FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Resolutions and Receiverships (DRR)

Regulation 12 CFR 360.9 Large-Bank Deposit Insurance Determination Modernization Project

Date Approved by Chief Privacy Officer (CPO)/Designee
4/3/2018

Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

This project directly supports the FDIC's goal of achieving compliance with regulation 12 CFR 360.9, Large-Bank Deposit Insurance Determination Modernization (LBDIDM) rule.[3]
It is intended to allow the deposit and other operations of a large insured depository institution (defined as a "covered institution") to continue functioning on the day following failure. It also is intended to permit the FDIC to fulfill its legal mandates regarding the resolution of failed insured institutions to provide liquidity to depositors promptly, enhance market discipline, ensure equitable treatment of depositors at different institutions and reduce the FDIC's costs by preserving the franchise value of a failed institution. When an institution fails, the FDIC facilitates the transfer of the institution's deposits to an assuming institution or pays insured depositors directly. The FDIC's goal is to provide customers with access to their insured deposits within one to two business days. The FDIC continually monitors changes

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

[3] For details visit the FDIC website for 12 CFR 360.9.

in financial institution operations and products to ensure the FDIC's ability to handle potential financial institution failures. The FDIC develops, tests, and maintains contingency plans to ensure it is prepared to handle a wide range of potential failure scenarios, including the failure of a large financial institution; simultaneous, multiple failures; the failure of an institution with large international holdings; and the failure of an insured institution that operates primarily through the Internet.
Method: The compliance testing, through use of a productivity tool developed using Statistical Analysis System (SAS) programs, encompasses a review of the format and layout of standardized data extract files (as detailed in the rule), linkages between the files, provisional hold calculations, and the institution's capability to process FDIC holds. The data is collected as described in Section 3.4, processed by the SAS tool, and stored as local files on a user's computer. Upon completion of the testing, raw and any generated data files will be removed by using Entrust Secure Delete.

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

The following PII is needed to ensure institutions are complying with 12 CFR 360.9: Full Name, Date of Birth, Social Security Number (SSN), Home Address, Home Phone, Financial Information (Bank Account Numbers and Account Balance), and Non-work Email Address. This data is used to ensure that the correct holds are placed on deposit accounts in the event of a failure of a large bank.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

The data is used to verify that covered institutions are adhering to Regulation 12 CFR 360.9. This is a project that supports the FDIC testing requirements and the FDIC in the event of a large bank failure as noted in Regulation 12 CFR 360.9, which states that covered institutions must provide appropriate assistance by providing data files for FDIC to review to ensure they are complying with the regulation.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

a) Explain the business purpose/need requiring the collection of SSNs.
12 CFR 360.9 requires FDIC to validate that a covered institution shall be able to provide a standard data format for deposit account data. The tax identification number maintained on the account is one of the required data fields. For consumer accounts, typically, the tax identification number would be the primary account holder's SSN.

b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

☒ Yes List any additional legal authorities: Regulation 360.9 "Large-Bank Deposit Insurance Determination Modernization"
☐ No

c) Is the SSN is masked or otherwise truncated within the system?

☐ Yes. Explain:
☒ No. Is it possible to mask or otherwise truncate the SSN within the system?
☐ Yes. Explain how it may be masked or truncated and why this has not been implemented:
☒ No. Explain why it may not be masked or truncated:
Due to the size of the institutions that fall under the regulation, truncating the SSNs will not allow the staff to identify the bank depositor accounts for insurance determinations. If only the last 4 digits are used it will be the same as other

depositors' SSNs, and the insurance determination will be incorrect and could potentially provide monies to the incorrect depositor.

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

☒ Yes. Explain: Bank Account numbers are restricted to DRR CFI staff that has been granted access by DRR Management

☐ No. Is it possible to restrict access to specific groups of users within the system?

☐ Yes. Explain how access may be restricted and why this has not been implemented:

☐ No. Explain why access cannot be restricted:

3.4 Who/what are the sources of the information in the system? How are they derived?

Members of the Large Bank Deposit Claims & Compliance team request standardized, formatted deposit files from the bank or its servicer. The bank or servicer is requested to transmit the files via their secured FTP file transfer tool; or, via FDIC's GlobalScape Secured FTP file transfer protocol. In some occasions, the bank may insist that files be provided via read only encrypted USB drive or CD/DVD disk that are owned by the bank and remain at the bank site.

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

No federal, state or local agencies provide data for this project.

