FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Financial Disclosure Online (FDO)

October 16, 2023

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC's public-facing website,[1] which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

Abstract

Financial Disclosure Online (FDO or FDonline) is the central repository for Federal Deposit Insurance Corporation (FDIC) employees' confidential financial disclosure and initial ethics orientation training records. FDIC employees file confidential financial disclosure reports as required by the Ethics in Government Act, U.S. Office of Government Ethics (OGE), and FDIC-specific supplemental financial disclosure requirements. This PIA is being conducted because FDO collects and maintains personally identifiable information (PII).

Background

The FDIC is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, making large and complex financial institutions resolvable, and managing receiverships.

Within FDIC, the Legal Division's Ethics Unit promotes high ethical standards for FDIC employees by providing advice and guidance on avoiding conflicts of interest, conducting training on the ethics laws, regulations and Executive Orders and administering the FDIC financial disclosure program. The Unit strengthens the public's confidence that the Corporation and its employees operate with impartiality and integrity.

FDIC employees are required to file confidential financial disclosure reports and related FDIC disclosure forms pursuant to Title I of the Ethics in Government Act of 1978 (5 U.S.C. 131),

[1] www.fdic.gov/privacy

Executive Order 12674 (as modified by Executive Order 12731), the Ethics Reform Act of 1989, Pub. L. 101-194, and FDIC-specific supplemental financial disclosure regulations. Confidential financial disclosure preserves the public's trust in FDIC operations and helps prevent inadvertent conflicts of interest.

Overview

FDO is a Software as a Service (SaaS) solution that serves as the central repository for FDIC employees' confidential financial disclosure and initial ethics orientation training records. FDIC Legal Division's Ethics Unit staff use FDO to electronically assign and track FDIC employees' completion of required confidential financial disclosure reports and related FDIC disclosure forms. FDO automates the disclosure filing process, eliminating cumbersome, manual processing and encouraging timely compliance with applicable Federal conflict of interest laws and regulations.

To initiate the disclosure process, FDO receives a limited feed of employee data from FDIC's Corporate Human Resources Information System (CHRIS)[2] via FDIC's Enterprise Data Warehouse (EDW)/Person Master Dimension (PMD). FDO uses this data for administrative contact purposes and to assign and route required ethics forms to FDIC employees for completion. FDO automatically assigns the appropriate ethics forms to FDIC employees based on their division, pay plan, pay grade, and occupational series. FDO notifies employees by email of any required disclosures.

FDIC employees/filers gain access to FDO via Single Sign On (SSO). Upon accessing the system, employees follow a step-by-step report wizard process to review, complete and submit (eSign) the appropriate disclosure report form(s). Depending on the duties and responsibilities of their respective positions, FDIC employees may be required to complete some or all of the following forms in FDO:

- OGE Form 450, *Confidential Financial Disclosure Report* – The OGE Form 450 assists employees and their agencies in avoiding conflicts between official duties and private financial interests or affiliations.

- Form FDIC 2410/06, *Confidential Report of Indebtedness* – For certain FDIC positions, employees are required to report obligations/debt to FDIC-insured institutions using this form and update that information annually thereafter.

---

[2] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html and Office of Personnel Management (OPM)/GOVT-1, *General Personnel Records*, 87 Fed. Reg. 5874 (February 2, 2022), https://www.federalregister.gov/documents/2022/02/02/2022-02057/privacy-act-of-1974-system-of-records.

- Form FDIC 2410/07, *Confidential Report of Interest in FDIC-Insured Depository Institution Securities* – Within 30 days, all FDIC employees must report the acquisition or sale of any stocks, bonds, and other securities of FDIC-insured banks, bank holding companies, financial holding companies, and savings and loan (S&L) holding companies by completing this form.

- Form FDIC 2410/09, *Employee Certification and Acknowledgement of Standards of Conduct Regulation* – New FDIC employees must complete this form to certify receipt of initial ethics orientation and acknowledgement of ethical standards of conduct.

