP, in coordination with the CIO, shall evaluate whether the format or media of the PII may make its use difficult and resource-intensive. The format of the PII or media on which it is maintained may make the PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable USB flash drive does not require any special skill or knowledge to access and an unauthorized user could quickly search for specific data fields such as a nine-digit SSN. Conversely, a magnetic tape cartridge used for backing up servers that is one of a set of 30 and contains a large volume of unstructured PII would require special expertise and equipment to access and use the information.

The SAOP shall also consider the type, value, or sensitivity of the PII. If the PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. This is because the value of the information may outweigh the difficulty and resources needed to access the information.

7.2.3 Duration of Exposure

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP shall consider the amount of time that the PII was exposed. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users. For example, a briefcase containing PII left in a hotel lobby for an hour before being recovered is less likely to have been accessed by an unauthorized user than if it had been left for three days prior to being recovered. Similarly, PII inadvertently published to a public Internet page for an hour before being removed is less likely to have been

[32] NIST Special Publication 140, *Security Requirements for Cryptographic Modules* (Mar. 22, 2019), iv.
[33] NIST Special Publication 800-124, Rev. 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (Mar. 24, 2020), 21.

accessed by an unauthorized user than if it had been available on the public Internet page for a week.

7.2.4 Evidence of Misuse

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP shall determine whether there is evidence of misuse. In some situations, an agency may be able to determine with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach of that PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, agencies may determine with reasonable certainty that the PII will not be misused. For example, a forensic analysis of a recovered device may reveal that the PII was not accessed.[34]

7.3 Type of Breach

The SAOP shall consider the following when determining the type of breach:

7.3.1 Intent

When assessing the risk of harm to individuals potentially affected by a breach, the SAOP shall consider whether the breach was intentional, unintentional, or whether the intent is unknown. If a breach was intentional, the SAOP should determine whether the information was the target, or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional breach include the theft of a device storing PII from a car or office, the unauthorized intrusion into a government network that maintains PII, or an employee looking up a celebrity's file in an agency database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

The risk of harm to individuals may be lower when a breach unintentional, either by user error or sometimes by failure to comply with agency policy. However, that is not always the case, and breach response officials must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional breach include an employee accidentally emailing another employee's PII to the wrong email address or a contractor storing

[34] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 23-26.

personnel files in a shared folder that the contractor thought was access-controlled but that actually was not.

In many circumstances, the SAOP may be unable to determine whether a breach was intentional or unintentional. In these instances, the SAOP shall consider the possibility that the breach was intentional. For example, if an employee realizes her mobile device is missing, it may be that it was stolen intentionally or that she dropped it accidentally. Similarly, a shipment of files containing PII that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

In circumstances where an agency has notified law enforcement of a breach, the SAOP shall consider any relevant information provided to the agency by law enforcement that may help inform whether the breach was intentional or unintentional.

7.3.2 Recipient

In some cases, the agency may know who received the PII. This information, when available, may help the SAOP assess the likely risk of harm to individuals. For example, a breach is often reported by a recipient who receives information he or she should not have. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another employee within the agency's IT network. One common type of low-risk breach is when an employee sends an individual's PII via email to another employee at the same agency who does not need to know that PII for his or her duties. In many cases, it may be reasonable to conclude that there is a negligible risk of harm. Even where PII is inadvertently sent to an individual outside an agency, the risk of harm may be minimal if it is confirmed that, for example, the individual is known to the agency, acknowledged receipt of the PII, did not forward or otherwise use the PII, and the PII was properly, completely, and permanently deleted by the recipient. This is a breach that must be reported within the agency and appropriately responded to, but the risk of harm is low enough that the response often does not necessitate that the agency notify or provide services to the individual whose PII was compromised.

Conversely, if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher. In many cases, an agency will not have any information

indicating that compromised or lost PII was ever received or acquired by anyone. In such circumstances, the SAOP shall rely upon the other factors set forth in this section.[35]

8.0 Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach

Once the SAOP assesses the risk of harm to individuals potentially affected by a breach, the SAOP, in coordination with the breach response team when applicable, shall consider how best to mitigate the identified risks. The SAOP, in coordination with the breach response team when applicable, is responsible for advising the head of the agency on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to offer guidance or provide services to individuals will depend on the circumstances of the breach. When deciding whether or not to offer guidance or provide services to potentially affected individuals, agencies shall consider the assessed risk of harm conducted as described in section 7.0 of this privacy breach response plan. The assessed risk of harm to individuals shall inform the agency's decision of whether or not to offer guidance or provide services. The head of the agency is ultimately responsible for making final decisions regarding whether to offer guidance or provide services to individuals potentially affected by a breach.

