FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Research Using Failed Insured Depository Institution Data

May 13, 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

Under the FDI Act, the FDIC Division of Resolutions and Receiverships (DRR) collects records from failed insured depository institutions ("failed bank data") for which the FDIC is appointed as receiver into electronic and physical storage managed by the FDIC.[2] The FDIC then uses failed bank data to support asset management, customer service, investigations, litigation, and research, and to respond to Privacy Act requests, and document requests in litigation and subpoenas. Thereafter, provided there are no legal exceptions, failed bank data identified as necessary for research purposes are transferred to the FDIC Division of Insurance and Research (DIR) Research Environment. The DIR Research Environment includes research software that are used to conduct statistical analyses of the data, including the use of statistical learning methods like machine-learning and natural language processing that enable aggregate analysis of both structured and unstructured data.

Structured data for each failed bank is stored in a database. Unstructured data for each failed bank is stored on tape and retrieved when needed. The failed bank data generally includes the following standard data sets: Assets, Deposits, Financials, Human Resources, Customer, Securities, Emails, Item Processing (e.g. check images, deposit tickets), and Document Archives (department shares, meeting minutes, collaboration tools). Records may also include documents (e.g., Board minutes, loan records, etc.) belonging to the failed bank. The failed bank data may include PII from bank customers, guarantors, and vendors who provided services to the failed bank, as well as bank employees, officers, and directors. The PII is used for research purposes, such as for matching records across different systems of a failed bank to conduct aggregate analyses. For example, matching records of customers can help determine the share of deposits with different types of deposit insurance coverage. FDIC maintains the data is maintained for thirty years from its appointment as a receiver.

DIR uses failed bank data to conduct research and analyses that inform decisions regarding core business objectives of the FDIC. The findings from research and analyses of this data have the potential to help the FDIC improve its operations and processes, and to inform national and international policy discussions and rule-making in areas as varied as resolutions, emerging risks and risk assessments, deposit insurance, and banking policy, among others. The research findings can also provide important contributions to the broader academic literature on many topics of relevance to the FDIC.

Research Governance Framework
DIR has implemented a research governance framework that maximizes the value of failed bank data to inform decisions made by multiple FDIC Divisions and protects the confidentiality and privacy of the data used in research. The governance framework has five-prongs:

1. **Research initiation management**— All research that is conducted must be approved, which ensures that the research relates to the FDIC's mission and has the potential to inform FDIC's decisions and/or operations.
2. **Disclosure review**— All research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and meets disclosure avoidance requirements to minimize the

[1] www.fdic.gov/privacy
[2] The majority of institutions that enter receiverships are banks, however, FDIC may be designated as Receiver for any financial institution as defined in 31 U.S.C. 5312(a)(2).

risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment. Removal of research results can only be carried out by staff with specific authorization.

3. **User training and rules-of-behavior**—All researchers must complete annual training on the rules-of-behavior and protection of confidentiality and privacy. The training covers the research approval process, the rules-of-behavior for conducting research in the DIR Research Environment, and the process for disclosure review that must occur prior to the release of research results. The training emphasizes the responsibility of researchers to protect the confidentiality of the data, and the need to be aware of and to minimize disclosure and re-identification risks in all research output.
4. **Access control procedures**—Access control procedures ensure that only authorized individuals have access to the DIR Research Environment and that access is only granted after the user has completed training on the rules-of-behavior and protection of confidentiality and privacy.
5. **Technological safeguards**—Technological safeguards ensure that all research and analyses using failed bank data are conducted within the DIR Research Environment. Technological safeguards also ensure that no data other than research output that have been disclosure reviewed can be removed from the DIR Research Environment. Any removal of research results from the DIR Research Environment are logged.

All components of this five-pronged approach are continuously reviewed and regularly revised to incorporate applicable elements of industry best practices. The overarching goals in the design of the five-pronged approach are to ensure that:

- no failed bank data is removed from the DIR Research Environment;
- all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment; and
- all research results that are removed from the environment are logged.