These forms collect information about FDIC employees and, in some cases, about other individuals, such as FDIC employees' spouses, dependent children, and individual employers, creditors, and gift-providers. Legal authority for this information collection is provided by Title I of the Ethics in Government Act of 1978 (5 U.S.C. 131), Executive Order 12674 (as modified by Executive Order 12731), the Ethics Reform Act of 1989, Pub. L. 101-194, and FDIC-specific supplemental financial disclosure regulations.

After employees/filers submit the required form(s) in FDO, the system sends email notification(s) to their division or office Deputy Ethics Counselors who are trained by the Ethics Unit and delegated the authority to review and certify disclosure forms. Deputy Ethics Counselors access FDO to review for conflicts of interest the forms of those employees in their areas of responsibility. They can return forms to an employee to be updated or corrected as needed. Deputy Ethics Counselors also have the ability to enter comments and upload supporting documentation into FDO, such as an email confirming the filer sold a specific asset. Deputy Ethics Counselors do not ask filers to attach the full portfolio information itself because it typically includes PII; they endeavor to minimize the collection of unnecessary PII whenever possible. Once completed and certified, forms are retained in FDO for the duration of their established retention periods.

Collectively, the forms maintained in FDO may include the following types of information about FDIC employees/filers: full name; employee ID; work address; phone numbers; job title; FDIC Division description; grade; Department name; FDIC region; pay plan; pay grade; occupational series code; employment status; hire date; grade entry date; financial information and/or numbers (including information regarding an employee's financial interest in FDIC-insured depository institution securities; any non-credit card financial obligations owed to FDIC-insured depository institution and/or its subsidiary; and any other reportable assets, income, and liabilities); outside positions; agreements and arrangements for benefits, payments, and employment; gifts; and travel reimbursements. Certain forms in FDO may include the following information about spouses and dependent children of FDIC employees/filers, as applicable: financial information; income; employer name; assets; liabilities; financial interests; and loan information. Additionally, forms may contain limited information about individual employers, gift-providers, and creditors of filers, including: full

name; city; state; terms of agreement/arrangement (if applicable); and description of gifts/travel reimbursement (if applicable).

Authorized staff in the FDIC Ethics Unit have administrator access to all data in FDO. Administrator access to data is determined by the Ethics Program Manager for FDO based on the user's business requirements and granted on a "need to know" basis. The purpose for their access is to maintain the system, review completed ethics forms for accuracy, notify employees of any updates/corrections that need to be made to the forms, approve forms, and run reports to track compliance/completion of ethics forms and training by employees.

Consistent with the Ethics in Government Act, as amended, FDIC must furnish to OGE all information and records in its possession which OGE deems necessary to the performance of its oversight responsibilities, except to the extent prohibited by law. For financial disclosure audit purposes, this typically includes copies of the disclosure reports, number of filers, and data related to filing, review, and certification timeliness. The information may be provided securely to OGE electronically or in hard-copy upon request. The FDO system is not directly linked to OGE and information, if requested, is manually shared.

FDIC is conducting this PIA to evaluate and document its use of FDO and to identify associated privacy risks and mitigations. The type and extent of PII collected depends on which of the aforementioned form(s) employees are required to complete based on the duties and responsibilities of their respective FDIC positions. Information collected through and maintained in FDO is covered by the following System of Records Notices (SORNs): FDIC-006, *Employee Financial Disclosure Records*;[3] OGE/GOVT-1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records*;[4] and OGE/GOVT-2, *Executive Branch Confidential Financial Disclosure Reports*.[5]

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to

[3] FDIC SORN-006, *Employee Financial Disclosure Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[4] OGE GOVT-1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records*, 84 Fed. Reg. 47303 (September 9, 2019), https://www.federalregister.gov/documents/2019/09/09/2019-19372/privacy-act-of-1974-systems-of-records.
[5] OGE GOVT-2, *Executive Branch Confidential Financial Disclosure Reports*, 84 Fed. Reg. 47301 (September 9, 2019), https://www.federalregister.gov/documents/2019/09/09/2019-19373/privacy-act-of-1974-systems-of-records.

mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency
- Data Minimization
- Data Quality and Integrity
- Use Limitation

Transparency:

Privacy Risk: When the FDO system was initially launched, it did not display a Privacy Act Statement when an employee entered the system using Single Sign On (SSO). This introduced the risk that the employee may not have been aware of the purpose, use, and other disclosures related to their PII found in the Privacy Act Statement.