The SAOP shall determine and document the actions that the agency will take to mitigate the risk of harm. These actions can include:

8.1.1 Countermeasures

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the agency shall consider the countermeasures it can take. Countermeasures may not always prevent harm to potentially affected individuals but may limit or reduce the risk of harm. For example, if credit card information is potentially compromised, the agency may proactively notify appropriate banks so they can monitor the associated accounts or reissue the lines of credit using new accounts. If the information is only useful in a specific context, there may be context-specific countermeasures that can be taken to limit the risk of harm. For example, if information related to disability beneficiaries is potentially compromised, the agency may consider monitoring beneficiary databases for unusual activity that may signal fraudulent activity, such as a sudden request for a change of

[35] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 26-27.

address. Similarly, if individuals' passwords are potentially compromised in a breach, the agency should require those users to change their passwords.

8.1.2 Guidance

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall consider what guidance to provide to those individuals about how they may mitigate their own risk of harm. There are several steps individuals can take to mitigate their own risk of harm resulting from a breach. These steps including setting up fraud alerts or credit freezes, changing or closing accounts, and taking advantage of services made available by the Federal Trade Commission (FTC). The guidance will necessarily depend on the potentially compromised information. Agencies should use the information available at www.IdentityTheft.gov/databreach as the baseline when drafting guidance. The FTC provides specific guidance for when a breach involves SSNs, payment card information, bank accounts, driver's licenses, children's information, and account credentials. Additionally, the agency may advise individuals to change passwords and encourage the use of multi-factor authentication for account access. When choosing guidance to mitigate the risk of harm, the SAOP should consider the guidance options included in Appendix II of this privacy breach response plan.

8.1.3 Services

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall determine if there are services the agency can provide. Many of the services currently available in today's marketplace only mitigate risks of financial identity theft, and even the most comprehensive services are unable to mitigate the potential harms resulting from the evolving threat and risk landscape. When selecting services, the SAOP shall identify those services that best mitigate the specific risk of harm resulting from the particular breach. If the SAOP determines that no service currently available mitigates a specific risk of harm, the agency may choose not to provide services to potentially affected individuals. Choosing not to provide services is a decision separate from the decision to provide notification and there may be circumstances where potentially affected individuals are notified but not provided services. OMB Memorandum M-17-12 does not set a specific threshold for providing services to individuals.

When choosing identity monitoring, credit monitoring, and other related services to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall take advantage of the General Services Administration blanket purchase agreements in

accordance with OMB Memorandum M-16-14. In addition, the SAOP should consider the services included in Appendix III of this memorandum as well as additional services available in the future.[36]

9.0 Notifying Individuals Potentially Affected by a Breach

The SAOP, in coordination with the breach response team when applicable, is responsible for advising the head of the agency on whether and when to notify the individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to notify individuals will depend on the circumstances of the breach. When deciding whether or not to notify individuals potentially affected by a breach, agencies shall consider the assessed risk of harm conducted in accordance with section 7.0 of this privacy breach response plan. The assessed risk of harm to individuals shall inform the agency's decision of whether or not to notify individuals. The head of the agency is ultimately responsible for making a final decision regarding whether or not to provide notification.

The agency's decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may necessarily require the agency to notify those individuals both of the breach and of those steps taken to mitigate any identified risks. For example, if an agency decides to provide identity and credit monitoring to individuals potentially affected by a particular breach, the agency would need to notify those individuals so that they can use the service. However, agencies may also choose to notify individuals even when the agency is not providing a specific service. For example, an agency may notify individuals that their passwords were potentially compromised by a breach and offer guidance but no services.

Agencies should balance the need for transparency with concerns about over-notifying individuals. Notification may not always be helpful to the potentially affected individuals, and agencies should exercise care to evaluate the benefit providing notice to individuals or notifying the public.

Certain federal information systems may be subject to other breach notification requirements, such as those subject to the Health Insurance Portability and Accountability Act. The SAOP shall ensure that appropriate subject matter experts who can identify those requirements are part of the breach response team. In circumstances where multiple

[36]OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 27-28.

notification requirements apply to a breach, agencies should provide a single notice to potentially affected individuals that complies with the guidance in this privacy breach response plan as well as any other notification requirements.

