FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Receivership Data Administration

March 30, 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 personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

When a financial institution closes, its chartering authority typically appoints the FDIC as receiver, responsible for resolving the failed institution. The FDIC employs a variety of strategies and business practices to resolve a failed institution. Depending on the characteristics of the institution, the FDIC may use several of these methods to ensure the prompt and efficient payment of deposit insurance to insured depositors, to minimize the impact on the Deposit Insurance Fund, and to speed dividend payments to uninsured depositors and other creditors of the failed institution. Once the FDIC has completed the disposition of the receivership's assets and has resolved all obligations, claims, and other legal impediments, the receivership is terminated, and a final distribution is made to its creditors. A receivership is created when the FDIC takes on custodial responsibility for the disposition of a failed institution. The FDIC in its capacity as a receiver is responsible for resolving all obligations, claims, and other legal activities of the failed financial institution. Under the Federal Deposit Insurance (FDI) Act, the chartering authority for a failed financial institution appoints the FDIC as the receiver,[2] and the FDIC Division of Resolutions and Receiverships (DRR) leads the administration of the receivership.

The most common, and preferred, method for resolving a failing financial institution is a Purchase and Assumption (P&A) transaction, whereby a healthy institution (acquiring institution) agrees to purchase some or all of the assets and assume some or all of the liabilities (including insured deposits) of the failed financial institution. When a P&A transaction with a third party is not feasible, the FDIC may implement a deposit payout, where the FDIC pays all the insured deposits of the failed financial institution. In the absence of a P&A transaction, or if the acquiring institution does not acquire all of the assets, the FDIC as a receiver for the failed financial institution, assumes ownership of the failed financial institution's remaining assets and must manage, market, and sell the assets. Once the FDIC sells the assets, distributes any proceeds, and completes legal activity of a failed financial institution, the FDIC terminates the receivership. The scope of this PIA is receivership data administration. This PIA will be updated as necessary.

FDIC Business Data Services

When a financial institution fails, the FDIC sends a team to collect all of the electronic and physical records necessary to accomplish its responsibilities as receiver. The FDIC stores electronic failed financial institution data collected from the institutions in the FDIC Business Data Services (FBDS) system and hard copy documents and media at an off-site storage facility. While the data from each financial institution is different in structure, nomenclature, and format, FBDS is managed to process, organize, and load the data in similar fashion to simplify use by FDIC. The physical records are inventoried and stored securely.

Failed Financial Institution Data

The failed financial institution data generally include the following standard data sets: Assets, Deposits, Financials, Human Resources, Customers, Securities, Emails, Item Processing (e.g. check images, deposit tickets), and Document Archives (e.g., Department shares, meeting minutes, collaboration tools). The PII in failed financial institution data are about customers, borrowers, guarantors, and vendors who provided services to the failed financial institution as well as employees, officers, directors, attorneys and others.

[1] www.fdic.gov/privacy

[2] 12 U.S.C. § 1821 (c).

The FDIC must retain records from a failed financial institution for which it is appointed as receiver for a minimum of six years in accordance with 12 U.S.C. § 1821(d)(15)(D). Those records are collected into electronic and physical storage managed by the FDIC. Upon the collection of failed financial institution data, FDIC uses databases and environments to format the data into datasets that are in a standard FDIC structure and can more effectively support the FDIC mission. The FDIC then uses some records to support asset management, customer service, investigations, litigation, research, and to respond to Privacy Act requests, document requests in litigation, and subpoenas.

Purchase and Assumption Settlement System (PASS)

The purpose of the Purchase & Assumption Settlement System (PASS) is to establish an end-to-end business solution for DRR business, FDIC Legal Division, and external stakeholders at acquiring institutions. It has a cloud-based component for operations and storage and an offline component to support P&A scenarios within limited internet connectivity. PASS supports the following capabilities:

- Allows internal and external stakeholders (at acquiring institutions) to electronically submit, route, review, and approve action items, transactions, line items, and documents.
- Generates and tracks P & A agreement options, deadlines, extensions, correspondence, etc.
- Provides business rules, calculations, and workflow by transaction and line item type.