Mitigation: A software fix has been implemented to ensure the system displays a Privacy Act Statement, which requires acknowledgement before the employee begins entering information into each of the ethics forms (i.e., FDIC 2410/06, 2410/07, 2410/09 and OGE 450 forms). No additional mitigation actions are recommended.

Privacy Risk: Individuals other than the employee, such as the employee's spouse, children, and individual creditors, may not be aware that their information is being collected and maintained in the system.

Mitigation: Employees are responsible for providing appropriate notice to their spouses, children, and other individuals on whom they provide information in the system. This PIA and the SORN(s) listed in 2.2 also serve as notice and implicit consent with respect to the collection, use, and disclosure of PII. Additionally, the information collected is not used to make determinations regarding individuals other than the employee. No additional mitigation actions are recommended.

Data Minimization:

Privacy Risk: When completing their ethics forms, employees may include unnecessary PII in supporting documents and/or free text comment fields.

Mitigation: In rare instances, employees may be required to upload supporting documentation into the system upon the request of Deputy Ethics Counselors. In addition, comments fields may only be initiated by Deputy Ethics Counselors as a means of requesting additional clarification from employees. Deputy Ethics Counselors provide instructions and guidance to employees to minimize any unnecessary PII and only collect that which is required to ensure compliance with applicable Federal conflict of interest laws and

regulations. Deputy Ethics Counselors have the ability to delete any PII that is not required in the system during the course of their review. Additionally, FDO includes an automated retention reminder that indicates to administrators when records maintained in the system have reached the end of their retention period.

Privacy Risk: Due to the storage of data on a commercial cloud platform, there is a risk that the cloud service provider (vendor) could fail to adhere to FDIC record retention guidelines and schedules.

Mitigation: During the period that FDIC's contract with the FDO cloud service provider is active, the FDIC has direct access to its data and ensures that appropriate retention schedules are followed. After the contract period ends, the vendor is required to adhere to the retention restrictions specified in its contractual agreement with FDIC. Technical controls, including an encryption key management service within the FDO cloud architecture, prevent vendor personnel from using or redistributing any FDIC data processed and stored within FDO. Should the vendor be required to access FDIC data to comply with Federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the vendor with the necessary encryption keys to access the data. In the rare instances that vendor personnel have access to FDIC data due to a law enforcement requirement or court order, the vendor is obligated, by contract, to abide by all FDIC record retention schedules and privacy and security requirements. FDIC has access to the vendor's cloud hosting environment and may periodically audit the vendor to ensure information is retained in accordance with applicable retention schedules. No additional mitigation actions are recommended.

Data Quality and Integrity:

Privacy Risk: There is a risk that information collected indirectly about the employee's spouse, creditors, and others listed in Section 1.1 may be inaccurate.

Mitigation: Employees are responsible for and have a vested interest in providing accurate information on their ethics forms, including information pertaining to their spouses, children, and other individuals as applicable. This responsibility is reinforced in annual employee ethics training and in the certification acknowledged by the employee prior to the completion of each form. This certification stipulates that providing the requested information is mandatory, and any falsification of information or failure to file or report required information may be subject to disciplinary action, including dismissal, by the FDIC or other appropriate authority. Knowing and willful falsification of information required to be filed may also result in criminal prosecution under 18 U.S.C. §1001. Additionally, Ethics Unit reviewers and Deputy Ethics Counselors provide instructions and guidance to assist employees with any difficulties that may arise in providing the required information.

Use Limitation:

Privacy Risk: Due to the system's reliance on a commercial cloud service provider, there is a risk that the cloud service provider could potentially misuse the data.

