FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Receivership Investigations

March 31, 2022

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

The Federal Deposit Insurance Corporation (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, and managing receiverships. FDIC handles the resolution of failing FDIC-insured financial institutions and provides prompt, responsive, and efficient administration to maintain confidence and stability in our financial system, to minimize losses, and to ensure continuity of financial services for financial institution customers. The FDIC, as Receiver, succeeds to all rights, titles, powers, privileges, and assets of the failed institution. As successor to the failed institution, the FDIC has the statutory duty to pursue each viable claim of the institution against those who may have caused losses or those who insured the institution against losses. Those claims with merit and deemed to be cost-effective are pursued until a settlement is reached with the defendant(s) or a judgment is rendered. Those without merit are closed out.

The FDIC's right and obligation, as Receiver, to pursue all legal courses of action for sources of recovery would be limited if it did not include the collection of criminal restitution actions awarded to failed financial institutions. Criminal cases are a potential source of recovery to the FDIC through restitution orders. Restitution orders are awarded by the courts as part of the sentencing of defendants, to repay financial institutions for criminal acts that caused losses to the financial institutions. The FDIC Investigations Department works with the U.S. Department of Justice to collect amounts due from federal criminal restitution orders, with state probation offices or in its own capacity to collect on state criminal restitution orders.

FDIC uses a combination of systems, the Receivership Investigations Systems, to track investigation information, professional liability claims, and criminal restitutions. The Receivership Investigations Systems are comprised of the following four basic components:

1. The first component is institutional. This contains the name of the failed institution and the transaction involved with the failure. There is no Personally Identifiable Information (PII) contained in this component of the Receivership Investigations Systems.

2. The second component contains non-PII and limited PII pertaining to each professional liability claim (e.g. Bond, Director and Officer Liability, Attorney Malpractice, Account Malpractice, Appraiser Malpractice, and Other). This component is used to track each claim to conclusion. Within this section, tracking is also maintained for those judgment, settlements, or note receivables that are obtained from either individuals or firms/companies. Within the judgments, settlements or note receivables, the Receivership Investigations Systems have sub-screens, with the ability to track individual defendants by name. These are rarely used for the individuals. In this section, the Receivership Investigations Systems also track payments from insurance companies, individual firms or companies and individual defendants.

3. The third component of the Receivership Investigations Systems contain PII and non-PII pertaining to criminal restitutions. Within this section, the name of the defendant, status of the order, the amount of the order, Social security Number (SSN) and payment histories are included. The Receivership

[1] www.fdic.gov/privacy

Investigations Systems store and track payments received from criminal restitutions from failed financial institutions.

4. The fourth component consists of Directors and Officers as Persons of Interest (POIs) who are named either in an approved Board case or actual filed complaint. This section also has the capability to identify these individuals by SSN, and birth date.

FDIC acquires data processed within the Receivership Investigations Systems from a failing institution, from the FDIC team finalizing the closing of an institution, or from the courts further to the filing of a Judgment and Commitment Order. Additionally, data may be derived from other FDIC systems, the Department of Justice (DOJ), state agencies, and/or third-party sources. Authorized FDIC Investigations personnel manually input data into the Receivership Investigations Systems.

Each professional liability claim and criminal restitution in the Receivership Investigations Systems also contain a "Comments" field. While the "Comments" field is generally used to track the status of the case, sensitive information and/or PII about individuals associated with the case could potentially be entered into this field. Additionally, the Receivership Investigations Systems do not contain a field for address information; this information is typically acquired from the courts or from DOJ and, if it is retained, it is included in the "Comments" field for the relevant section.

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 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
- Access and Amendment
- Minimization
- Data Quality and Integrity
- Individual Participation

Transparency

Privacy Risk: Receivership Investigations Systems contain third-party data from financial institutions and government agencies, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection, use, processing, storage, maintenance, dissemination, and disclosure of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC.

Mitigation: This PIA serves as notice to the general public regarding the collection and use of information in the Receivership Investigations Systems to fulfill FDIC's corporate and receivership responsibilities. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. Specifically, in cases where the Receivership Investigations Systems imports or derives PII from other FDIC Privacy Act Systems of Records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. In cases where PII is received from financial institutions, government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. On occasions when notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

Access and Amendment

Privacy Risk: There is a risk that individuals are not able to access and amend information about themselves within the Receivership Investigations Systems.

