FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Freedom of Information Act (FOIA) System

April 11, 2021

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 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

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government that protects the funds depositors place in banks and savings associations. FDIC makes available to the public on its website and through publications a significant amount of information about FDIC activities and FDIC-insured institutions. When individuals are unable to find the information they seek, they may file a request for access to nonpublic FDIC records under the Freedom of Information Act (FOIA). FOIA is a federal statute that provides individuals with the right, enforceable in court, to access federal agency records, except to the extent the records are protected from disclosure by any of the nine exemptions contained in the law or by one of three special law enforcement record exclusions. FOIA was amended by the Electronic Freedom of Information Act Amendments of 1996 (E-FOIA). Among other things, E-FOIA grants the public access to certain government documents via computer telecommunications.

In addition, individuals may seek access or amendment to nonpublic FDIC records about themselves under the Privacy Act of 1974 (PA). The Privacy Act is a federal statute that permits an individual to seek access to agency records pertaining to himself or herself, provided the record is maintained within a "system of records," i.e., the record is retrieved by that individual requester's name or personal identifier. Individuals seeking access to their records under the Privacy Act must provide a copy of a government-issued photo ID (e.g., a driver's license) before the records are released. The FDIC is required to process and respond to such requests in a timely manner.

Within FDIC, the Legal Division's FOIA/PA Group is responsible for administering the Corporation's FOIA/PA program. The FDIC's FOIA/Privacy Act Group has implemented a comprehensive suite of data management tools, hereinafter referred to as the "FOIA System" or "system," in order to automate compliance with record access and disclosure requirements under FOIA and other federal information regulations, as well as to enhance the availability of FDIC records to the public. The FOIA System enables the Legal Division to track and fulfill FOIA requests filed by members of the public seeking access to nonpublic FDIC records, as well as requests from individuals seeking access to or amendment of records about themselves, pursuant to the Privacy Act of 1974 (PA). The FOIA System also automates FDIC's compliance with record access and disclosure requirements under several regulations including FOIA, PA, E-FOIA and the 2005 Executive Order 13392 for Improving Agency Disclosure of Information.

The FOIA System is a Commercial Off-The-Shelf (COTS) product that consists of the following components:

1. **FOIAXpress**: FOIAXpress automates and streamlines the tracking, processing and reporting of FOIA/PA requests received by the FDIC Legal Division's FOIA/PA Group, which uses the system to:

    - Log and track the receipt and processing of each FOIA or PA request from individuals (i.e., "requesters"), using data that is either received from the requester or automatically generated by the system about the request and the requester (e.g., record number).

[1] www.fdic.gov/privacy

- Record the status of the request, relevant deadlines, and other key events or data, such as the Corporation's response to the request, and any related administrative appeals or court litigation if the request was denied.

- Scan, store, redact and manage copies of the nonpublic Corporation records that have been gathered in response to each request, some of which contain personally identifiable information (PII) about the requester or about other individuals mentioned or discussed in the scanned records.

- Track FOIA processing statistics and fees, and generate compliance reports on the number, type, and disposition of FOIA requests processed, as required by the U.S. Department of Justice.

2. **Public Access Link (PAL):** PAL is a secure web-based component that enables the public to submit and view their FOIA and PA requests; download their requested documents; and view documents in the FDIC's online Public Reading Room.

PRIVACY RISK SUMMARY

In conducting this PIA, we identified potential privacy risks, which are outlined below. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks are categorized within the following privacy functional areas:

- Data Minimization
- Use Limitation
- Data Quality and Integrity

Data Minimization Risk: There is a risk of unnecessary or excess PII being included in correspondence or other information submitted by requesters, as well as in responsive records collected by the FDIC to respond to requesters. This risk may occur when requesters file their access requests and include sensitive personal information about themselves or about other individuals in their request. Similar risks are presented by the responsive documents in the system.

Mitigation: The FDIC's Legal FOIA/PA Group has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL component of the system only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests. In addition, the Legal FOIA/PA Group does not ask requesters to provide sensitive information, such as Social Security numbers. Furthermore, when the FOIA/PA Group receives documents in response to a request, they redact any unnecessary PII from the documents when the information, if publicly disclosed, would cause a "clearly unwarranted invasion of personal privacy."[2] When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. This includes requiring requesters to submit a written attestation/certification and proof of identity, which are uploaded and appended to the relevant requester record in the system. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. No additional mitigation actions are recommended.

Use Limitation Risk: There is a potential risk that PII maintained in the system could be used or accessed inappropriately.

