FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Failed Financial Institution Employee Data Management

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 PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

During the closing of a failed financial Institution, the FDIC assumes responsibilities for the institution, including certain responsibilities toward its employees. Specifically, FDIC's Division of Resolutions and Receiverships (DRR) is responsible for the general oversight of failed financial institution employee benefit and welfare plans. Because the FDIC as Receiver becomes the 'successor' Plan Sponsor, DRR coordinates all business decisions relating to the administration and termination of failed institution sponsored employee benefit plans. DRR is also responsible for processing the final payroll, closing weekend payroll, and vacation time for the employees of a failed financial institution at the institution's closing. In addition, FDIC must provide for the continuation of health insurance coverage to failed financial institution employees.[2] FDIC contracts the services of a third-party administrator (TPA) to administer the group welfare plans. Internally, FDIC relies on two main information technology systems to help fulfill its responsibilities to a failed financial institution's employees: the Pension Tracking System – Plus (Pentrax+) and the Resolution and Receivership Management Portal (RRMP). The scope of this PIA is FDIC's management of failed financial institution employee data and the systems that support it.

Pension Tracking System – Plus (Pentrax+)
Pension Tracking System – Plus (Pentrax+) is an application used to support the tracking, management and reporting of sponsored employee benefit plans inherited from failed financial institutions. When a financial institution fails, the FDIC assumes administrative responsibility for the termination of the institution-sponsored employee benefit plans that are not passed onto an acquiring institution. FDIC also handles the administration of the plan distributions to the plan participants. Pentrax+ is the management tool utilized by DRR Employee Benefits Plan Specialists to ensure that essential tasks are performed and serves as a resource for information about the plans. Additionally, Pentrax+ also tracks failed financial institution welfare plans (i.e., health, dental, and vision). Data is acquired from the failed financial institution's employee benefit systems and entered into Pentrax+ after the failure of a financial institution occurs. The system is used to track information on the termination of failed institution employee benefit plans. Data tracked includes target and completion data for tasks necessary to terminate applicable employee benefit plans. The system also has a comments section allowing for a narrative description of the status of the benefit plan termination, key contacts including contractors, the value of plan assets, as well as search and reporting capabilities. Plan participants who have a balance as of financial institution failure are entered into Pentrax+.

Resolution and Receivership Management Portal (RRMP)[3]
The Resolution and Receivership Management Portal (RRMP) is a web-based tool used by DRR to track requests and inquiries (called "cases") related to financial institution resolution and receivership activities that are submitted from external users. For the purposes of this PIA, RRMP processes information from employees of the failed institutions for employee benefit plans and provides an external-facing portal for failed financial institution employees to complete timesheets with the Receiver of the failed institution and complete waivers to release personnel files to an acquiring institution. Additional information about how RRMP is used in the claims process can be found in the FDIC Insurance Determinations and Payouts Privacy Impact Assessment.[4]

[1] www.fdic.gov/privacy
[2] 12 U,S.C. § 1821 note.
[3] The Resolution and Receivership Management Portal was previously called the Receivership Request Management Portal.
[4] https://www.fdic.gov/policies/privacy/assessments.html

During a financial institution closing event, DRR engages employees of the failed institution and instructs them to go to the RRMP Failed Bank Employee Portal (FBE)[5], where they can submit personnel file release forms and validate timesheets.

Following the closing event, failed financial institution employees can access RRMP via the FDIC Information and Support Center (FISC)[6], where they can use RRMP to:

- Verify former employee's previous employment with a failed institution;
- Request a Form 1098, 1099, or W2;
- Ask a question about their former institution's employee benefits plan;
- Ask about their pay for time worked before the institution failed;
- Ask about their pay for time worked after the institution failed;
- Change their address with the FDIC;
- Open a claim for unpaid, unused time-off;
- Request the status of their existing claims; and
- Ask other questions.

Information about the failed financial institution employee is loaded into RRMP prior to failure, but purged if the institution doesn't fail. Authorized DRR personnel have the ability to extract a report for employee benefits from RRMP and use an import tool to enter that data into Pentrax+, but RRMP does not have a direct connection with Pentrax+. Information is not loaded into Pentrax+ until after the failure of the financial institution.

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
- Data Minimization
- Data Quality and Integrity
- Individual Participation

Transparency

Privacy Risk: There is a risk that failed financial institution employees may not be aware that their data is being maintained and processed by the FDIC.