Mitigation: Since the Receivership Investigations Systems collects records gathered from other agencies' recordkeeping systems and third-party sources, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases where Receivership Investigations Systems import or derive PII from other FDIC Privacy Act SORs, individuals seeking access to any record contained in those SORs may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or FOIA (for all individuals) request to FDIC in writing or electronically at www.fdic.gov/policies/privacy/request.html.

However, depending on the nature of the records being processed, FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal an investigative or enforcement interest on the part of FDIC. In cases where receivership investigations systems receive PII from financial institutions or other government agencies, individuals should contact the source entities and agencies that originated their data to access and amend their information.

Minimization

Privacy Risk: The Receivership Investigations Systems do not yet have an established records retention schedule.

Mitigation: FDIC is currently engaged in a large effort to establish formal retention schedules for all systems. Also, FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

Data Quality and Integrity

Privacy Risk: There is a potential risk associated with data quality and integrity because information processed by the Receivership Investigations Systems could be inaccurate or incomplete.

Mitigation: The Receivership Investigations Systems' program managers verifies the completeness of the data within the systems and is responsible for the proper use and integrity of the data maintained in the system.

Individual Participation

Privacy Risk: In cases where individuals do not provide personal information directly to the FDIC, they may be unaware that the FDIC maintains their PII. Additionally, individuals are generally not provided with an opportunity to consent to or opt out of the FDIC's collection and use of their PII as part of enforcement actions.

Mitigation: In cases where PII is received from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. In addition, the FDIC is required to collect and maintain the PII in accordance with a legally authorized purpose.

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?

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) (non-work)	☐	☒
Email Address (non-work)	☐	☒
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	☐	☒

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

Data Source	Description of Information Provided by Source
FDIC Receivership Investigations Staff	Authorized Investigations staff manually enters data into the Receivership Investigations Systems during the course of their investigative work and analysis from failed financial institutions. Part of the data is based on Judgment and Commitment Orders from the courts. Certain data may be derived from information collected from the failed financial institution, in both hard copy and electronic format. FDIC Investigations staff may obtain data by inventorying the desks of key bank personnel at the failed institution; auditing expense accounts; reviewing loan files; examining board of directors' minutes; tracing loan proceeds; reviewing data captured by FDIC from certain hard drives, file shares and/or emails off of the failed institution's exchange server; and interviewing key failed institution personnel. Other sources of data may include information from other FDIC systems, such as information about payments from the New Financial Environment (NFE).
Department of Justice (DOJ)	The Criminal Restitution component within the Receivership Investigations Systems is derived from information provided by the DOJ at the request of FDIC Investigations staff. This information includes information relating to collection activity on criminal restitution orders. The information provided may include name, address, and SSN.
State and Local Agencies	The FDIC Investigations staff may obtain data from State Officials whose court handled the case or other state agencies, such as the State Division of Corporation, State Business and Labor, and Secretary of State. The information obtained from these state agencies is used by the FDIC Investigation staff to confirm collection activity for criminal restitution orders. Additionally, FDIC Investigations staff may obtain a Judgment and Commitment Order from the courts providing criminal restitution data of individuals convicted of contributing to the failure of a financial institution.
Credit Report Bureaus	FDIC Investigation staff may request credit reports, such as debts and the location of assets from credit reporting bureaus.
Commercial Database and Third-Party Services:	The FDIC Investigation staff utilizes commercial databases and third-party data aggregator services to establish or confirm an individual's asset information, in order to collect on active criminal restitutions or pursue collection on professional liability claims.
New Financial Environment (NFE)	Receivership collections and expense accounting
Communication, Capability, Challenge and Control (4C)	Professional liability claims and restitution orders account information.

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

All FDIC information systems must achieve an Authority to Operate (ATO) via the Assessment and Authorization process that aligns with the Risk Management Framework. Information systems that process receivership investigations information have been granted ATO or are in the process to achieve ATO. The ATO for each FDIC system 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 Privacy Act SORN-013, Insured Financial Institution Liquidation Records, applies to the receivership investigations process.

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

No. The SORN listed in Question 2.2 does not require amendment or revision. Generally, the FDIC conducts a review of its SORNs every three years or as needed.

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."

Since the Receivership Investigations Systems collects information from third-party sources, it is not always possible or practical to provide notice to individuals prior to the collection and processing of their information within the receivership investigations system. Nonetheless, the FDIC provides notice to individuals at the original point of collection wherever possible. For example, in cases where the Receivership Investigations Systems imports or derives PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. In addition, this PIA serves as notice to the public about FDIC's collection and use of information in the receivership investigations system. When the Receivership Investigations Systems receives data from a financial institution, government agency or other third-party entity, it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information.