Mitigation: To avoid unauthorized access or disclosure, system access is restricted (by software licenses) to a limited number of FDIC staff who require system access to process FOIA and PA requests. Each user must have a valid and current password. Only the user and designated FOIA staff with administrator rights can change these passwords. In addition, all FOIA/PA Group staff are subject and must adhere to agency policies and procedures for using and safeguarding PII. All FOIA/PA Group staff receive annual Information Security

[2] See 5 U.S.C. § 552(b)(6).

and Privacy Awareness training, as well as system-specific and specialized training on FOIA and PA issues, which helps ensure PII is handled and safeguarded appropriately. No additional mitigation actions are recommended.

Data Quality and Integrity Risk: There is a potential risk associated with data quality and integrity because requester information may be manually entered into the system by FDIC staff.

Mitigation: Requester information is collected directly from the requesters to the greatest extent practicable. Specifically, the PAL component of the system allows users to enter their requests and contact information directly into the system, and they have the ability to update their information at any time, thereby helping to enhance the accuracy and timeliness of their information. In addition, the Legal FOIA/PA Group checks the accuracy and timeliness of requester information (e.g., contact information, precise scope of the request, etc.) as necessary to ensure FDIC is able to contact and appropriately respond to a requester. When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. This includes requiring requesters to submit a written attestation/certification and proof of identity, which are uploaded and appended to the relevant requester record in the system. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. Further, the system has built-in data integrity checks to ensure that certain fields are correctly populated. No additional mitigation actions are recommended.

Section 1.0: Information System

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

Each Requester File/Case Folder in the system contains the following categories of personally identifiable information (PII) and non-PII:

- **Requester Information**: When making written FOIA/PA requests, individual requesters provide both required and optional contact information, including name, address, telephone number, email address, and details about their request directly to the FDIC by mail, fax, or online via the PAL online form available on www.fdic.gov.[3] Upon receipt of a mail or fax request, authorized FOIA/PA Group staff manually enters the information provided by the requester into a new Requester File/Case Folder in FOIAXpress. Request information submitted through the PAL online form is automatically and securely uploaded to the FOIAXpress system for response and tracking by the FOIA/PA Group. Requesters may also submit a request to the FDIC through the National FOIA Portal (FOIA.gov) operated by the Department of Justice (DOJ) in accordance with the FOIA Improvement Act of 2016. (Note: Individuals wishing to submit and check their requests online need to first register on the FDIC FOIA website, and create a username and password.)

  In addition, information regarding the amount of fees paid or outstanding for each request (i.e., invoice information) is entered into the relevant file in the system by authorized Division of Finance (DOF) employees, who process payments for FOIA requests. All other payment information is managed through DOF and not retained in the system.

- **Correspondence Log Information:** In addition to the initial request, communications (e.g., letters, emails and facsimiles) to and from the requesting party may occur. Both the initial request and additional information (e.g., copy of requester's attestation/certification, proof of identification, etc.) are manually entered or scanned into the "Correspondence Log" of the system

[3] To learn more about filing a FDIC FOIA request, visit http://www.fdic.gov/about/freedom/guide.html.

by authorized FOIA Coordinators and Specialists in the Legal Division, FOIA/PA Group. Any additional correspondence sent or received is added to the relevant requester record.

- **Responsive Materials:** The system also stores copies of the materials that are responsive to the request for information (e.g., documents, e-mails, records, etc.). Responsive materials are gathered from FDIC Divisions and Offices at the request of the FOIA/PA Group. Responsive materials also may be obtained from other Federal regulatory agencies. The materials are then scanned and uploaded into the system by authorized Division/Office-level FOIA Coordinators or by FOIA Specialists in the Legal Division, FOIA/PA Group, and stored in the "File Cabinet" / "Document Management" section of FOIAXpress. Materials may consist of legal, administrative, resolution/receivership, or other nonpublic FDIC records, some of which may contain PII about the requester or about other individuals mentioned or discussed in the responsive records. Depending on the type and nature of the record, the responsive materials may include PII.

  Note: Final disposition of responsive materials, if any, is approved by appropriate delegated authority in accordance with the requirement of the FOIA, Privacy Act, and applicable FDIC regulations. Responsive materials are sent to the requester via mail, fax, secure email, encrypted CD, or via a secure download to those using the PAL option on the FDIC FOIA webpage.

- **Review Log/Case Folder Information**: Once responsive materials are redacted, they are saved in the appropriate Requester File/Case Folder in the "Document Management" section and reviewed/approved by the FOIA Supervisor by clicking on the "Review Log" tab.