Mitigation: While Pentrax+ may not collect PII directly from the individual employees, DRR Payroll Leads and Employee Benefit Leads disseminate pertinent information to the employees of failed financial institutions related to FDIC's processing of their benefits and HR information as part of the failed financial institution closing process. This includes providing a point of contact DRR Specialist if the employees have additional questions.

Access and Amendment

Privacy Risk: Failed financial institution employees may not be able to access and amend their information that has been collected from the failed financial institution.

Mitigation: The publication of this PIA and the SORN described in Question 2.2 detail the procedures for access and amendment to the information collected from the failed financial institution In addition, failed financial institution employees may contact DRR Employee Benefit Specialists to requests updates to their information in RRMP.

[5] https://resolutions.fdic.gov/fbeportal/s/

[6] https://ask.fdic.gov/fdicinformationandsupportcenter/s/?language=en_US.

Data Minimization
Privacy Risk: Some systems supporting failed financial institution employee data management do not yet have an established records retention schedule.

Mitigation: FDIC Records and Information Management Unit (RIMU) is currently engaged in a large effort to establish formal retention schedules for all systems. FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes, periodically evaluating and verifying PII that is collected, and ensuring that any duplicate data sets are overwritten.

Data Quality and Integrity
Privacy Risk: The FDIC collects information from failed and failing financial institutions and cannot attest directly to the data quality of the information received. 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: To the extent possible, the FDIC uses system-to-system transfers to reduce the inadvertent alteration of data. For data that is manually uploaded by DRR employees, there are a number of validation points and safeguards to avoid the alteration of data uploaded from the failed financial institutions. See Section 7.1 for more information. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate. See Section 3.0 for more information.

Individual Participation
Privacy Risk: Since most data in Pentrax+ is not collected directly from individuals, there is a risk that these individuals will not know how their data are being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: In cases where FDIC does collect PII directly from individuals, Privacy Act Statements are provided where appropriate. The FDIC does not have the ability to provide privacy notices prior to its processing of individuals' PII. Individuals may review the relevant third party's privacy notices. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII. Failed Financial Institution Employees can and should review their paystubs to ensure they are correct and consistent with previous paystubs and should reach out to the DRR POC they were assigned during closing.

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
Pentrax+	• Full Name • Date of Birth • Social Security number (SSN) • Home Address • Non-work Phone Numbers • Email Address • Financial Information (e.g., account and loan balances, trust statements, hardship withdrawal information) • Employment Information (e.g., date of hire, date of termination) • Legal Documentation • Supporting Documentation (Pentrax+ has the ability to upload supporting documentation pertaining to participant accounts after the closing of a financial institution. These records may include PII beyond the above PII elements. Pentrax+ does not use this information beyond its initial capture)
RRMP	• Full Name • Date of Birth • SSN • Financial Information • Home address

System	Information Summary
	• Phone number • Email address • Gender • Supporting documentation
TPA	• Full Name • Date of Birth • SSN • Certificates (e.g., birth, death, marriage) • Medical Information • Home Address • Phone Numbers • Legal Documents • Gender

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

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

Data Source	Description of Information Provided by Source
Failing/Failed Financial Institutions and Third Party Administrators	DRR obtains employee benefit plan data from the failing or failed institutions and third party administrators. DRR then prepares the required employee benefit data for upload to the Pentrax+.
Failed Financial Institution Employee Requests to FDIC	The employees of a failed financial institution can request updates to some of their information in RRMP and DRR Employee Benefit specialists can make the requested changes.
Failed Financial Institution Employee to TPA	In order to administer the FIA group health plan, authorized TPA staff may collect sensitive PII data directly from qualifying beneficiaries/participants (i.e., eligible employees of failed financial institutions and their dependents).

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 failed financial institution employee data management 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.

These systems operate under FDIC Privacy Act SORN-013, Insured Financial Institution Liquidation Records. This SORN covers the individual's files held by the closed or assisted financial institution, including contractual agreements, related documents, and correspondence.

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.

Information collected from third parties: FDIC systems store data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Given that the FDIC is not the initial collector of the PII, a Privacy Act Statement is not required to explain the purpose for collection and the intended uses of the information.

Information collected by FDIC: When information is collected directly from the individual, FDIC provides the individual with a Privacy Act Statement prior to the collection of his or her personal information.

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: There is a risk that failed financial institution employees may not be aware that their data is being maintained and processed by the FDIC.

Mitigation: While Pentrax+ may not collect PII directly from the individual employees, DRR Payroll Leads and Employee Benefit Leads disseminate pertinent information to the employees of failed financial institutions related to FDIC's processing of their benefits and HR information as part of the failed financial institution closing process. This includes providing a point of contact DRR Specialist if the employees have additional questions.