PASS Data

Upon the closing of a failed financial institution, an FDIC settlement agent will load settlement information into PASS, which may contain payroll registers, agreement and contracts, loan documents, promissory notes, security or collateral agreements, deposit histories, loan histories, appraisals, name, address, social security and account numbers, EIN numbers, phone numbers, email addresses, account statements and check copies including ABA routing and account numbers. The offline component of PASS, Offline PASS, may contain financial institution demographic information, EIN numbers, contact names, work and email addresses, phone numbers, instructional and informational documents, agreement and contracts. Offline PASS post-close activity will not include the PII that is found in the Online PASS request and financial transactions. Records captured in PASS are deleted or destroyed ten years after the termination of the receivership.

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: FDIC does not collect failed financial institution customer or employee information directly from individuals. Instead, FDIC captures data from the failed institution and receives failed institution data from third parties. The FDIC does not have the ability to provide notice to individuals prior to the exchange of their PII between the third party and FDIC. Therefore, individuals may not be aware that their data has been provided to FDIC and that FDIC may keep that data for 30 years for research purposes.

Mitigation: This PIA and the FDIC Privacy Act SORN 30-64-0013, Insured Financial Institution Liquidation Records[3] are made publicly available and provide transparency to this process. The FDIC also publishes a notice

[3] https://www.fdic.gov/policies/privacy/documents/fdic-13-insured-financial-institution-liquidation-records.pdf.

in the local newspaper(s) about the financial institution failure.

Access and Amendment

Privacy Risk: When a financial institution fails, consumers may have difficulty obtaining access to their records and amending their information.

Mitigation: The FDIC voluntarily complies with the Privacy Act's requirements. The FDIC believes that it will be to the advantage of the individuals whose loan records have come into the possession of the FDIC as receiver to establish formal procedures under the Privacy Act. This will assure that such individuals will know the procedures to be followed to gain access to their record and the steps taken by the FDIC to safeguard their privacy. The resulting procedures for access and correction can be found within FDIC Privacy Act SORN 30-64-0013, Insured Financial Institution Liquidation Records. Under this SORN, information will be made available to the individual except to the extent that it has been compiled in reasonable anticipation of litigation or other legal proceeding.

Minimization

Privacy Risk: When acting as receiver of a failed financial institution, the FDIC obtains records of the failed financial institution. The complexity of litigation and its various timelines can make it difficult to adhere to the retention period.

Mitigation: The FDIC has established a process by which failed financial institution data are tracked and managed to their appropriate retention schedules. Six years after the FDIC is appointed as receiver of a failed financial institution DRR confirms with the FDIC's Legal Division that all applicable litigation activity has been closed. Thereafter, any data relevant for research purposes are transitioned to the Division of Insurance Research (DIR), and any failed financial institution data are destroyed unless they are subject to a legal hold.

Data Quality and Integrity

Privacy Risk: The FDIC collects information from failed or failing financial institutions and cannot attest directly to data quality that it receives. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and the failed or failing financial institutions.

Mitigation: Since the FDIC does not use any customer information provided from a failed or failing financial institution to deprive those individuals a right or benefit, the privacy-related data quality and integrity risks associated with data exchanges between those entities and the FDIC are minimal. No mitigation actions are recommended.

Individual Participation

Privacy Risk: Because the FDIC collects failed financial institution data directly from failed institutions, there is limited opportunity for individual participation.

Mitigation: 12 U.S.C. § 1821(d)(2)(A) specifically gives the FDIC general power to succeed to rights, titles, powers, and privileges of the insured depository institution and title to the records, and assets of any previous conservator or other legal custodian of a failed financial institution. This legal authority provides transparency to the public and general notice to the individual regarding the processing of their PII. 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?

System	Information Summary
FBDS	• Full Name of the customer (including primary account holder and trustees or beneficiaries) • Date of Birth • Social Security number (SSN) and Taxpayer Identification Number (TIN) • Home Address • Non-work Phone Numbers • Financial Information (e.g., checking and savings account numbers and balances) • Type of account (e.g., single/joint account; revocable trust account; corporate, partnership and unincorporated associations account, irrevocable trust account, employee benefit plan account or government account)
PASS	• Payroll registers • Agreement and contracts • Loan documents • Promissory notes • Security or collateral agreements • Deposit histories • Loan histories • Appraisals • Names • Address • Social Security number • Account numbers • EIN numbers • Phone numbers • Email addresses • Account statements • Check copies including ABA routing and account numbers.