- **System User Information**: The system also stores information on the identity of system users with password-protected access, including the specific record requests they worked on. The system maintains records showing who has access to the system, who are the active users, and what record requests users have been assigned to process.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☒	☐
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s)	☒	☐
Email Address	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☒	☐
Criminal Information	☒	☐
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: User name, password, information description, fee information, representative POC, system record number.)	☒	☐

1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Individuals	Members of the public and FDIC employees and contractors may file FOIA and Privacy Act requests with FDIC by mail, fax or online via the PAL request form or the National FOIA Portal operated by DOJ, as detailed in Section 1.1. These requests may include any of the information specified in Section 1.1.
FDIC Legal Division FOIA/PA Group Staff	Upon receipt of a mail, email or fax request, authorized FOIA/PA Group staff manually enter the information provided by the requester into a new Requester File/Case Folder in FOIAXpress. Authorized staff may enter or upload additional information into the system in the course of processing and responding to the requests, such as information required to verify the identity of the requester, as set out by 12 C.F.R. § 310.4, or notes from staff discussions with requesters.
FDIC Divisions and Offices	FDIC Divisions and Offices provide records that may contain information about individuals that are required to fulfill the request. These responsive documents are gathered from FOIA/PA Group records and other FDIC Divisions and Offices' records, scanned and uploaded into, and stored in the system by the Division's respective FOIA Coordinator. These documents may be redacted to protect certain information. Both original and redacted versions are stored in the system.
FDIC General Counsel	If an initial request for records is denied, either in whole or in part, the requester has the right to appeal the denial to the FDIC's General Counsel (or designee) within 30 business days after receipt of notification of the denial. The information may contain additional information relevant to consideration of the appeal. The appeal is received by the FOIA/PA Group staff, recorded in the system, and referred to the Commercial Litigation Unit, which is responsible for appellate review and for updating the system with information about the status of the appeal.
FDIC Division of Finance	The Division of Finance provides the amount of fees paid or not paid by the requester.

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

The FOIA System operates within the boundary of Windows Server with an ATO date of May 29, 2012 and is 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.

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 Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

FDIC 30-64-0022, Freedom of Information Act and Privacy Act Request Records.

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

The FDIC conducts reviews of its SORNs every three years, or as needed, to determine if revisions are required.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (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.) 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." FDIC's Legal Division uses the system to track and fulfill requests filed by members of the public seeking access to nonpublic FDIC records under the Freedom of Information Act (FOIA), and requests from individuals seeking access under the Privacy Act of 1974 (PA) to nonpublic FDIC records, if any, about themselves. Individuals seeking access to records pertaining to them must include appropriate proof of identity. To establish proof of identity, requesters must send the FDIC either of the following: a certification of a duly commissioned notary public attesting to his or her identity, or an unsworn declaration subscribed to as true under the penalty of perjury. Requesters must also attach copy of a government-issued photo ID, such as a driver's license, to their request. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. This same process is followed for agency referrals.

The FDIC notifies the public, including FOIA/PA requesters, and FOIAXpress system users, about what information is collected in the system, and how it is used and disclosed, through applicable system of records notices that the FDIC publishes in the *Federal Register* and posted online. The FDIC's website also contains information on FOIA and the Privacy Act at https://www.fdic.gov/about/freedom/other.html.

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.

This PIA and the associated SORN, FDIC 30-64-0022, Freedom of Information Act and Privacy Act Request Records, provide constructive notice of the FDIC's information collection practices. The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records Clearance Officer and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII. See https://www.fdic.gov/about/privacy/protecting.html.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There are no identifiable risks associated with transparency for FOIA.

Mitigation: No 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?

The FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA. Additionally, individual requesters using the PAL online request feature on the FDIC FOIA webpage only have access to their own registration and request information.

The FOIA & Privacy Act Group is responsible for processing all FOIA and Privacy Act requests received by the FDIC. Individuals, partnerships, corporations, associations, or public or private organizations may make a request on the FOIA website at https://www.fdic.gov/about/freedom/other.html. Requests also can be made by writing to the FDIC, Legal Division, FOIA/PA Group, 550 17th Street, N.W., Washington, D.C. 20429 or by sending the request by fax to 703-562-2797 or by email to efoia@fdic.gov.