When the head of the agency determines that it is necessary to notify individuals potentially affected by a breach, the SAOP, in coordination with the breach response team when applicable, shall consider the following:

9.1.1 Source of the Notification

When notification is necessary, helpful, or otherwise required, the head of the agency or a senior-level individual he or she may designate in writing shall be the source of the notification to potentially affected individuals. Notification from this level demonstrates that the breach has the attention of the head of the agency.

In instances where a small number of individuals potentially are affected by a breach, and when the SAOP determines that there is a low risk of harm to the potentially affected individuals, the SAOP may issue the notification.

When PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor, or by a subcontractor (at any tier), on behalf of the agency is involved in a breach, the agency may require the contractor to notify any potentially affected individuals.

9.1.2 Timeliness of the Notification

The agency shall notify individuals potentially affected by a breach as expeditiously as possible and without unreasonable delay.[37] As a practical matter, the agency will avoid providing multiple notifications for a single breach and will balance the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm to potentially affected individuals. If a technical issue contributed to the breach, the head of the agency may also consider whether the issue has been corrected or resolved prior to providing notification.[38]

9.1.3 Contents of the Notification

The agency shall provide individuals potentially affected by a breach with notification that is concise and uses plain language. The agency shall avoid using generic or repetitive

[37] 44 U.S.C. § 3553, note ("Breaches")
[38] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 31.

language and should tailor the notification to the specific breach. In some instances, it may be necessary for the agency to draft different notifications for different populations affected by the same breach.

At a minimum, notifications shall include the following:

- A brief description of what happened, including the date(s) of the breach and of its discovery
- To the extent possible, a description of the types of PII compromised by the breach (e.g., full name, SSN, date of birth, home address, account number, and disability code)
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system
- Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the agency is taking, and services the agency is providing to potentially affected individuals, if any
- Steps the agency is taking, if any, to investigate the breach, to mitigate losses, and to protect against a future breach
- Whom potentially affected individuals should contact at the agency for more information, including contact information

The agency may provide additional details in a Frequently Asked Questions (FAQ) format internally, on the agency website, or via an enclosure. The FAQs on an agency website may be beneficial because they can be easily updated, contain links to more information, provide more tailored information than the formal notification, and can be easily translated into multiple languages. For a breach that potentially affects a large number of individuals, or as otherwise appropriate, the agency may establish toll-free call centers staffed by trained personnel to handle inquiries from the potentially affected individuals. If the agency has knowledge that the potentially affected individuals are not English speaking, or require translation services, notification may also be provided in the appropriate languages to the extent feasible. The agency may seek additional guidance on how to draft a notification

from the FTC, which is a leader in providing clear and understandable notifications to consumers, as well as from communication experts.[39]

9.1.4 Method of Notification

The SAOP shall select the method for providing notification. The best method for providing notification will potentially depend on the number of individuals affected, the available contact information for the potentially affected individuals, and the urgency with which the individuals need to receive the notification.

- **First-Class Mail:** First-class mail notification to the last known mailing address of the individual in agency records should be the primary means by which notification is provided. Where the agency has reason to believe the address is no longer current, the agency should take steps to update the address by consulting with other agencies, such as the U.S. Postal Service. The notification should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency that experienced the breach uses another agency to facilitate mailing, care should be taken to ensure that the agency that suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents and should be marked with the name of the agency as the sender to reduce the likelihood the recipient thinks it is advertising mail. Agencies should anticipate mail returned as undeliverable and should have procedures in place for how to provide a secondary notification.

- **Telephone:** Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

- **Email:** Email notification, especially to or from a non-government email address, is not recommended due to the high risk of malicious email attacks that are often launched when attackers hear about a breach. Emails often do not reach individuals because they are automatically routed to spam or junk mail folders. Individuals who receive notifications via email are often uncertain of the legitimacy of the email and will not open the notification. While email is not recommended as the primary form of notification, in limited circumstances it may appropriate. For example, if the

[39] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 31.

individuals potentially affected by a breach are internal to the agency, it may be appropriate for an agency to use an official email address to notify a small number of employees, contractors, detailees, or interns via their official email addresses. A ".gov" or ".mil" email may be used to notify an individual on his or her ".gov" or ".mil" email that his or her PII was potentially compromised by a breach.