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 (Specify: See above)	☒	☐

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

Data Source	Description of Information Provided by Source
Failed Financial Institution	Failed financial institution data includes: Loan and Collateral Files, Deposit Files, Financial Institution Financials, Email, File Shares, Suspicious Activity Reports (SAR), Reports of Examinations (ROEs), Payroll records, HR records, Board Minutes, and other related Financial Institution records as necessary to meet the FDIC statutory requirements. This data has the potential to include PII including but not limited to: full name, date of birth (DOB), social security number (SSN), mother's maiden name, home address, financial information, employment status/history, etc.
Acquiring Institutions	Acquiring Institution information collected, processed, and stored by FDIC may contain payroll registers, agreement and contracts, loan documents, promissory notes, security or collateral agreements, deposit histories, loan histories, appraisals, name, address, social security and account numbers, EIN numbers, phone numbers, email addresses, account statements and check copies including ABA routing and account numbers.
Servicers	FDIC collects loan information from various Servicers with which the Corporation has contracted. The data may include full name, home address, loan amounts, SSN, phone numbers, and other information related to a sale of an institution.

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 support receivership data administration 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 provides SORN coverage for both FBDS and PASS. FDIC Privacy Act SORN-013, Insured Financial Institution Liquidation Records, covers the individual's files held by the closed or assisted financial institution, including loan or contractual agreements, related documents, and correspondence. The system also contains FDIC asset files, including judgments obtained, restitution orders, and loan deficiencies arising from the liquidation of the obligor's loan assets and associated collateral, if any; information relating to the obligor's financial condition such as financial statements and income tax returns; asset or collateral verifications or searches; appraisals; and potential sources of repayment. FDIC asset files also include intra- or inter-agency memoranda, as well as notes, correspondence, and other documents relating to the liquidation of the loan obligation or asset. FDIC receivership claim files may include all

information related to claims filed with the receivership estate by a failed financial institution's landlords, creditors, service providers or other obligees or claimants.

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

No, the SORNs listed in Question 2.2 do 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.

FBDS: The FDIC collects failed financial institution data containing PII from failed financial institutions and not directly from the individual. Therefore, no Privacy Act Statement is provided to the individual.

PASS: No Privacy Act Statement is required. Asset information which may contain PII is collected from the financial institution and not the individual. FDICConnect provides the authentication mechanism for the acquiring institution users attempting to use PASS. The following privacy notice is provided on the FDICconnect information page: https://www.fdicconnect.gov/login_privpol.asp.

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'.

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: FDIC does not collect failed financial institution customer or employee information directly from individuals. Instead, FDIC captures data from the failed institution and receives failed financial institution data from third parties. The FDIC does not have the ability to provide notice to individuals prior to the exchange of their PII between the third party and FDIC. Therefore, individuals may not be aware that their data has been provided to FDIC and that FDIC may keep that data for 30 years for research purposes.

Mitigation: This PIA and the FDIC Privacy Act SORN-013, Insured Financial Institution Liquidation Records[4] are made publicly available and provides transparency to this process. The FDIC also publishes a notice in the local newspaper(s) about the financial institution failure.

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?

[4] https://www.fdic.gov/policies/privacy/documents/fdic-13-insured-financial-institution-liquidation-records.pdf.

For PASS, system users are able to access their account information after registering for a user account and logging into the system. After logging into the system, users have the ability to make changes to their information.

The FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program". Access procedures for this information system or project are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. 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 Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

The FDIC complies with the Privacy Act when acting as a receiver just as it does in its agency capacity. The FDIC believes that it will be to the advantage of the individuals whose financial records have come into the possession of the FDIC as receiver to establish formal procedures under the Privacy Act.

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

For PASS, system users are able to access their account information after registering for a user account and logging into the system. After logging into the system, users have the ability to make changes to their information.

The FDIC allows individuals to correct or amend PII maintained by the FDIC on a limited basis according to the procedures published in the SORN(s) listed in Question 2.2 of this PIA.