Mitigation: Technical controls, including an encryption key management service within the vendor's cloud architecture, prevent vendor personnel from using or redistributing any FDIC data processed and stored within FDO. Should the vendor be required to access FDIC data in order to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the vendor with the necessary encryption keys to access the data. In the rare instances that vendor personnel have access to FDIC data because of a law enforcement requirement or court order, the vendor is obligated, by contract, to abide by all FDIC data protection requirements. Additionally, FDIC has access to the vendor's cloud hosting environment and may periodically audit the vendor to ensure information is protected in accordance with applicable contractual requirements. No additional mitigation actions are recommended.

Section 1.0: Information System

1.1 What information about individuals, including PII (e.g., name, Social Security number, date of birth, address) and non-PII, will be collected, used or maintained in the information system or project?

FDO maintains the following types of information about FDIC employees (filers): full name; employee ID; work address; phone numbers; job title; FDIC Division description; grade; Department name; FDIC region; pay plan; pay grade; occupational series code; employment status; hire date; grade entry date; financial information and/or numbers (including information regarding an employee's financial interest in FDIC-insured depository institution securities; any non-credit card financial obligations owed to FDIC-insured depository institution and/or its subsidiary; and any other reportable assets, income, and liabilities); outside positions; agreements and arrangements for benefits, payments, and employment; gifts; and travel reimbursements. In addition, in rare instances, Deputy Ethics Counselors may upload supporting documentation into FDO, such as an email confirming the filer sold a specific asset. Deputy Ethics Counselors do not ask filers to attach the full portfolio information itself because it typically includes PII; only a copy of the filer's email statement indicating the asset was sold is attached.

The following information is maintained on spouses and dependent children of FDIC employees: financial information; income; employer name; assets; liabilities; financial interests; and loan information.

The following information is maintained on creditors, gift-providers, individual employers: full name; city; state; terms of agreement/arrangement (if applicable); and description of gifts/travel reimbursement (if applicable).

PII Element	Yes
Full Name	☒
Date of Birth	☐
Place of Birth	☐
Social Security number (SSN)	☐
Employment Status, History or Information	☒
Mother's Maiden Name	☐
Certificates (e.g., birth, death, naturalization, marriage)	☐
Medical Information	☐
Address	☐
Phone Number(s)	☒
Email Address	☒
Employee Identification Number (EIN)	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report)	☒
Driver's License/State Identification Number	☐
Vehicle Identifiers (e.g., license plates)	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	☐
Education Records	☐
Criminal Information	☐
Military Status and/or Records	☐
Investigation Report or Database	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐

Photographic Identifiers (e.g., image, video)	☐
User Information (e.g., User ID, password)	☐
Specify other: Outside work activities as pertinent to required/confidential financial disclosures for OGE ethics forms, such as positions held outside of US Government, gifts/travel reimbursements, and agreements/arrangements (Requested on OGE Form 450)	☒

1.2 What are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
FDIC's Corporate Human Resources Information System (CHRIS)[6] via FDIC's Enterprise Data Warehouse (EDW)/Person Master Dimension (PMD)	EDW/PMD provides a limited feed of data from FDIC's Corporate Human Resources Information System[7] for administrative contact purposes, as well as to appropriately assign and route required ethics forms to FDIC employees for completion.
Employee Ethics Forms and Supporting Documentation (as applicable)	The information in the system consists of various ethics disclosure forms completed by individual FDIC employees or a person or entity designated by the individual. These forms include OGE Form 450, *Confidential Financial Disclosure Report*; Form FDIC 2410/06, *Confidential Report of Indebtedness*; Form FDIC 2410/07, *Confidential Report of Interest in FDIC-Insured Depository Institution Securities*; and Form FDIC 2410/09, *Employee Certification and Acknowledgement of Standards of Conduct Regulation*. Deputy Ethics Counselors have the ability to upload supporting documentation into FDO, such as an email confirming the filer sold a specific asset. Deputy Ethics Counselors do not ask filers to attach the full portfolio information itself because it typically includes PII; Ethics reviewers endeavor to minimize the collection of unnecessary PII.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

FDO completed its initial ATO on September 24, 2019 and will be periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

[6] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html and OPM GOVT-1, *General Personnel Records*, 87 Fed. Reg. 5874 (February 2, 2022), https://www.federalregister.gov/documents/2022/02/02/2022-02057/privacy-act-of-1974-system-of-records.
[7] Ibid.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act System of Records Notice (SORN) does this information system or project operate? Provide number and name.