When FDIC collects information as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is

governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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: Receivership Investigations Systems contain third-party data from financial institutions and government agencies, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection, use, processing, storage, maintenance, dissemination, and disclosure of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC.

Mitigation: This PIA serves as notice to the general public regarding the collection and use of information in the Receivership Investigations Systems to fulfill FDIC's corporate and receivership responsibilities. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. Specifically, in cases where the Receivership Investigations Systems import or derive PII from other FDIC Privacy Act Systems of Records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. In cases where PII is received from financial institutions, government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. On occasions when notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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?

Because the Receivership Investigations Systems process information from third-party sources pursuant to investigation requirements, they are not designed and do not have procedures to allow individuals to access their information. However, in cases where the Receivership Investigations systems process information about individuals imported from other FDIC Privacy Act Systems of Records (SORs), the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and 12 C.F.R. § 310. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each SOR, as specified by the Privacy Act and 12 C.F.R. § 310.3 and 310.4. 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. Depending on the nature of the records being processed (and any applicable Privacy Act exemptions), FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal a prospective enforcement or investigative interest on the part of FDIC.

In addition, the Receivership Investigations Systems process data from financial institutions, government agencies or other third-party entities. The system does not have procedures for individual access in these cases. Individuals should contact these source entities directly for access to their personal information.

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

Because the Receivership Investigations Systems process information from third-party sources pursuant to investigation requirements, it is not designed to allow individuals to correct inaccurate or erroneous information about themselves. Therefore, the systems do not have Privacy Act redress procedures. However, in cases where the Receivership Investigations Systems import or derive PII from other FDIC Privacy Act Systems of R(SORs), the FDIC allows these individuals to correct or amend PII maintained by the FDIC in the respective source systems of records as specified by the Privacy Act and 12 C.F.R. § 310. The procedures for correcting inaccurate data are provided in related the FDIC-013, Insured Financial Institution Liquidation Records SORN. Individuals seeking to correct inaccurate data in the source systems can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. These requests are subject to any applicable Privacy Act exemptions intended to prevent harm to FDIC's investigation and enforcement interests. In addition, this PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Program.

In cases where the Receivership Investigations Systems receives third-party data from banks or government agencies, the FDIC does not have the ability to implement procedures to allow individuals to correct inaccurate or erroneous information within the Receivership Investigations Systems. Individuals should contact their bank or the government agency directly to correct any erroneous or inaccurate information.

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

Because the Receivership Investigations Systems process information from third-party sources pursuant to investigation requirements, it is not designed to allow individuals to correct inaccurate or erroneous information about themselves. However, the Receivership Investigations Systems process information about individuals derived from other FDIC Privacy Act systems of records, and the FDIC allows these individuals to be notified about procedures to correct or amend PII maintained in the respective source systems as specified by the Privacy Act and 12 C.F.R. § 310. The notification procedures are provided in related the FDIC-013, Insured Financial Institution Liquidation Records SORN. Individuals seeking to correct inaccurate data can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. In addition, this PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In some cases, the Receivership Investigations Systems process data from banks, government agencies or other third-party entities. Individuals should contact these entities directly for access to their personal information.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There is a risk that individuals are not able to access and amend information about themselves within the Receivership Investigations Systems.

Mitigation: Since the Receivership Investigations Systems collects records gathered from other agencies' recordkeeping systems and third-party sources, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases where the Receivership

Investigations Systems import or derive PII from other FDIC Privacy Act Systems of Records (SORs), individuals seeking access to any record contained in those SORs may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or FOIA (for all individuals) request to FDIC in writing or electronically at www.fdic.gov/policies/privacy/request.html. However, depending on the nature of the records being processed, FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal an investigative or enforcement interest on the part of FDIC. In cases where receivership investigations systems receive PII from financial institutions or other government agencies, individuals should contact the source entities and agencies that originated their data to access and amend their information.

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 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?

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 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program"). PIAs are posted on FDIC's public-facing website, www.fdic.gov/privacy.

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

Contractors are responsible for designing, developing, troubleshooting, applying corrections, and implementing enhancements to systems maintained by FDIC based on evolving business requirements and discovery of security vulnerabilities and system functionality defects. Contractor access is typically limited to the Development and Quality Assurance (QA) versions of most systems; however, if there is a need for contractor administrator-level support, some contractors may be granted access to the production versions and data contained within.

All individuals that have access to applications complete a Contractor Confidentiality Agreement and Non-Disclosure Agreement appropriately. All contractors must also pass a background check.