- **Substitute Notification:** Agencies may provide substitute notification if the agency does not have sufficient contact information to provide notification, and also as supplemental notification for any breach to keep potentially affected individuals informed. This type of notice may also be beneficial if the agency needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time-sensitive. A substitute notification should consist of a conspicuous posting of the notification on the home page of the agency's website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Notification to media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the breach. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, the agency will consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates. Depending on the individuals potentially affected and the specific circumstance of a breach, it may be necessary for the agency to provide notifications in more than one language.[40]

9.1.5 Special Considerations

When a breach potentially affects a vulnerable population, the agency may need to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary.

There may be instances when the agency provides notification to individuals other than those whose PII was potentially compromised. For example, when the individual whose information was potentially compromised is a child, the agency may provide notification to the child's legal guardian(s). Special care may be required to determine the appropriate recipient in these cases.

[40] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 32-33.

The agency should give special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973, as amended. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency website.[41]

[41] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 33.

Appendix I: DFC Privacy Breach Reporting Form

U.S. International Development Finance Corporation (DFC)

Privacy Breach Reporting Form

Breach Reported by:					
Name:	<<First>>	<<Last>>	**Supervisor:**	<<First>>	<<Last>>
Email:	<<Official Email>>		**Email:**	<<Official Email>>	
Phone:	<<Official Phone>>		**Phone:**	<<Official Phone>>	
Office:			<<Office that Reported the Breach>>		
DFC Tracking Number:			<<Internal Tracking Number>>		

Summary of the Breach:	
Do not include sensitive personally identifiable information (SPII) or classified information. Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including: a. A description of the parties involved in the breach b. The physical or electronic storage location of the information at risk c. If steps were immediately taken to contain the breach d. Whether the breach is an isolated occurrence or a systematic problem e. Who conducted the investigation of the breach, if applicable f. Any other pertinent information	
Date and Time of the Breach:	<<Month/Day/Year, Approximate Time>>
Date and Time of Discovery:	<<Month/Day/Year, Approximate Time>>
Location of Breach:	<<Street Address>>
Office Responsible for the Breach:	<<Office that Caused the Breach>>

Type of Breach:			
Lost Information or Equipment	Y/N	**Unauthorized Disclosure** (e.g., email sent to incorrect email address, oral or written disclosure to unauthorized person, disclosing documents publicly with sensitive information not redacted)	Y/N
Stolen Information or Equipment	Y/N	**Unauthorized Access** (e.g., an unauthorized employee or contractor accesses information or an information system)	Y/N
Unauthorized Equipment (e.g., using an unauthorized personal device, server, or email account to store PII)	Y/N	**Unauthorized Use** (e.g., employee with agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)	Y/N

Storage Medium:

Laptop or Tablet	Y/N	**Smartphone**	Y/N
Desktop	Y/N	**Paper Files**	Y/N
External Storage Device	Y/N	**External Storage Device** (e.g., CD, DVD, USB Drive, etc.)	Y/N
IT System (Intranet/Shared Drive)	Y/N	**Oral Disclosure**	Y/N
Email:	<<Sender and recipient domains (e.g., dfc.gov to gmail.com)>>		
Other:	<<Provide a detailed description of the medium>>		

Reported to US-CERT, Law Enforcement, or Congress		
Reported to US-CERT	Y/N	**<<If applicable, specify law enforcement agency or congressional committee>>**
Reported to Law Enforcement	Y/N	
Reported to Congress	Y/N	
Name:	<<Reporting Official>>	
Title:	<<Reporting Official's Title>>	
Email:	<<Official Email>>	
Phone:	<<Official Phone>>	
Office:	<<Reporting Official's Office>>	
US-CERT Incident ID Number:	<<US-CERT Incident ID Number>>	
Date and Time of the Report:	<<Month/Day/Year, Approximate Time>>	

Number of Individuals and Safeguards	
Number of Individuals Potentially Affected by the Breach?	<<#>>
Was the Information Unstructured? (e.g., open fields on a form or survey)	Y/N
Was the Information Encrypted?	Y/N
Does a Duplicate Set of the Potentially Compromised Information Exist?	Y/N