The following SORNs apply to this project: FDIC-006, *Employee Financial Disclosure Records*;[8] OGE/GOVT-1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records*;[9] and OGE/GOVT-2, *Executive Branch Confidential Financial Disclosure Reports*.[10]

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

No, the system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every five years or as needed.

2.4 If a Privacy Act Statement[11] is required, how is the Privacy Act Statement provided to individuals before collecting their PII? Explain.

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1 'FDIC Forms Management Program'. The following forms collect PII for this system and contain Privacy Act Statements: FDIC 2410/06, 2410/07, 2410/09 and OGE 450 forms.

---

[8] FDIC SORN-006, *Employee Financial Disclosure Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

[9] OGE GOVT-1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name- Retrieved Ethics Program Records*, 84 Fed. Reg. 47303 (September 9, 2019), https://www.federalregister.gov/documents/2019/09/09/2019-19372/privacy-act-of-1974-systems-of-records.

[10] OGE GOVT-2, *Executive Branch Confidential Financial Disclosure Reports*, 84 Fed. Reg. 47301 (September 9, 2019), https://www.federalregister.gov/documents/2019/09/09/2019-19373/privacy-act-of-1974-systems-of-records.

[11] *See* 5 U.S.C. §552a(e)(3). The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: When the FDO system was initially launched, it did not display a Privacy Act Statement when an employee entered the system using Single Sign On (SSO). This introduced the risk that the employee may not have been aware of the purpose, use, and other disclosures related to their PII found in the Privacy Act Statement.

Mitigation: A software fix has been implemented to ensure the system displays a Privacy Act Statement, which requires acknowledgement before the employee begins entering information into each of the ethics forms (i.e., FDIC 2410/06, 2410/07, 2410/09 and OGE 450 forms). No additional mitigation actions are recommended.

Privacy Risk: Individuals other than the employee, such as the employee's spouse, children, and individual creditors, may not be aware that their information is being collected and maintained in the system.

Mitigation: Employees are responsible for providing appropriate notice to their spouses, children, and other individuals on whom they provide information in the system. This PIA and the SORN(s) listed in 2.2 also serve as notice and implicit consent with respect to the collection, use, and disclosure of PII. Additionally, the information collected is not used to make determinations regarding individuals other than the employee. No additional mitigation actions are recommended.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

FDIC employees are able to access their information by logging into the system through Single Sign On (SSO).

Additionally, the FDIC provides individuals with access to their PII maintained in FDIC's systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1360.20. Access procedures for this information system are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes instructions for how individuals may request access to records that are maintained in each system of record, as specified by the Privacy Act and FDIC Circular 1360.20. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

3.2 What procedures are in place to allow the individuals to correct inaccurate or erroneous information?

After logging into the system, employees have the ability to make changes to any inaccurate or erroneous information they previously entered into the system on forms that have not been certified. Deputy Ethics Counselors can, in certain instances, reopen certified reports for additional correction.

For information fed to FDO from other systems, correction of inaccurate or erroneous information would be handled through the procedures specific to that system.

Additionally, the FDIC allows individuals to correct or amend PII maintained by the FDIC. Access procedures for this information system are detailed in the SORN(s) listed in Question 2.2 of this PIA.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

FDIC employees are notified by emails linked to their assigned disclosure forms which provide contact information for Deputy Ethics Counselors and the FDIC Ethics Unit in the event they have questions on any aspect of completing their forms.

Additionally, the FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users. The procedures for this information system are

detailed in the SORN(s) listed in Question 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable privacy risks related to access and amendment for FDO.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy, and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002; Section 522 of the 2005 Consolidated Appropriations Act; Federal Information Security Modernization Act of 2014; Office of Management and Budget (OMB) privacy policies; and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program supports the SAOP in the management and execution of the FDIC's Privacy Program.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy Program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Yes, this PIA captures privacy risks posed by the FDO through the privacy risk analysis sections throughout the document. PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/policies/privacy/index.html.

4.4 What roles, responsibilities and access will contractors have with the design and maintenance of the information system or project?