PRIVACY RISK SUMMARY

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

- Transparency
- Minimization
- Use Limitation

Transparency

Privacy Risk: The FDIC retains failed bank data for thirty years in order to use those records for research purposes in accordance with a newly established records retention schedule. The retroactive application of the records schedule results in the maintenance of failed bank data for longer than the public may have expected at the time of collection based on 12 U.S.C. 1821(d)(15)(D).

Mitigation: The FDIC conducted this PIA, which informed the establishment of the new thirty-year retention period for the use and retention of failed bank data for research purposes, and has made the PIA publicly available on the FDIC.gov website. The FDIC has also established a new System of Records under the Privacy Act, FDIC-038 Failed Insured Depository Institution Research, notice of which has been published in the Federal Register and is available on the FDIC.gov website.

Minimization

Privacy Risk: The volume of failed bank data maintained for thirty years is significant, and the maintenance of any records creates a vulnerability of such records to unauthorized access, use, disclosure and retention.

Mitigation: The collection of failed bank records is determined by operational application of rule 12 C.F.R. § 360, which addresses the risk of over-collection of information that is made available for research in the DIR Research Environment. Continued retention of failed bank data for research purposes is based on the nature of the data, the availability of tools to analyze that data, and the relevance of that data to providing the public with a sound deposit insurance and contributing to the broader academic literature on many topics of relevance to the FDIC. The FDIC evaluated a number of proposals to determine the extent to which all or portions of failed bank data should be maintained and for how long. It was determined that all failed bank data are valuable to the Corporation for addressing current policy-relevant questions and are also likely to prove critical in addressing future policy-relevant questions. Failed bank data represent a source of data that are not otherwise available for research and analysis, and have the potential to allow the FDIC to answer important questions that would otherwise not be answerable. At times, these policy questions come at a time of crisis, where having detailed data provide critical decision-making support and finding the data elsewhere is not an option. Finally, the FDIC established a retention schedule to ensure that records are not maintained longer than necessary to support research purposes.

Individual Participation

Privacy Risk: Individuals are not provided with an opportunity to choose to participate in research related to failed banks.

Mitigation: The FDI Act gives the FDIC general power to succeed to title to the books, records, and assets of any previous conservator or other legal custodian of a failed bank, and conduct research and analyses to inform decisions regarding core business objectives of the FDIC. This legal authority and the FDIC-038 Failed Insured Depository Institution Research SORN provide transparency to the public and general notice to the individual regarding the processing of their PII. No additional mitigation actions are recommended.

Use Limitation

Privacy Risk: Given the highly individualized nature of the information in failed bank data, it is possible that published research findings could, alone or in combination with other data available outside of the DIR Research Environment, inadvertently lead to the disclosure of sensitive information.

Mitigation: To reduce this risk, FDIC has implemented a disclosure review process wherein all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment. Removal of research results can only be carried out by staff with specific authorization.

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?

Failed bank data in the DIR Research Environment may contain full name, date of birth (DOB), social security number (SSN), mother's maiden name, home address, financial information, employment status/history, etc. The data includes PII about bank customers, guarantors, and vendors who provided services to the bank, as well as bank employees, officers, and directors.

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: System User Information)	☐	☒

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

Data Source	Description of Information Provided by Source
FDIC Business Data Services (FBDS)	Failed bank data stored in the DIR Research Environment includes: Loan and Collateral Files, Deposit Files, FI Financials, Email, File Shares, Suspicious Activity Reports, Reports of Examinations, Payroll records, HR records, Board Minutes, and other related FI records. This data has the potential to include PII including but not limited to: full name, DOB, SSN, mother's maiden name, home address, financial information, employment status/history, etc., pertaining to the following categories of individuals: •Customers •Failed Bank Vendors •Failed Bank Officers, Directors, and Employees

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

The ATO was issued on 1/9/2021 and will be periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

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

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. This PIA clarifies the use and retention of failed bank data for thirty years for research purposes.

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.

The following SORN applies to the project: FDIC-038, Failed Insured Depository Institution Research, which covers loan and collateral files; deposit files; financial institution financials, email, file shares, Suspicious Activity Reports, Reports of Examinations, payroll records, human resources records, Board of Directors' minutes, and other related records as necessary to meet the FDIC statutory requirements.