Additional Information	
Internal Breach (e.g., Within the Agency's Network), External, Both, or Unknown?	<< >>
What Countermeasures, if Any, Were Enabled When the Breach Occurred?	
<<List all that apply; include whether National Institute of Standards and Technology certified (e.g., hard drive encryption on laptop, encryption of electronic files, password on smartphone)>>	
What Steps, if Any, Have Already Been Taken to Mitigate Potential Harm?	
<<E.g., calling or sending separate email(s) to recipient(s) of an unauthorized email to request deletion of original email, contacting web publishing to remove unredacted documents from public website, etc.>>	
Do You Have Knowledge that Any Information Involved in the Breach Was Intentionally Stolen or Misused?	Y/N
<<If yes, describe the basis for your knowledge and how the information may have been misused (e.g., evidence of identity theft, hacking, adverse publicity, etc.)>>	

Data Elements and Information Types

Identifying Numbers	
☐ Social Security Number	☐ Truncated or Partial Social Security Number
☐ Driver's License Number	☐ License Plate Number
☐ Drug Enforcement Agency Registration Number	☐ File/Case ID Number
☐ Patient ID Number	☐ Health Plan Beneficiary Number
☐ Student ID Number	☐ Federal Student Aid Number
☐ Passport Number	☐ Alien Registration Number
☐ DFC ID Number	☐ DFC Benefits Number
☐ Employee Identification Number	☐ Professional License Number
☐ Taxpayer Identification Number	☐ Business Taxpayer Identification Number
☐ Credit Card/Debit Card Number	☐ Business Credit Card Number
☐ Vehicle Identification Number	☐ Business Vehicle Identification Number
☐ Personal Bank Account Number	☐ Business Bank Account Number
☐ Personal Device Identifiers or Serial Numbers	☐ Business Device Identifiers or Serial Numbers
☐ Personal Mobile Number	☐ Business Mobile Number

Biographical Information		
☐ Name (including nicknames)	☐ Gender	☐ Race
☐ Date of Birth	☐ Ethnicity	☐ Nationality
☐ Country of Birth	☐ City or County of Birth	☐ State of Birth
☐ Country of Residence	☐ City or County of Residence	☐ State of Residence
☐ Marital Status	☐ Citizenship	☐ Immigration Status
☐ Religion/Religious Preference	☐ Home Address	☐ Zip Code
☐ Home Phone or Fax Number	☐ Spouse Information	☐ Sexual Orientation
☐ Parent Information	☐ Children Information	☐ Other Relative Information (e.g., siblings, cousins, etc.)
☐ Group/Organization Membership	☐ Military Service	☐ Mother's Maiden Name
☐ Business Mailing Address	☐ Business Phone or Fax Number	☐ Global Positioning System (GPS)/Location Data
☐ Personal Email Address	☐ Business Email Address	☐ Employment Information
☐ Personal Financial Information (including loan information)	☐ Business financial information (including loan information)	☐ Alias (e.g., username or screen name)
☐ Education Information	☐ Resume or Curriculum Vitae	☐ Professional/Personal References

Biometrics/Distinguishing Features/Characteristics		
☐ Fingerprints/Palm Prints	☐ Blood Type	☐ Vascular Scans

☐ Retina/Iris Scans	☐ Dental Profile	☐ Scars, Marks, Tattoos
☐ Hair Color	☐ Eye Color	☐ Height
☐ Video Recording	☐ Photos	☐ Voice/Audio Recording
☐ DNA Sample or Profile	☐ Signature	☐ Weight

Medical/Emergency Information (Select All that Apply)		
☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

Device Information		
☐ Device Settings or Preferences (e.g., security level, sharing options, ringtones)	☐ Cell Tower Records (e.g., logs, user location, time, etc.)	☐ Network Communications Data

Specific Information/File Types		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance/Background Check Information
☐ Civil/Criminal History Information/Police Record	☐ Academic and Professional Background Information	☐ Health Information
☐ Case Files	☐ Personnel Files	☐ Credit History Information

Appendix II: Examples of Guidance the Agency May Offer[42]

Credit Freeze: A credit freeze restricts access to an individual's credit report. When offering this type of guidance, an agency should be aware that because access to a credit report is usually required by creditors, a credit freeze can prevent creditors from approving a new account.

Credit Freezes/or Children: Guardians are sometimes able to place a freeze on a child's credit, even if the child does not yet have a credit history. Several states mandate that all credit bureaus provide this option. Outside those states, the option may still be available depending on the credit bureau. In these instances, guardians may have to provide additional information about themselves as well as the child in order to show the relationship.

Closing or Changing Accounts: Individuals should immediately dispute any unauthorized charges to existing accounts, including closing or changing account numbers so that unauthorized activity does not continue. This will not prevent new unauthorized accounts of which individuals may be unaware.