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

The FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users, the procedures for which are published in the SORN(s) listed in Section 10.4 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program"

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: When a financial institution fails, consumers may have difficulty obtaining access to their records and amending their information.

Mitigation: The FDIC voluntarily complies with the Privacy Act's requirements. The FDIC believes that it will be to the advantage of the individuals whose loan records have come into the possession of the FDIC as receiver to establish formal procedures under the Privacy Act. This will assure that such individuals will know the procedures to be followed to gain access to their record and the steps taken by the FDIC to safeguard their privacy. The resulting procedures for access and correction can be found within FDIC Privacy Act SORN-013, Insured Financial Institution Liquidation Records. Under this SORN, information will be made available to the individual except to the extent that it has been compiled in reasonable anticipation of litigation or other legal proceeding.

Privacy Risk: The FDIC uses failed financial institution data to provide customer service, such as to obtain a lien release and process claims. To the extent that the retention period is limited by statute, the FDIC is limited in its ability to provide such customer service and records research.

Mitigation: The FDIC provides the public notice via the fdic.gov website of the opportunity for customer service and also explains how customer service may be limited as FDIC is not the actual lender, and the failed financial institution data in FDIC possession is limited. In the event that FDIC may be unable to provide customer service and assets of the failed financial institution were acquired by another institution, an individual may seek assistance from the Acquiring Institution.

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?

The FDIC contracts with a number of service providers in order to efficiently execute receivership administration. These services include but are not limited to securely capturing, imaging, indexing and maintaining the failed financial institution data, as well as disaster recovery services and off-site physical storage. Contractor staff also manages system accounts, including establishment, activation, modification, review, disablement, and removal.

Due to contractors' access to PII, contractors are required to satisfy the necessary background investigation, sign confidentiality agreements, and 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 receivership data administration. 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 (SAOP) Report 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. In circumstances where the FDIC relies on a contractor-operated system, the contracts include clauses placing requirements on the contractor to ensure the contractor is held to the same standards.

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 risks associated with Accountability.

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 personally identifiable information (PII) are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of System of Records 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:

- 12 U.S.C. § 1819: states that FDIC can make examinations of and to require information and reports from depository institutions
- 12 U.S.C. § 1822: deals with FDIC as a receiver of failed financial institutions
- 12 C.F.R. § 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 FDIC limits its collection of failed financial institution data to what is necessary under Section 1821(d)(15)(D) of the FDI Act for responsibly managing a receivership. The FDIC has defined the term "records" of failed financial institutions in 12 C.F.R. Part 360 using a two-part test. Part one is a formal definition: records are "any reasonably accessible document, book, paper, map, photograph, microfiche, microfilm, and computer or electronically-created record generated or maintained by an insured depository institution in the course of and necessary to its transaction of business.'' Part two is a functional test where the FDIC considers the following factors: "(1) Whether the documentary material related to the business of the insured depository institution, (2) Whether the documentary material was generated or maintained as records in the regular course of the business of the insured depository institution in accordance with its own recordkeeping practices and procedures or pursuant to standards established by its regulators,(3) Whether the documentary material is needed by the FDIC to carry out its receivership function, and(4) The expected evidentiary needs of the FDIC." This definition is intended to clarify the statutory term, exclude from collection documentation material that has no relevance to its business, or which lacks evidentiary value, and avoids unnecessary burdens and inefficiencies that arise from the increase in record creation due to increasing technology use and data storage capabilities.

The FDIC creates an approved collection plan that identifies what information is considered relevant and where that information may be found. The FDIC also creates an exit memo with an inventory of the collected information to help create accountability and ensure effective management of the data throughout its lifecycle. Moreover, FBDS has security controls that minimize access to those individuals with a need to know granted on principle of least privilege.

Additionally, through the conduct, evaluation and review of privacy artifacts,[5] 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?

In accordance with Regulation P, 12 C.F.R. § 1016.15(a)(7)(iii), financial institutions are required to provide notice to their customers about their privacy policies and disclosures to third parties, this includes mandatory disclosure to federal regulators. The FDIC only collects failed financial institution data after a financial institution has failed for the purposes of fulfilling its statutory obligations.

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

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?

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.