When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. To establish proof of identity, requesters must provide either of the following: (1) a certification of a duly commissioned notary public attesting to his or her identity, or (2) an unsworn declaration subscribed to as true under the penalty of perjury. In addition, requesters must attach copy of a government-issued photo ID, such as a driver's license. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. This same process is followed for agency referrals.

If an initial request for records is denied, either in whole or in part, the requester has the right to appeal the denial within 30 business days after receipt of notification of the denial.

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

The FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA. In addition, the PAL website enables the public to submit and view their FOIA and PA requests; download their requested documents; and view documents in the FDIC's online Public Reading Room. If an initial request for records is denied, either in whole or in part, the requester has the right to appeal the denial.

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

The system enables the Legal Division to track and fulfill FOIA requests filed by members of the public seeking access to nonpublic FDIC records, as well as requests from individuals seeking access to or amendment of records about themselves, pursuant to the Privacy Act of 1974 (PA). Additionally, the FDIC has a process for disseminating corrections or amendments of collected PII, the procedures for which are published in FDIC SORNs 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 risks associated with access and amendment for FOIA.

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 Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

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 PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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?

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/about/privacy/index.html.

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

Contractors may be employed to provide support and maintenance of this system. Due to the contractors' access to PII, contractors are required to 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, Confidentiality Agreements have been completed and signed for contractors who work on the information system or project. 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 is currently in the process of implementing 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.

System-specific training is required for all users of the FOIA System. This training has specific information regarding the compromise of data, including PII, and how to prevent its misuse. Additionally, the FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. 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 staff 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 following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

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

The system includes automated checks to ensure that the data entered by FOIA/PA Group staff is complete (e.g., mandatory fields are not left blank). In addition, 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 if possible. FDIC also 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, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using FOIAXpress.

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 FDIC Circular 1031.1.

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 FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for the system.

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: Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819); Freedom of Information Act (5 U.S.C. 552), the Privacy Act of 1974 (5 U.S.C 552a), and 12 CFR parts 309 and 310. In addition, the FOIA Improvement Act of 2016 requires the Federal government to create a consolidated online request portal that allows a member of the public to submit a request for records to any agency from a single website. Information related to FOIA/PA requests is collected, maintained, used, and disseminated in accordance with FDIC SORN 30-64-0022, Freedom of Information Act and Privacy Act Request Records.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with authority for FOIA.

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 personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

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. Only a minimal amount of PII is required online to register a requester and process a request. In addition, the FDIC's Legal FOIA/PA Group has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL component of the system only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests. Also, the Legal FOIA/PA Group does not ask requesters to provide sensitive information, such as Social Security numbers. Furthermore, when the FOIA/PA Group receives documents in response to a request, they redact any unnecessary PII from the documents when the information, if publicly disclosed, would cause an unwarranted invasion of personal privacy.[4] When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. To establish proof of identity, requesters must send the FDIC either of the following: (1) a certification of a duly commissioned notary public attesting to his or her identity, or (2) an unsworn declaration subscribed to as true under the penalty of perjury. In addition, requesters must attach copy of a government-issued photo ID, such as a driver's license. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. This same process is followed for agency referrals.

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?

Only a minimal amount of PII is required online to register a requester and process a request. Also, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding 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?

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of 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.

All information processed through the system is maintained exclusively in electronic form. 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. The system is configured to retain electronic data in accordance with the FDIC Records Schedule. Data in the information system is not monitored. Additionally, records are retained in accordance with the FDIC Circular 1210.1, FDIC Records and Information Management Policy Manual, and the following FDIC Records Retention Schedule: "Electronic Information Systems schedule, EIS1002." 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 1210.1 and 1360.9.

[4] See 5 U.S.C. § 552(b)(6).

6.5 What are the policies and procedures that minimize the use of personally identifiable information (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 is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize 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: There is a risk of unnecessary or excess PII being included in correspondence or other information submitted by requesters, as well as in responsive records collected by the FDIC to respond to requesters. This risk may occur when requesters file their access requests and include unnecessary or excess personal information about themselves or about other individuals in their requests. Similar risks are presented by the responsive documents.

Mitigation: The FDIC's Legal FOIA/PA Group has taken steps to minimize the amount of information that the agency collects and maintains while processing requests. For example, the PAL feature only asks for the minimum amount of contact information necessary to communicate with requesters and respond to requests. In addition, the Legal FOIA/PA Group does not ask requesters to provide sensitive information, such as Social Security numbers. Furthermore, when the FOIA/PA Group receives documents in response to a request, they redact any unnecessary PII from the documents when the information, if publicly disclosed, would cause an unwarranted invasion of personal privacy.[5] When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. This includes requiring requesters to submit a written attestation/certification and proof of identity, which are uploaded and appended to the relevant requester record in the system. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. No additional mitigation actions are recommended.