Obtaining a Free Credit Report: Individuals can obtain a free credit report yearly from each of the three national credit bureaus (Equifax, Experian, and Trans Union) from annualcreditreport.com or by calling the credit reporting agencies' toll-free numbers. Individuals should review their credit reports for any accounts they do not recognize.

Cyber Hygiene: Agencies should also consider providing individuals with resources on good cyber hygiene (e.g., setting up multi-factor authentication, using complex passwords). Resources include:

- ***CISA Cybersecurity Awareness Program:*** https://www.cisa.gov/cisa-cybersecurity-awareness-program
- ***FTC's Tips on Protecting Online Privacy and Security:*** https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

[42] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 42.

- ***CISA's Tips on Preventing Online Identity Theft:*** https://www.us-cert.gov/ncas/tips/ST05-019

Deceased Alerts: Deceased individuals can be at heightened risk for identity fraud that may impact the deceased individual's estate. This creates liability for a surviving spouse if, for example, his or her name is on joint accounts. To prevent this, death certificates can be sent to the IRS as well as the major credit bureaus, with a request to place a "deceased alert" on the account to prevent new activity.

Fraud Alert: A fraud alert tells creditors that they must take reasonable steps to verify the identity of the individual who is applying for credit. A fraud alert also allows individuals to order one free copy of the individual's credit report from each of the three national credit bureaus. To place this alert, individuals can contact one of the three national credit bureaus, who must then notify the others. The initial fraud alert stays on the credit report for 90 days and can be renewed.

FTC.gov/idtheft: The FTC's website provides free identity theft resources for individuals as well as community leaders, businesses, advocates, and law enforcement to share in their communities. The website includes resources on proactive steps individuals can take to monitor and protect their information and educate themselves on the different types of identity theft and the resources available to protect against and recover from identity theft.

IdentityTheft.gov: This is the federal government's one-stop resource for identity theft victims. Individuals can use the website to report identity theft and get a personalized recovery plan that walks them through each step, updates the plan as needed, and pre-fills letters and forms. It also advises individuals on steps they can take to prevent identity theft when they receive notice that their PII has been compromised. The website is managed by the FTC and is integrated with the FTC's complaint system, which makes the complaint information available to law enforcement across the country through Consumer Sentinel, a secure online database available to law enforcement.

Tax Fraud: Agencies may consider recommending that individuals file an IRS Identity Theft Affidavit (Form 14039) to prevent an identity thief from using compromised PII to falsely claim the individual's tax refund.

Appendix III: Examples of Services the Agency May Offer[43]

Credit Monitoring: Many companies, including credit reporting agencies, offer this service as a subscription for a defined period of time. The service includes monitoring an individual's credit report, and notifying the potentially affected individual, usually via email, when new activity is reported to their credit report. Credit monitoring notifies individuals that compromised information may have been used to open a new credit account using their information. It does not monitor other non-credit-based risks for misuse of compromised information.

Identity Monitoring: These services monitor the use of an individual's overall identity beyond information contained in a credit report. This monitoring generally tracks whether the individual's information has been exposed online, in addition to monitoring other databases, which may include information related to change of address, court records, payday loans, health, criminal, and other identifying information beyond just financial credit information. These more comprehensive services mitigate risks of the non-credit identity thefts outlined above. Each company provides different monitoring services, so the agency should ensure that monitoring options are appropriate given the compromised information. The effectiveness of the monitoring will depend on factors such as the databases monitored, the amount and accuracy of the information in the databases, and how often the company checks the databases.

Full-Service Identity Counseling and Remediation Services: These are additional services that provide trained counselors or case managers to help individuals recover from identity theft. The services may include assisting individuals with preventing pre-screened offers of credit, helping consumers dispute charges and removing fraudulent information, and providing legal assistance. Generally, individuals authorize companies offering these services to act on their behalf.

Identity Theft Insurance: Insurance reimburses individuals for certain losses resulting from identity theft. Generally, this insurance covers only out-of-pocket expenses directly associated with recovery from the identity theft. Typically, these are limited to things like postage, copying and notary costs. Some policies cover lost wages or legal fees. Generally, these policies do not provide reimbursement for any funds that are stolen as a result of the

[43] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), 44.

identity theft. Agencies should understand what they are purchasing and communicate clearly within any guidance provided the details of what the insurance covers as well as any limitations and exclusions to the potentially affected individuals.