Due to 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, Contractor Confidentiality Agreements have been completed by contractors who support FDIC receivership investigations. Access to individual's PII is role-based and minimized. All contractors must also pass a background check. Additionally, 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.

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?

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. 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 SOR under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program." 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 FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program."

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 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program."

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to accountability for the Receivership Investigations Systems.

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. These particular systems collect PII pursuant to the following laws and regulations:

- 12 U.S.C. 1821: deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 U.S.C. 1822: deals with FDIC as a Receiver of failed banks

- Executive Order 9397: stipulates the requirement for the use of SSNs by President Roosevelt
- 12 CFR 366: deals with FDIC contractors

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority, as FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIA and the development and review of SORNs.

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?

The Receivership Investigations Systems only collect information for which the FDIC has the authority to collect pursuant to the pursuit of each viable claim of an institution against those who may have caused losses or those who insured the institution against losses in its capacity as Receiver. The Receivership Investigations Systems leverage an access control system to restrict user view and edit rights to the minimum necessary to perform tasks aligned with their user role. This includes limiting access to the Receivership Investigations Systems tools and data contained therein to only those authorized users with a need-to-know.

Additionally, through the conduct, evaluation and review of privacy artifacts,[2] 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?

All FDIC personnel are required to complete annual information security and privacy awareness training. This is required for the receivership investigations systems' end-users prior to gaining access to the systems. This online training addresses how to determine what constitutes PII and how to handle it. In addition, breach prevention is addressed in the training. the receivership investigations systems have built-in user security features to help manage and restrict what information users have access to on a "need-to-know" basis and according to their work responsibilities. These user security permissions are controlled by the receivership investigations systems administrators.

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 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?

[2] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

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.

FDIC is in the process of developing a records schedule for the Receivership Investigations Systems.

Information related to the retention and disposition of data are captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Directives 1210.01, "Records and Information Management Program" and 1360.9, "Protecting Sensitive Information."

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. The project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: The Receivership Investigations Systems do not yet have an established records retention schedule.

Mitigation: FDIC is currently engaged in a large effort to establish formal retention schedules for all systems. Also, FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

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.

The Receivership Investigations Systems program managers are responsible for the proper use and integrity of the data maintained in the system. The data within the components of the Receivership Investigations Systems is verified for completeness on a case-by-case basis and this verification is measured by the program managers.

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?

Systems involved in the receivership Investigations process receive third-party data from banks, federal, state and local agencies, and credit monitoring services. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information collected from those entities.

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 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.

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 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, 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 information processed by the Receivership Investigations Systems could be inaccurate or incomplete.

Mitigation: The Receivership Investigations Systems' program managers verify the completeness of the data within the systems and are responsible for the proper use and integrity of the data maintained in the systems.

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.

Because the Receivership Investigations Systems process information from third-party sources pursuant to investigation requirements, it is not always possible or practical to provide notice and choice opportunities to individuals prior to the collection and processing of their information within the Receivership Investigations Systems. Wherever feasible, FDIC provides notice and relevant consent options to individuals at the original point of collection. For example, in cases where the Receivership Investigations Systems import or derive PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When the Receivership Investigations Systems receive third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII.

When FDIC collects information as part of an ongoing investigation, individuals may not receive notice (or consent opportunities) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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.

As detailed above in Section 8.1, the systems process information collected from other agency record systems and third-party sources to pursue all legal courses of action for sources of recovery as is required of the FDIC in its role as Receiver for a failed financial institution. Therefore, opportunities for providing individualized notice and consent options may be limited or non-existent. In cases where the Receivership Investigations Systems import or derive PII from other FDIC record systems, the FDIC provides notice and consent opportunities to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When the Receivership Investigations systems receive third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII.

When FDIC collects information pursuant to an ongoing investigation, individuals may not receive notice (or the opportunity to consent) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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.

Systems supporting the receivership investigations process receive data from third-parties. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant third party's privacy notices. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

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, 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: In cases where individuals do not provide personal information directly to the FDIC, they may be unaware that the FDIC maintains their PII. Additionally, individuals are generally not provided with an opportunity to consent to or opt out of the FDIC's collection and use of their PII as part of enforcement actions.

Mitigation: In cases where PII is received from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. In addition, the FDIC is required to collect and maintain the PII in accordance with a legally authorized purpose.

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 data collected as part of FDIC Receivership Investigation activities is used to ensure FDIC can pursue all legal courses of action for sources of recovery as is required of the FDIC in its role as Receiver for a failed financial institution. The FDIC, as Receiver, succeeds to all rights, titles, powers, privileges, and assets of the failed institution, and this includes the statutory duty to pursue each viable claim of the institution against those who may have caused losses or those who insured the institution against losses.