FDO is a Software-as-a-Service (SaaS) solution. FDO's vendor will be responsible for the design and maintenance of the system. The FDIC also uses contractors to provide technical support to the system and work with the vendor on future design and development needs.

Due to contractors' access to PII, contractors take mandatory annual information security and privacy training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Yes, appropriate Confidentiality Agreements have been completed and signed for

contractors who work on FDO. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program implements a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

Safeguarding nonpublic information is discussed during ethics orientation (mandatory for all new hires) and during annual ethics training (required for all existing FDIC employees). All Ethics Unit staff and Deputy Ethics Counselors receive specialized training prior to reviewing the various ethics forms. This specialized training addresses (among other things) requirements for protecting the confidentiality of the ethics forms and information provided by FDIC employees, including any PII. In addition, and as needed, Ethics Unit staff and Deputy Ethics Counselors provide guidance and counseling to employees about what information, including PII, is or is not required for filing.

Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA, and regular reporting to the SAOP, the

CISO, and the Information Technology Risk Advisory Committee.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

FDO includes an automated retention reminder system that indicates to administrators when records maintained in the system reach the end of their retention period.

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls when possible. Additionally, FDIC has implemented technologies to track, respond, remediate, and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and 12 C.F.R. § 310. Disclosures are tracked and managed using the FDIC's FOIA solution.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and 12 C.F.R. § 310.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and 12 C.F.R. § 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to accountability for FDO.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws and regulations:

- Title I of the Ethics in Government Act of 1978 (5 U.S.C. 131)
- Executive Order 12674 (as modified by Executive Order 12731)
- Ethics Reform Act of 1989, Pub. L. 101-194
- 5 CFR Part 735, Employee Responsibilities and Conduct
- 5 CFR Part 2634, Executive Branch Financial Disclosure, Qualified Trusts, and Certificates of Divestiture

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority for FDO.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII that are relevant and necessary to accomplish the legally authorized purpose of collection?

The forms in the system, as well as any supporting documentation and comments, are reviewed by Ethics Unit staff and Deputy Ethics Counselors to ensure that the PII elements collected are minimized to that which is required to comply with applicable Federal conflict of interest laws and regulations.

Additionally, through the conduct, evaluation, and review of privacy artifacts,[12] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

The forms in the system, as well as any supporting documentation and comments, are reviewed by Ethics Unit staff and Deputy Ethics Counselors to ensure that the PII elements collected are minimized to that which is required to comply with applicable Federal conflict of interest laws and regulations. PII is collected directly from individuals to the greatest extent practicable. FDO also includes an automated retention reminder that indicates to Ethics administrators when records maintained in the system have reached the end of their retention period

Additionally, through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.3 How often does the information system or project evaluate the PII contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

---

[12] Privacy artifacts include Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Record Notices (SORN).

The FDIC maintains an inventory of systems that contain PII. The Privacy Program reviews information in the systems at the frequency defined in the FDIC Information Security Continuous Monitoring Strategy. New collections are evaluated to determine if they should be added to the inventory.

6.4 What are the retention periods of the data in this information system or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The FDIC Records Retention Schedule (RRS) for FDO is EIS1025, *FDonline*, and identifies the retention periods for all forms maintained in FDO. FDO provides notification emails to Ethics Unit staff and reports identifying forms that have reached the end of their retention period. Ethics Unit staff will then timely dispose of such documents in FDO. Documents needed for an ongoing investigation will be retained until no longer needed for that investigation.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with National Archives and Records Administration (NARA) guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

Additionally, records are retained in accordance with the FDIC Circular 1210.01, FDIC "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and NARA-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.01 and 1360.09.

6.5 What are the policies and procedures that minimize the use of PII for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

The FDIC has developed an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: When completing their ethics forms, employees may include unnecessary PII in supporting documents and/or free text comment fields.