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?

Information collected from third parties: FDIC systems process data provided by failed financial institutions to the FDIC during the pre-closing activities. Given the limitations around how this data can be used for monitoring or resolving failed financial institutions, the FDIC may not be authorized to provide individuals access to the information that it obtains.

Information collected and maintained by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, access procedures are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORN(s) 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.

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

Information collected from third parties: The FDIC systems that process information from failed or failing financial institutions initially operate from a point-in-time snapshot[7] of data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Given the limitations around how this data can be used for monitoring or resolving failed financial institutions, the FDIC may not be authorized to correct inaccurate or erroneous information.

Information collected and maintained by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, amendment procedures are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORN(s) on the FDIC public-facing website, which includes rules and regulations governing how individuals may amend their records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1, "Automated Information System (AIS) Security Program." In addition, failed financial institution employees may reach out to their assigned DRR Employee Benefits Specialist to request changes to their information in RRMP.

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

[7] When FDIC sends a file during the pre-close phase of the closing, it is an instance of what is on file with the institution(s) at that time. No changes are allowed after the financial institution has closed.

Information collected from third parties: FDIC systems process data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Accordingly, the FDIC is unable to notify individuals about the procedures for correcting their information that the FDIC collects from third parties.

Information collected by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, notification is provided as described in Question 3.1. Additionally, notification procedures are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may amend their records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1, "Automated Information System (AIS) Security Program." Additionally, 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."

At the beginning of the closing process, DRR sends failed financial institution employees an email with instructions about required activities during each of the closing days. This email includes a link to the RRMP-FBE Portal and instructions for registering for and using the portal.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: Failed financial institution employees may not be able to access and amend their information that has been collected from the failed financial institution.

Mitigation: The publication of this PIA and the SORN described in Question 2.2 detail the procedures for access and amendment to the information collected from the failed financial institution In addition, failed financial institution employees may contact DRR Employee Benefit Specialists to requests updates to their information in RRMP.

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 DRR based on evolving business requirements and the 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.

Contractors may also provide services to the FDIC, such as staff and operations augmentation to support noticing and claims administration in the event that DRR must scale its operations to support resolution of a large and complex financial institution that has failed.

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

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

Yes, Contractor Confidentiality Agreements have been completed by contractors who support failed financial institution employee data management. 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 inventories.

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 Notices (SORNs). FDIC Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. These particular system collect 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. 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 financial institutions.
- Executive Order 9397: pertaining to the requirement for the use of SSNs.
- 12 CFR 360.9: pertains to allowing large financial institutions to continue function on the day of closing to permit FDIC meeting legal mandates and performing required functions.
- 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 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.

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?

FDIC minimizes the PII elements to what is relevant and necessary to accomplish the legally authorized purpose of providing closing and post-closing support to failed financial institution employees in the following ways:

- DRR extracts the minimum data elements needed to support the processing of failed financial institution personnel human resources administration from the failed or failing institution to FDIC during the financial institution closing process.

- Pentrax+ and RRMP are analyzed by FDIC Records and Information Management (RIMU) to establish retention and disposition schedules to reduce privacy risk.
- Data entry screens and load modules in Pentrax+ managed by DRR include edit checks to ensure business rules and data relationships are maintained.

Additionally, through the conduct, evaluation and review of privacy artifacts,[8] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

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

The FDIC only collects and retains PII from financial institution employees when a financial institution is being monitored for resolution planning or has failed.

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.

Records related to failed financial institution employees maintained within RRMP are destroyed ten years after the termination of the receivership. Pentrax+ does not yet have a formal retention policy. The TPA maintains data in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

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

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

Privacy Risk: Some systems supporting failed financial institution employee data management do not yet have an established records retention schedule.

Mitigation: FDIC Records and Information Management Unit (RIMU) is currently engaged in a large effort to establish formal retention schedules for all systems. FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes, periodically evaluating and verifying PII that is collected, and ensuring that any duplicate data sets are overwritten.

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. Additionally, 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.

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.

Pentrax+ begins with a point-in-time snapshot of data provided by the failed or failing financial institution during closing activities. The responsibility for quality, utility, and objectivity of that point-in-time snapshot of data belongs to the failed or failing financial institutions. Pentrax+ data entry screens and load modules include edit checks to ensure that business rules and data relationships are maintained. Data validation has been incorporated within the system and the database, to ensure data is entered in the required format. There are validations at the data field level (e.g., monetary fields must be numeric), and there are calculated fields to avoid manual entry errors. Once data is loaded into Pentrax+, the DRR Resolution and Receivership Specialist/Technician or Claims Analyst reviews the file from the failed institution to ensure that data was loaded properly. FDIC can also update the data in Pentrax+ when the reports are pulled from RRMP.