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond what is necessary.

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

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.

PII stored in the system about requesters is collected directly from the requesters themselves (i.e., their FOIA and/or PA requests and related communications) or is generated and entered by the Legal FOIA/PA Group. The Legal FOIA/PA Group checks the accuracy and timeliness of this information (e.g., contact information, precise scope of the request) as necessary to allow FDIC to contact or respond to a requester, as well as to ensure that FDIC staff are able to accurately interpret and handle

[5] See 5 U.S.C. § 552(b)(6).

the request. Furthermore, as set out by 12 C.F.R. § 310.4, when the request is from an individual seeking access to his or her own records under the Privacy Act, the Legal FOIA/PA Group may require additional verification of that requester's identity when reasonably necessary to assure that records are not disclosed to someone other than the requester (or the requester's representative). This includes requiring requesters to submit a written attestation/certification and proof of identity, which are uploaded and appended to the relevant requester record in the system. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester.

The Legal FOIA/PA Group does not correct the accuracy or timeliness of responsive documents that are scanned into the system, including any PII that may be contained in such documents. The FDIC is required under the FOIA to grant or deny access to responsive records "as is," without alteration. The accuracy and timeliness of the information (including any PII) contained in such records, would be governed by other laws and authorities, if any, applicable at the time the agency compiles those records (e.g., FDI Act, personnel laws, administrative or court evidentiary rules and procedures).

The system also has built-in data integrity checks to ensure that certain fields are correctly populated. In addition, the FDIC reviews privacy artifacts for adequate measures 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?

Requester information is collected directly from the requesters to the greatest extent practicable. Information also may be collected through FOIA referrals from other agencies. Requesters or their representatives are responsible for providing accurate data to the FDIC or other agencies to process their request. The FOIA/PA Group is responsible for verifying the accuracy and timeliness of initial request information (e.g., contact information, precise scope of the request) that they input into the system.

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

Accuracy is critical to ensure the appropriate response to the request, as well as to ensure that the identity of the individual seeking access to his or her own records under the Privacy Act. For example, the identity of a PA requester is appropriately verified by FOIA/PA Group staff to prevent unauthorized disclosure. In addition, the FDIC reviews privacy artifacts to ensure adequate measures to check for and correct any inaccurate or outdated PII in its holdings.

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.

The Legal Division's FOIA Program Manager/Data Owner is responsible for the management and oversight of the data. In addition, through its PTA adjudication process, the FDIC Privacy Program utilizes 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 prescribes 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, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a potential risk associated with data quality and integrity because requester information may be manually entered into the system by FDIC personnel.

Mitigation: Requester information is collected directly from the requesters to the greatest extent practicable. Specifically, the PAL component of the system allows users to enter their requests and contact information into the system, and they have the ability to update their information at any time, thereby helping to enhance the accuracy and timeliness of their information. In addition, the Legal FOIA/PA Group checks the accuracy and timeliness of requester information (e.g., contact information, precise scope of the request, etc.) as necessary to ensure FDIC is able to contact and appropriately respond to a requester. When a requester is seeking his or her own information under the PA, the FOIA/PA Group verifies the individual's identity as required in 12 C.F.R. § 310.4 before disclosing the records to him/her. This includes requiring requesters to submit a written attestation/certification and proof of identity, which are uploaded and appended to the relevant requester record in the system. As a regular course of business, FOIA analysts perform quality checks to ensure that the requester's attestation and proof of identity appear to be legitimate and match the information provided by the requester. Additionally, all requests are carefully reviewed by the supervising attorney prior to releasing records to the requester. The system also has built-in data integrity checks to ensure that certain fields are correctly populated. No additional mitigation actions are recommended.

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, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (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. 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.

8.3 Explain how the information system or project obtains consent, where 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 Privacy Act SORN(s) as well as the relevant PIA.

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

The system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN 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.

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, https://www.fdic.gov/about/privacy/index.html, instructs viewers 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 risks associated with individual participation for FOIA.

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 intended use of the PII in the system is to enable the Legal Division to track and fulfill FOIA/PA requests filed by members of the public seeking access to nonpublic FDIC records, as well as requests from individuals seeking access to or amendment of records about themselves, pursuant to the Privacy Act of 1974.