Mitigation: In rare instances, employees may be required to upload supporting documentation into the system upon the request of Deputy Ethics Counselors. In addition, comments fields may only be initiated by Deputy Ethics Counselors as a means of requesting additional clarification from employees. Deputy Ethics Counselors provide instructions and guidance to employees to minimize any unnecessary PII and only collect that which is required to ensure compliance with applicable Federal conflict of interest laws and regulations. Deputy Ethics Counselors have the ability to delete any PII that is not required in the system during the course of their review. Additionally, FDO includes an automated retention reminder that indicates to administrators when records maintained in the system have reached the end of their retention period.

Privacy Risk: Due to the storage of data on a commercial cloud platform, there is a risk that the cloud service provider (vendor) could fail to adhere to FDIC record retention guidelines and schedules.

Mitigation: During the period that FDIC's contract with the FDO cloud service provider is active, the FDIC has direct access to its data and ensures that appropriate retention schedules are followed. After the contract period ends, the vendor is required to adhere to the retention restrictions specified in its contractual agreement with FDIC. Technical controls, including an encryption key management service within the FDO cloud architecture, prevent vendor personnel from using or redistributing any FDIC data processed and stored within FDO. Should the vendor be required to access FDIC data to comply with Federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the vendor with the necessary encryption keys to access the data. In the rare instances that vendor personnel have access to FDIC data due to a law enforcement requirement or court order, the vendor is obligated, by contract, to abide by all FDIC record retention schedules and privacy and security requirements. FDIC has access to the vendor's cloud hosting environment and may periodically audit the vendor to ensure information is retained in accordance with applicable retention schedules. No additional mitigation actions are recommended.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

The FDIC reviews privacy artifacts for adequate controls to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

FDO collects PII on the employee directly from the employee to the maximum extent possible with some PII fed into FDO from EDW/PMD. The employee may provide additional PII on the employee's spouse, dependent children, creditors, and others listed in Section 1.1. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

The FDIC reviews privacy artifacts to ensure adequate controls to check for and correct any inaccurate or outdated PII in its inventory.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Through the PTA adjudication process, the FDIC Privacy Program uses the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer validates the configuration of administrative and technical controls for the system or project based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the

Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988. Consequently, the FDIC does not need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a risk that information collected indirectly on the employee's spouse, creditors, and others listed in Section 1.1 may be inaccurate.

Mitigation: Employees are responsible for and have a vested interest in providing accurate information on their ethics forms, including information pertaining to their spouses, children, and other individuals as applicable. This responsibility is reinforced in annual employee ethics training and in the certification acknowledged by the employee prior to the completion of each form. This certification stipulates that providing the requested information is mandatory, and any falsification of information or failure to file or report required information may be subject to disciplinary action, including dismissal, by the FDIC or other appropriate authority. Knowing and willful falsification of information required to be filed may also result in criminal prosecution under 18 U.S.C. §1001. Additionally, Ethics Unit reviewers and Deputy Ethics Counselors provide instructions and guidance to assist employees with any difficulties that may arise in providing the required information.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as

necessary, to individuals prior to the collection of PII. This implied consent from individuals authorizes the collection of the information provided.

The system also receives data from the employee on his or her spouse, dependent children, creditors and other individuals listed in Section 1.1. The FDIC does not have the ability to provide notices prior to the Agency's processing of PII pertaining to these individuals. The FDIC does not make determinations on these individuals based on the information received from the employee.

Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

When the FDIC collects information directly from individuals, it describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

The system also receives data from the employee on his or her spouse, dependent children, creditors and other individuals listed in Section 1.1. The FDIC does not have the ability to provide notices prior to the Agency's processing of PII pertaining to these individuals. The FDIC does not make determinations on these individuals based on the information received from the employee. This PIA and the SORN(s) listed in 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, when feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant SORN(s) as well as the relevant PIA.

8.4 Explain how the information system or project ensures that individuals are aware of and, when feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the FDIC collected the PII.

The project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

The system also receives data from the employee on his or her spouse, dependent children, creditors and other individuals listed in Section 1.1. The FDIC does not have the ability to provide notices prior to the Agency's processing of PII pertaining to these individuals. The FDIC does not make determinations on these individuals based on the information received from the employee. This PIA and the SORN(s) listed in 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, http://www.fdic.gov/privacy/, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There are no identifiable privacy risks related to individual participation for FDO.