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

No. FDIC-038, Failed Insured Depository Institution Research is a new SORN. Generally, FDIC conducts reviews of its SORNs every three years or as needed.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01 'Forms Management Program'. However, the information covered by FDIC-038 Failed Insured Depository Institution Research is typically collected from the insured depository institutions and therefore no Privacy Act Statement would be required.

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: The FDIC retains failed bank data for thirty years in order to use those records for research purposes in accordance with a newly established records retention schedule. The retroactive application of the records schedule results in the maintenance of failed bank data for longer than the public may have expected at the time of collection based on 12 U.S.C. 1821(d)(15)(D).

Mitigation: The FDIC conducted this PIA, which informed the establishment of the new thirty-year retention period for the use and retention of failed bank data for research purposes, and has made the PIA publicly available on the FDIC.gov website. The FDIC has also established a new System of Records under the Privacy Act, FDIC-038 Failed Insured Depository Institution Research, notice of which has been published in the Federal Register and is available on the FDIC.gov website.

Section 3.0: Access and Amendment

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

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

The FDIC 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. Access procedures for this information system or projected 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 1360.20. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

The FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.20. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

3.3 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 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1360.20.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable risks associated with access and amendment.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

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

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

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

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

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

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

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes personally identifiable information (PII); (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.20). 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?

Contractor staff manage the operations and security of the DIR Research Environment, including the establishment, activation, modification, review, disablement, and removal of system accounts. Contractor staff also load failed bank data into the DIR Research Environment and are responsible for transferring research results out of the DIR Research Environment upon receiving authorization to do so, and logging all such approved transfers.

Academic researchers and researchers from other agencies may serve as visiting scholars in DIR. These visiting scholars contract with the FDIC and may be provided access to conduct research, in conjunction with FDIC staff, using the failed bank data. These visiting scholars, like FDIC staff, are subject to the research governance framework and responsible for protecting privacy and confidentiality when using the failed bank data for research.

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, appropriate confidentiality agreements have been completed and signed for contractors who work on the project. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

Prior to obtaining access to failed bank data in the DIR Research Environment, researchers receive in-person training that covers all five components of the multi-pronged approach to protecting privacy and confidentiality when using the failed bank data for research. This training is repeated annually. Researchers receive documentation with detailed rules-of-thumb that they are required to use in preparing their research output for disclosure review and these detailed rules-of-thumb are covered in the training. The training also reminds researchers to report only aggregate statistics that they need to support their analyses; and to report aggregate statistics with a level of precision that conveys results and protects from re-identification risk.

The FDIC Privacy Program also maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

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

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

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

Failed bank data in the DIR Research Environment are secured with multi-factor user authentication and FIPS 140-2 validated encryption. Additional technological safeguards include but are not limited to:

- the disabling of users' ability to screen capture and to copy contents from inside the DIR Research Environment and paste outside of the Environment;
- the disabling of Internet access for users; and
- the disabling of file transfer ability for users from inside the environment to locations outside the environment.

The technological safeguards, together with research governance framework ensure that:

- no failed bank data is removed from the DIR Research Environment;
- all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and meets disclosure avoidance requirements to minimize the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment; and
- all research results that are removed from the environment are logged.

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

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and FDIC Circular 1360.20. Disclosures are tracked and managed using FDIC's Freedom of Information Act 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.

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.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There is minimal privacy risk to accountability due to the adoption of a research governance framework that helps protect privacy and confidentiality when using the failed bank data for research. All components of this five-pronged approach are continuously reviewed and regularly revised to incorporate applicable elements of industry best practices.

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. § 1822: deals with FDIC as a Receiver of failed banks
- 12 U.S.C. § 1820: discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 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 C.F.R. § 360.11: deals with records of failed insured depository institutions
- 12 C.F.R. § 366: deals with FDIC contractors

Privacy Risk Analysis: Related to Authority

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

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?

Failed bank data collected in accordance with 12 C.F.R. § 360 are evaluated for continued retention for research purposes with the goal of maximizing the value of the failed bank data to inform decisions made by multiple FDIC Divisions through research and analyses and protecting the confidentiality and privacy of the information in failed bank data that are used in research.

Additionally, through the conduct, evaluation and review of privacy artifacts,[3] 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?