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.

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.

FDIC application Program Managers and Data Owners are responsible for the management and decision authority over a specific area of corporate data. Program Managers/Data Owners have overall responsibility for protecting the privacy rights of individuals by developing data access guidelines and standards which must be followed. Additionally, Program Managers/Data Owners and Information Security Managers serve as the source of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

Although the Program Managers/Data Owners and Information Security Managers share this data responsibility, it is every user's responsibility to abide by FDIC data protection rules that are outlined in the Corporate Security and Privacy Awareness Training, 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.

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 users that require access to applications involved in FDIC Receivership Investigations must submit a request using the FDIC's Access Request and Certification System (ARCS) and have the approval of their Manager and the application Access Approver prior to being granted authority to use the system. Users are provided a role that limits their view of data only to the data needed to complete their job task. Per FDIC Circular 1360.15, user access levels are reviewed periodically to ensure they reflect current business needs.

All access is granted on a need-to-know basis. 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 The Receivership Investigations Systems interface with a number of FDIC systems.

- **Advanced Legal Information System (ALIS) and Receivership Oversight Management System (ROMS):** ALIS has direct access to populate the Matter and Budget staging tables in the Receivership Investigations Systems and retrieve Claim and Payment information. ROMS has direct access to the databases on the Receivership Investigations Systems.
- **Communication, Capability, Challenge, and Control (4C) and Track and Route Authorization Cases (TRAC):** The Receivership Investigations Systems have direct read-only access to the 4C and TRAC databases. The Receivership Investigations Systems access the TRAC database to get case numbers for a claim or restitution asset. Receivership Investigations Systems access 4C for professional liability claims and restitution orders account information.
- **Receivership Asset Accounting (RAA)**: Receivership Investigations Systems retrieve payment information from RAA.
- **New Financial Environment (NFE)**: Data exchange is performed indirectly between the Receivership Investigations Systems and for Investigations' assessment of a claim's damages/possible recovery against all costs associated with the claim.
- **Financial and Management Reporting Portal (F&MR Portal):** Claims and Authority to Sue data is obtained from the Receivership Investigations Systems for awareness and analysis.

These system interfaces allow for system-to-system information to be accessed for tracking and reporting purposes, and Investigations staff are only required to complete minimal data entry. Certain data may also be derived from information collected from the failed financial institution, in both hard copy and electronic format. FDIC Investigations staff may obtain data by inventorying the desks of key bank personnel at the failed institution; auditing expense accounts; reviewing loan files; examining board of directors' minutes; tracing loan proceeds; and reviewing data captured by FDIC Bank Data Services (FBDS). Authorized staff manually enters data into the Receivership Investigations Systems during the course of their investigative work and analysis from failed financial institutions.

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 programmatic level decisions.

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.

Department of Justice (DOJ): The Criminal Restitution components within the Receivership Investigations Systems are derived from information provided by the DOJ at the request of FDIC Investigations staff. This information includes information relating to collection activity on criminal restitution orders. The information provided may include name, address, and SSN. There is an existing agreement with DOJ from 1992, but most of the other sharing is done on an individual case basis working with FDIC Legal, the Office of Inspector General, and the Federal Bureau of Investigation.

State and Local Agencies: The FDIC Investigations staff may obtain data from State Officials whose court handled the case or other state agencies, such as the State Division of Corporation, State Business and Labor, and Secretary of State. The information obtained from these state agencies is used by the FDIC Investigation staff to confirm collection activity for criminal restitution orders. Additionally, FDIC Investigations staff may obtain a Judgment and Commitment Order from the courts providing criminal restitution data of individuals convicted of contributing to the failure of a financial institution.

Credit Report Bureaus: When legally permissible, FDIC Investigation staff may request credit reports, such as debts and the location of assets from credit reporting bureaus.

Commercial Database and Third-Party Services: The FDIC Investigation staff utilizes commercial databases and third-party data aggregator services to establish or confirm an individual's asset information, in order to collect on active criminal restitutions or pursue collection on professional liability claims.

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, FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) 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, "Information Technology Security Guidance for FDIC Procurements/Third Party Products" and FDIC Circular 1360.9, "Protecting Sensitive Information."

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 staff 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: There are no identifiable risks associated with use limitation. Through role-based access, employee training, and the review of privacy artifacts, FDIC ensures that PII is used only for authorized purposes.

Mitigation: No 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).

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 associated with security for these systems.

Mitigation: No mitigation actions are recommended.