Mitigation: No mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose 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.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

The records are maintained to assure compliance with the standards of conduct for Government employees contained in the Executive Orders, Federal Statutes and FDIC

regulations and to determine if a conflict of interest exists between employment of individuals by the FDIC and their personal employment and financial interests.

9.2 Describe how the information system or project uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Through the conduct, evaluation, and review of privacy artifacts, and in conjunction with the implementation of applicable privacy controls, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.09, "Protecting Information." Additionally, annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

The Ethics Program Manager/Data Owner serves as the primary sources of information for data definition and data protection requirements for FDO. They are collectively responsible for supporting a corporate-wide view of data sharing. Although they share this data responsibility, it is every user's responsibility to abide by FDIC data protection rules that are outlined in the Corporate Security Awareness Training and Privacy Act Awareness Orientation, which all employees take and certify they will abide by the Corporation's Rules of Behavior for data protection. This makes it the responsibility of every user to ensure the proper use of corporate data.

When contractors have access to PII, contractors are required to take mandatory annual Information Security and Privacy Awareness Training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

All FDIC employees have limited access to FDO through SSO to complete, review, and file their own ethics forms. Each employee has access only to his or her respective ethics forms.

Deputy Ethics Counselors will have access to review for conflicts of interest the forms of those employees in their areas of responsibility. They will be unable to access forms outside of their areas of responsibility.

Authorized staff in the FDIC Ethics Unit will have administrator access to all data in the system. Administrator access to data is determined by the Ethics Program Manager/Data Owner for FDO based on the user's business requirements and granted on a "need to know" basis. The purpose for their access is to maintain the system, review completed ethics forms for accuracy, notify employees of any updates/corrections that need to be made to the forms, approve forms, and run reports to track compliance/completion of ethics forms and training by employees.

In addition, consistent with the Ethics in Government Act, as amended, each agency must furnish to OGE all information and records in its possession which OGE deems necessary to the performance of its oversight responsibilities, except to the extent prohibited by law. For financial disclosure audit purposes, this typically includes copies of the disclosure reports, number of filers, and data related to filing, review, and certification timeliness. The information may be provided securely to OGE electronically or in hard-copy upon request. This system is not directly linked to OGE and information, if requested, is manually shared.

All access is granted on a need-to-know basis. FDIC follows Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☒ No
☐ Yes

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No, FDIC does not aggregate data to make program-level decisions.

9.6 Does the information system or project share PII externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used? Please explain.

As noted, consistent with the Ethics in Government Act, as amended, each agency must furnish to OGE all information and records in its possession which OGE deems necessary to the performance of its oversight responsibilities, except to the extent prohibited by law. For financial disclosure audit purposes, this typically includes copies of the disclosure reports, number of filers, and data related to filing, review, and certification timeliness. The information may be provided securely to OGE electronically or in hard-copy upon request. This system is not directly linked to OGE and information, if requested, is manually shared

Additionally, through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1360.20 "Privacy Program," and FDIC Circular 1360.17 "Information Technology Security Guidance for FDIC Procurements/Third Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.09.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: Due to the system's reliance on a commercial cloud service provider, there is a risk that the cloud service provider could potentially misuse the data.

Mitigation: Technical controls, including an encryption key management service within the vendor's cloud architecture, prevent vendor personnel from using or redistributing any FDIC data processed and stored within FDO. Should the vendor be required to access FDIC data in order to comply with federal law, or with a valid and binding order of a governmental or regulatory body, FDIC will provide the vendor with the necessary encryption keys to access the data. In the rare instances that vendor personnel have access to FDIC data because of a law enforcement requirement or court order, the vendor is obligated, by contract, to abide by all FDIC data protection requirements. Additionally, FDIC has access to the vendor's cloud hosting environment and may periodically audit the vendor to ensure information is protected in accordance with applicable contractual requirements. No additional mitigation actions are recommended.

Section 10.0: Security

Agencies should establish administrative, technical, and physical 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.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing PII.

The FDIC Privacy Program maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the CISO on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to security for FDO.

Mitigation: No mitigation actions are recommended.