Failed bank data are collected and retained with the goal of maximizing the value of the failed bank data to inform decisions made by multiple FDIC Divisions through research and analyses and protecting the confidentiality and privacy of the information in failed bank data that are used in research. The FDIC discussed the evidentiary needs of the FDIC and the public when it issued the

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

Final Rule, Record Retention Requirements, 81 Fed. Reg. 41411 (June 27, 2016). PII is not the focus of the research; typically, it is used to match records, such as matching a master record with a transaction record.

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.

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

Failed bank data in the DIR Research Environment is maintained for thirty years after the appointment of FDIC as receiver. Additionally, data is retained in accordance with FDIC Circular 1210.01, "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9.

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 bank data in the DIR Research Environment are not used for testing or training.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: The volume of failed bank data maintained for thirty years is significant, and the maintenance of any records creates a vulnerability of such records to unauthorized access, use, disclosure and retention.

Mitigation: The collection of failed bank records is determined by operational application of rule 12 C.F.R. § 360, which addresses the risk of over-collection of information that is made available for research in the DIR Research Environment. Continued retention of failed bank data for research purposes is based on the nature of the data, the availability of tools to analyze that data, and the relevance of that data to providing the public with a sound deposit insurance and contributing to the broader academic literature on many topics of relevance to the FDIC. The FDIC evaluated a number of proposals to determine the extent to which all or portions of failed bank data should be maintained and for how long. It was determined that all failed bank data are valuable to the Corporation for addressing current policy-relevant questions and are also likely to prove critical in addressing future policy-relevant questions. Failed bank data represent a source of data that are not otherwise available for research and analysis, and have the potential to allow the FDIC to answer important questions that would otherwise not be answerable. At times, these policy questions come at a time of crisis, where having detailed data provide critical decision-making support and finding the data elsewhere is not an option. Finally, the FDIC established a retention schedule to ensure that records are not maintained longer than necessary to support research purposes.

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.

DIR receives the failed bank data from DRR, which collected the data in a forensically sound manner from the systems of failed banks. DRR validates the collected data against the data in the source systems but does not otherwise have any ability to assess the accuracy, relevancy, timeliness, and completeness of the PII data. When the data is transferred to the DIR Research Environment, validation checks are performed to ensure that the transferred data match the source data. Similar to DRR, DIR does not have the ability to assess the accuracy, relevancy, timeliness, and completeness of the failed bank data.

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?

DIR receives the failed bank data from DRR, which collected the data in a forensically sound manner from the systems of failed banks. No data is collected from individuals.

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

DIR receives the failed bank data from DRR, which collected the data in a forensically sound manner from the systems of failed banks. DRR validates the collected data against the data in the source systems but does not otherwise have any ability to detect or correct inaccurate or outdated data. When the data is transferred to the DIR Research Environment, validation checks are performed to ensure that the transferred data match the source data. Similar to DRR, DIR does not have the ability to detect or correct inaccurate or outdated PII data. Also, no users in the DIR Research Environment have the ability to change any of the failed bank data.

The FDIC reviews privacy artifacts to ensure there are no missed opportunities 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.

DIR has implemented a five-pronged research governance framework that maximizes the value of failed bank data to inform decisions made by multiple FDIC Divisions and protects the confidentiality and privacy of the data used in research. No failed bank data is removed from the DIR Research Environment. All research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and meets disclosure avoidance requirements to minimize the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment. The research governance process includes consulting with stakeholder divisions within the FDIC, including a review of privacy considerations and a review by subject matter experts, as well as FDIC management review, before research is distributed publicly.

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 uses the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII.

The Office of the Chief Security Officer prescribes administrative and technical controls for the system or project based on the FIPS 199 determination.

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable risks associated with data quality and integrity.

Mitigation: 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.

The system or project 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. This PIA serves as notice of the information collection. The FDIC does not make decisions regarding individuals based on the PII received from third-parties.

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.

The system or project 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. This PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. The FDIC does not make decisions regarding individuals based on the PII received from third-parties.

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

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

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

The project or system only uses PII for the purposes listed in Section 9.1. This PIA serves 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 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: Individuals are not provided with an opportunity to choose to participate in research related to failed banks.