FOIA Division/Office Coordinators may also run reports of their FOIA activity for their supervisors to allow for appropriate supervisory oversight and exercise of delegated authority. These reports generally include PII, such as the name of the requester, description of the request, results of the request (denied, granted), date of request, etc. In addition, FOIA Division/Office Coordinators may provide their supervisors with copies of records that are potentially responsive for review and approval prior to release to ensure those records are accurate and responsive to the request.

The FOIA/PA Group provides notice of potentially sensitive FOIA requests to authorized staff within the Legal Division and Executive Management for awareness of operational impacts. The notice includes the name of the requester, description of the request, and the date the response is due. In addition, Executive Management is typically provided copies of records that are potentially responsive to sensitive requests for review and approval prior to release.

9.2 Describe how the information system or project uses personally identifiable information (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, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

The Legal Division's FOIA Program Manager/Data Owner is responsible for the management and oversight of the data. Additionally, an audit trail process captures actions performed on any of the data objects. An application-specific Security Awareness Training and a Corporate Security Awareness and Privacy Orientation, which includes Rules of Behavior, are mandatory trainings for all users of the FOIA System to assure proper use of data. Additionally, FOIA/PA staff in the FDIC's Legal Division have User IDs and password-protected access to the records as necessary to prepare responses to FOIA/PA requests and appeals and to prepare periodic reports, as required by law. The FDIC notifies the public, including FOIA/PA requesters, and FOIAXpress system users about what information is collected in the system, and how it is used and disclosed, through applicable system of records notices that the FDIC has published in the *Federal Register* and posted online.

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 authorized FDIC users who have access to data in the system must have the approval of the FOIA Program Manager/Data Owner in the FDIC Legal Division before access is granted to the system. Additionally, the system's functional security limits a user's access to specific functions and regulates a user's ability to update data for a specific function. All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. However, there is some risk that requesters may include sensitive personal information about themselves, or about other individuals in their request, when filing their access request. Similar risks are presented by entering data into the system's responsive documents. This information could then be compromised by unauthorized access or disclosure.

Individual requesters using the PAL online request feature on the FDIC FOIA webpage only have access to their own registration and request information. FDIC user access is controlled by the user group permissions. FDIC users' access will be restricted into the following user groups: Accounting (Division of Finance), FOIA System Administrators, FOIA Coordinators, FOIA Management (i.e., Supervisors), and FOIA Specialists. Each user group will have specific system, file cabinet (document repository) and case function privileges dependent on their respective roles.

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

☒ No
☐ Yes

No other FDIC systems have a direct interface with FOIA. All responsive materials provided by other FDIC Divisions and Offices are manually scanned and uploaded into FOIAXpress by authorized FDIC FOIA/PA Group staff.

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?

The system data is not consolidated in a way that would yield personally identifiable information not already known in the system. The requester file in the FOIA System contains data entered/uploaded by the Legal Division FOIA/PA Group staff, including responsive materials obtained from FDIC Division/Programs or other Federal regulatory agencies.

9.6 Does the information system or project share personally identifiable information (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.

Data in the system is not shared with any other agencies, except in limited circumstances when it is necessary to refer a FOIA request to another Federal agency's FOIA office for a response. In such cases, only that information which is relative and necessary to the referral is provided to the other agency. Also, derived statistical data is sent to the Department of Justice for compliance reporting purposes. No personal information about requesters is provided in these compliance reports.

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.

Data in the system is not shared with any other agencies, except in limited circumstances as described above. Annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties and the prevention of its misuse.

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 Legal Division FOIA System Program Manager/Data Owner is contacted and responsible for determining when to refer a FOIA request to another Federal agency for response. In such cases, only that information which is relative and necessary for the agency to respond to the data owner's request is referred to the agency. Additionally, 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: There is a potential risk that PII maintained in the system could be used or accessed inappropriately.

Mitigation: To avoid unauthorized access or disclosure, system access is restricted to a limited number of FDIC staff who require system access to process FOIA and PA requests. Each user must have a valid and current password. Only the user and designated FOIA staff with administrator rights can change these passwords. In addition, all FOIA/PA Group staff are subject and must adhere to agency policies and procedures related to FOIA and PA, as well as those for handling and safeguarding PII. All FOIA/PA Group staff receive annual Information Security and Privacy Awareness training, as well as system-specific and specialized training on FOIA and PA issues, which helps ensure PII is handled and safeguarded appropriately. 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 personally identifiable information (PII).

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

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 Chief Information Security Officer (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 associated with security for the system.

Mitigation: No mitigation actions are recommended.