In RRMP, the ability to create new or edit existing records is determined by a user's role. Once data is loaded into RRMP, a DRR Resolution and Receivership Specialist/Technician or Claims Analyst reviews the files in RRMP to ensure that data was loaded properly. For timesheets processed in RRMP-FBE, there are validation checks in place. If a timesheet is incomplete, the end user will receive a verification error message: "Please complete the Timesheet Entry Date, Clock In Time, and Clock Out Time." Failed financial institution employees have the ability to Edit or Delete a timesheet entry. Additionally, they must also certify their timesheets are complete and accurate. Employees must also certify permission to release their personnel file. If the employee does not agree to the release of the personnel file, then that response is recorded in RRMP and also provided to the employee via email (a copy of that release form is emailed to the failed institution employee whether or not they select Yes or No). If the employee selects a No response, then the FDIC does not pass the personnel records to the acquiring institution. Employees may change their response from a No to a Yes at any time with the RRMP-FBE portal is open during the closing weekend. After the closing weekend, employees will not be able to change their response to the release of their personnel file via RRMP-FBE.

Authorized DRR Claims Administration Section staff can close the reporting period in RRMP and make changes to failed financial institution employee information and timesheet information if required.

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 FDIC collects PII directly from the individual to the greatest extent practicable, which primarily involves collecting directly from the individual via RRMP and the TPA to provide customer service related to failed financial institution employee benefits and human resource activities. Much of the data maintained in Pentrax+ relies on the collection of information from failed financial institution pension tracking systems.

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 and failing financial institutions and cannot attest directly to the data quality of the information received. 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: To the extent possible, the FDIC uses system-to-system transfers to reduce the inadvertent alteration of data. For data that is manually uploaded by DRR employees, there are a number of validation points and safeguards to avoid the alteration of data uploaded from the failed financial institutions. See Section 7.1 for more information. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate. See Section 3.0 for more information.

Section 8.0: Individual Participation

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

8.1 Explain how the information system or project provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

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

FDIC receives data from failed financial institution employee benefit plan third party administrators, and FDIC Specialists upload this data into Pentrax+. 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 and implicit consent with respect to the collection, use, and disclosure of PII. FDIC does not make decisions regarding individuals based on the PII received from third parties.

Otherwise, 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.

Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

8.3 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. Refer to Section 8.1 for additional information. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORNs 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.

Information systems supporting failed financial institution employee data management only process and store PII for the purposes listed in Section 9.1. This PIA and the relevant SORN listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

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

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

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Since most data in Pentrax+ is not collected directly from individuals, there is a risk that these individuals will not know how their data are being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: In cases where FDIC does collect PII directly from individuals, Privacy Act Statements are provided where appropriate. The FDIC does not have the ability to provide privacy notices prior to its processing of individuals' PII. Individuals may review the relevant third party's privacy notices. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII. Failed Financial Institution Employees can and should review their paystubs to ensure they are correct and consistent with previous paystubs and should reach out to the DRR POC they were assigned during closing.

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.

Pentrax+ houses PII from failed financial institutions to support the tracking, management, and reporting of sponsored employee benefit plans inherited from those failed financial institutions. RRMP FBE Portal collects information (not PII) from failed financial institution employees for the purposes of allowing those employees to complete timesheets for time worked over the closing weekend and to release personnel files to an acquiring institution. RRMP-FISC collects information from failed financial institution employees for the purpose of answering questions and addressing requests from those employees following the closing of the institution. In general, names, Social Security numbers, financial information, and contact information are necessary to support each of these functions. The TPA collects and processes PII in order to enroll and administer qualified beneficiaries under the health continuation coverage plan for failed financial institutions.

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.

Moreover, DRR 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 the FDIC 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 FDIC users that require access to Pentrax+ and RRMP 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, "Access Control for Information Technology Resources," user access levels are reviewed periodically to ensure they reflect current business needs.

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

☒ No
☐ Yes

DRR staff manually upload failed financial institution employee records into Pentrax+ and RRMP. No internal information systems receive data or have access to the failed financial institution employee data in Pentrax+ and RRMP.

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.

Information is shared externally pursuant to the routine uses described in the SORN referenced in Section 2.2.

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's 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.