Mitigation: The FDI Act gives the FDIC general power to succeed to title to the books, records, and assets of any previous conservator or other legal custodian of a failed bank, and conduct research and analyses to inform decisions regarding core business objectives of the FDIC. This legal authority and the FDIC-038 Failed Insured Depository Institution Research SORN provide 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.

DIR uses the failed bank data to conduct research and analyses that inform decisions regarding core business objectives of the FDIC. The findings from research and analyses of this data have the potential to help the FDIC improve its operations and processes, and to inform national and international policy discussions and rule-making in areas as varied as resolutions, emerging risks and risk assessments, deposit insurance, and banking policy, among others. Research using this data can also provide important contributions to the broader academic literature on many topics of relevance to the FDIC.

DIR has implemented a research governance framework to protect privacy and confidentiality when using the failed bank data for research.

Other than research outputs that don't include PII, disclosures of failed bank data from the DIR Research Environment are limited to the Routine Uses outlined in the FDIC-038 Failed Insured Depository Institution Research SORN, which include sharing PII to enable the management of a privacy breach, to contractors or other third parties working on behalf of the FDIC, and to congressional offices to address requests for constituent services.

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.

DIR has implemented a research governance framework that maximizes the value of failed bank data to inform decisions made by multiple FDIC Divisions and protects the confidentiality and privacy of the data used in research. The governance framework has five prongs. The overarching goals in the design of the five-pronged approach are to ensure that:

- no failed bank data is removed from the DIR Research Environment;
- all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment; and
- all research results that are removed from the environment are logged.

All components of this five-pronged approach are continuously reviewed and regularly revised to incorporate applicable elements of industry best practices.

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.

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

Access to the DIR Research Environment and the failed bank data housed therein is available to authorized DIR staff and to DIR visiting scholars (who are FDIC contractors) who work in conjunction with DIR staff. A formal application for access is required. In the application, the researcher agrees to uphold confidentiality and to abide by rules-of-behavior. In addition, the researcher receives in-person training that covers all five components of the research governance framework to protecting privacy and confidentiality when using the failed bank data for research. This training is repeated annually. The authorization process is implemented using an automated workflow that requires multiple approvals before the researcher is approved for an account in the DIR Research Environment. All requests and approvals are logged in the system and available for auditing. Access is reviewed monthly and access is promptly removed for users who no longer need access to the failed bank data.

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

☒ No
☐ Yes Explain.

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, the failed bank data in the DIR Research Environment will not be used to make determinations about individuals nor will it be used to derive new data about individuals. Research will be conducted using combined data from many individuals or entities to inform decisions regarding core business objectives of the FDIC.

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.

No failed bank data is removed from the DIR Research Environment. All research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment. Removal of research results can only be carried out by staff with specific authorization. All research results that are removed from the environment are logged.
Further, through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1360.20, Privacy Program, and FDIC Circular 1360.17, "Information Technology Security Guidance for FDIC Procurements/Third Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9.

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.

DIR has implemented a research governance framework that maximizes the value of failed bank data to inform decisions made by multiple FDIC Divisions and protects the confidentiality and privacy of the data used in research. The governance framework has five-prongs: The overarching goals in the design of the five-pronged approach are to ensure that:

- no failed bank data is removed from the DIR Research Environment;
- all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment; and
- all research results that are removed from the environment are logged.

All components of this five-pronged approach are continuously reviewed and regularly revised to incorporate applicable elements of industry best practices.

Annual Information Security and Privacy Awareness Training is mandatory for all FDIC 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.

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

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: Given the highly individualized nature of the information in failed bank data, it is possible that the publication of statistical analyses could, alone or in combination with other data available outside of the DIR Research Environment, inadvertently lead to the disclosure of sensitive information.

Mitigation: To reduce this risk, FDIC has implemented a disclosure review process wherein all research results (e.g., tables, charts, and text excerpts) are reviewed to ensure that the results are aggregated and minimizes the risk that individuals can be identified before the results are allowed to be removed from the DIR Research Environment. Removal of research results can only be carried out by staff with specific authorization.

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

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

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

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

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

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

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

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks associated with security.

Mitigation: No mitigation actions are recommended.