Failed financial institution data used for receivership purposes are retained for minimum of six years after the date the FDIC is appointed as receiver of a failed institution in accordance with the Federal Deposit Insurance (FDI) Act.[6] Failed Insured Depository Institution Records relevant for research purposes are maintained for 30 years after the FDIC is appointed as receiver.

Receivership Resolution Documentation is retained for ten years after the termination of the receivership.

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?

Failed financial institution data is not used for testing or training.

Failed financial institution data may be used for research purposes to better understand and optimize the resolution and receivership processes. When failed financial institution data are designated specifically for research purposes after 6 years from the date the FDIC is appointed as receiver of a failed financial institution, responsibility for record maintenance is transferred to the DIR. DIR may retain the data on behalf of the FDIC for an additional 24 years (totaling 30 years from date of FDIC appointment as receiver), in accordance with established records retention schedules.

The platform on which PASS resides allows for the de-identification and masking of data when being transferred to non-production environments.

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: When acting as receiver of a failed financial institution, the FDIC obtains records of the failed financial institution. The complexity of litigation and its various timelines can make it difficult to adhere to the retention period.

[6] 12 U.S.C. § 1821(d)(15)(D).

Mitigation: The FDIC has established a process by which failed financial institution data are tracked and managed to their appropriate retention schedule. Six years after the FDIC is appointed as receiver of a failed financial institution, DRR confirms with the FDIC's Legal Division that all applicable litigation activity has been closed. Thereafter, any data relevant for research purposes are transitioned to the DIR, and any failed financial institution data are destroyed unless they are subject to a legal hold.

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 FDIC loads failed financial institution data into the e-discovery platform in a forensically sound manner with identified chains of custody so all of the data can be used as evidence in civil and criminal courts. Before failed financial institution data are released to end users, a quality assurance team performs quality control checks using automated scripts, as well as a visual inspection to ensure that the data was correctly processed and loaded into the e-discovery platform.

Additionally, the quality assurance team validates any litigation data prior to release under protective orders. Examples of the quality control checks that are performed include verification of:

- Document & image counts, and metadata between the source files and the e-discovery platform;
- Confirmation of image rendering in the e-discovery platform;
- Confirmation that Suspicious Activity Reports & Reports of Examination documents were identified and properly secured; and
- Verification that document family relationships are maintained and searchable.

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?

The source of failed financial institution data are the systems and documents from the failed financial institution and servicers or third parties associated with the failed financial institution.

PASS only collects PASS user data directly from the individual. Otherwise, borrower and employee information comes from systems and documents from failed financial institutions and servicers.

The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

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

The FDIC reviews privacy artifacts to ensure adequate 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: The FDIC collects information from failed or failing financial institutions and cannot attest directly to data quality that it receives. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and the failed or failing financial institutions.

Mitigation: Since the FDIC does not use any customer information provided from a failed or failing financial institution to deprive those individuals a right or benefit, the privacy-related data quality and integrity risks associated with data exchanges between those entities and the FDIC are minimal. No 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.

FDIC received failed financial institution information from third-parties. Other than for PASS user information, PASS receives 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 collected via third party. Individuals should review the relevant third party's privacy notices.

PASS users from acquiring institutions authenticate through FDICConnect. A privacy notice is provided on the FDICconnect information page: https://www.fdicconnect.gov/login_privpol.asp.

Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

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. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, 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 receivership data administration only use PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC privacy policies.

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: Because the FDIC collects failed financial institution data directly from failed financial institutions, there is limited opportunity for individual participation.

Mitigation: 12 U.S.C. § 1821(d)(2)(A) of the FDI Act specifically gives the FDIC general power to succeed to rights, titles, powers, and privileges of the insured depository institution and title to the records, and assets of any previous conservator or other legal custodian of a failed financial institution. This legal authority provides transparency to the public and general notice to the individual regarding the processing of their PII. No additional 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.

Failed financial institution data are collected and retained in accordance with 12 U.S.C. § 1821(d)(15)(D) in order to function as a receiver. All PII within the failed financial institution data are used to support FDIC activities in accordance with FDIC receivership procedures. Failed financial

institution data may be used for research purposes to better understand and optimize FDIC's resolution and receivership processes.