3.6 What other third-party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

With the exception of the covered institutions no other third party provides data for this project.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☐ Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

☒ No Explain: Explain: The information is not obtained by individuals, but instead through a download of the data from the large bank during the compliance review process; therefore there is no opt-out option for individuals.

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

- FDIC DRR CFI Assistant Director – As the Program Manager the DRR CFI Assistant Director will have access to review and certify the data as advised by direct reports.
- Members of the Large Bank Deposit Claims & Compliance team (DRR CFI Staff) - Will have access to the data and will use the data to verify that large banks are adhering to 12 CFR 360.9, and also during closing of larger institution failures.

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

The DRR CFI Assistant Director determines the process to grant access to the data. Access to actual bank depositor PII and SI data is granted to the employees in the Large Bank Deposit Claims & Compliance team or other vetted DRR personnel.

Once an institution is determined to be covered by regulation 12 CFR 360.9, FDIC notifies the covered institution that they have 18 months to become compliant.

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

☒ No
☐ Yes Explain.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

No data is being shared with other agencies.

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

While the Assistant Director, DRR Complex Financial Institutions Operational Readiness & Assurance (ORA), is ultimately responsible, all parties who access the data are responsible for protecting the privacy rights of the public and employees affected by the interface. The policy and procedures for responsibility and accountability are included in the Corporate and DRR Security Awareness and Privacy Trainings which includes Rules of Behavior. All users must agree to abide by the Rules of Behavior before access is granted to the FDIC network and annually thereafter.

4.6 What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

DRR utilizes contracted developers who have the primary responsibility for design, enhancement, and maintenance of PHS. All individuals who have access to PHS have a security clearance and are required to complete a Contractor Confidentiality Agreement and Non-Disclosure Agreement on an annual basis. In addition, access requests must be approved by each contractor's Oversight Manager and the PHS Owner or the Project Manager. In addition, the contractors do not have access in the production environment where the live data is stored.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

All data attributes will be validated against regulation 12 CFR 360.9 to ensure data type, data length, and data linkages is accurate. The provisional hold amounts from the covered institutions are compared against the ones calculated by the FDIC. By regulation, all data files will be provided to the FDIC through an automated mechanism to ensure timeliness. Control totals will be provided by the covered institutions to check for data completeness. In addition, IT resources will have built-in controls for accuracy and completeness.

5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.

DRR Circulars and Job Aids, maintained by the Large Bank Deposit Claims & Compliance team, are the official documents to ensure the data is protected. These documents have been reviewed and approved by DRR Information Security Unit (ISU) team. Access to the data is granted using the discretionary access control method. Discretionary access is granted for users that perform specific job task and requires that access to the data to complete said job tasks. Access will be reviewed on an annual basis as per FDIC/DRR directives and guidelines.

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

During compliance testing SAS stores the data locally on a computer. Deposit account identifiers, for example, Bank Account Numbers, are used to retrieve data. Name and social security number are not used for provisional hold processing. All the bank data, including the SSN, are truncated as soon as the compliance testing is completed.

6.2 What kind of reports can be produced *on individuals*? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?

There are no reports produced on individuals.

6.3 What are the retention periods of data in this system? 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.

DRR CFI Assistant Director has determined that the retention period for storing and maintaining data is no more than 6 months from the time the data is received by FDIC DRR CFI. Upon completion of the compliance testing raw and any generated data files will be removed by using Entrust Secure Delete. Bank staff will be asked to observe the removal of any bank data containing PII or SI.

6.4 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

A FDIC SORN is not applicable to the data collected for compliance testing for regulation 12 CFR 360.9 testing as it is open bank data and owned by the bank and not the FDIC.

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

N/A

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy 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. This project will not aggregate or consolidate data in order to make privacy determinations or derive new data about individuals.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

No. This project will not use new technologies, such as those specified above, to collect, maintain or track information about individuals.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

No. This project will not be used to monitor individuals or users.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

The unauthorized disclosure of privacy-related data used for this project could have a serious adverse impact on FDIC's reputation and is deemed to be a moderate risk. Also, there is a high risk of harm if the depositor data in this project is misused or if unauthorized access is obtained. Since this project relates to insurance determinations for bank deposit data which includes an individual's PII, it is necessary to maintain safeguards against the potential of fraud or theft from either FDIC employees/contractors or persons outside the Corporation. Disclosure of this data could be harmful to both individuals and the FDIC reputation.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

No. The completion of this PIA did not result in changes to business processes or technology.