PASS data are collected and retained in accordance with 12 U.S.C. § 1819 in order to ensure the appropriate financial institution information is available in order to complete Purchase and Assumption transactions.

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.

All FBDS users are required to comply with Confidentiality and Rules of Behavior agreements which are renewed annually.

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.

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

FBDS:
To obtain access, users must have the approval of their manager/supervisor and the program manager/data owner. Users also must sign a confidentiality agreement and security principles of behavior. Further, all FDIC network users must annually complete the FDIC's Information Security and Privacy Awareness training, which includes the Corporation's general rules of behavior. All access granted is determined on a "need-to-know" basis, as defined by the Privacy Act of 1974. Guidelines established in the Corporation's access control policies and procedures are also followed. Controls are documented in system documentation. Program support staff manage information system accounts, including establishment, activation, modification, review, disablement, and removal. Additionally, the FBDS solution's security settings limit a user's access to specific financial institutions and databases. External users like opposing counsel may receive access to read-only segmented sub-folder information within FBDS. FDIC Legal reviews and authorizes all external access requests and approvals are granted once FDIC Program Management confirms need to know. Failed financial institution data loaded into FBDS are secured with multi-factor authentication and FIPS 140-2 validated encryption. Data is continuously replicated to a secondary data center. The evidentiary hard drives (original and forensic copies) are stored in Forensic Lab Evidence vault. The removable media (e.g., hard drive, CD) are encrypted via FIPS 140-2 validated encryption solutions as well.

PASS:
All internal users of PASS 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.

External Users use the FDICConnect authentication process and will only have access to limited roles for specific settlement cases within PASS.

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

PASS may share loan numbers and borrower names as part of journal entries with the FDIC's Dividend Processing System.[7] No other internal information system receive or have access to PASS data. For failed financial institution data, FDIC sends the data to an FDIC internal collaboration platform for the specific financial institution after it is formatted into FDIC datasets. Once the data is on the collaboration platform, FDIC staff can take resolution actions related to the specific failed institution. Following the disposition process of failed financial institution data, those records that are necessary for research purposes will be transferred to the DIR research environment.

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?

Failed financial institution data may be analyzed at an aggregate level in order to better understand and optimize the resolution and receivership process and provide on-going customer service. Such data-driven operations include the following controls; operations-based research is initiated by DRR management to ensure necessary authority and valid purpose specification and disclosure of results is limited to senior leadership within the FDIC, and external disclosures are approved by DRR management to limit potential risk of re-identification of individuals.

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.

FBDS shares PII externally with the following entities in order to help manage the receivership.

Data Destination	Description of Shared Data
FBDS: External Legal Counsel	The FDIC may share data from FBDS with its own retained counsel in order to defend or prepare litigation. The process of sharing that information is protected by an agreement with retained counsel. The FDIC might be required to share data from FBDS with opposing counsel or adverse parties in litigation. The processing of sharing that information is most often protected by a confidentiality or protective order from a court.
FBDS: Federal, State, and/or Local Agencies	Congressional inquiries, subpoenas, discovery orders, and other legal/investigatory matters may result in the need to provide subsets of FBDS data to federal government agencies, such as the Security Exchange Commission (SEC), Office of Inspector General (OIG), the Federal Bureau of Investigation (FBI), Department of Justice (DOJ), Department of Treasury, and other requesting government agencies. All access requests received from government agencies must be approved by an authorized FDIC manager/supervisor, as well as by FDIC Legal if the requests involve subpoenas or exempt information (e.g., Reports of Examination, Currency Transaction Reports, Suspicious Activity Reports). Once access is approved by FDIC, government officials do not receive direct access to the FBDS

[7] For more information about, the FDIC's Dividend Processing System, see the Insurance Determinations and Payouts PIA. Available at https://www.fdic.gov/policies/privacy/assessments.html.

Data Destination	Description of Shared Data
	solution via the e-discovery platform. Rather, FDIC loads the requested data to FIPS 140-2 validated encrypted hard drives and securely sends them to the requesting agency official(s). The process of sharing data from FBDS with other agencies might also be protected by a memorandum of understanding or agreement between the FDIC and another agency.

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).

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 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.