FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Resolutions and Receiverships (DRR)/Risk Share Data Analysis & Reporting

Receivership Assets Data Repository (RADR)

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.

To support the FDIC DRR Loss Share Program, DRR uses the loss share process to maximize asset recoveries and minimize FDIC losses during bank resolutions. A miscalculation can cost the FDIC a significant amount of money. The Receivership Assets Data Repository (RADR) is intended to simplify reporting and analysis of receivership asset data by combining data from multiple sales initiatives in a common, easy-to-use format. It currently includes Loss Share data extracted from the Resolution Transaction Submission Portal (RTSP) data aggregator application housed offsite at Midland Services, Inc. The RTSP sends a daily file using a secure transition method via FTP to the FDIC and that file is used to update the RADR. The data transferred in this process is financial data and is uploaded using an automated process.

[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.

The RADR is used by the FDIC Chairman's office and DRR Senior Management to monitor the status of the agreements in an easy to use format.

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.

RADR contains both PII and non-PII data for loans covered by loss share and LLC agreements. The data is obtained directly from the RDA (also known as the FDIC Resolution Transaction Submission Portal [RTSP]) on a weekly basis. This data is retrieved for research as well as reporting to the FDIC's Executives, Senior Managers, and other staff members. The file from the RDA includes the following types of PII about borrowers or customers of failed financial institutions:

- Full Name
- Home Address
- Home Phone Number(s)
- Email Address (non-work)
- Financial Information and/or Numbers (e.g., bank account numbers)
- Taxpayer ID number (which may be an individual's Social Security Number [SSN])

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

The purpose and intended use of the information is to report loss share and limited liability company (LLC) agreement information to the FDIC's Executives, Senior Managers, and other staff members.

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: The field in RADR is labeled as TAXPAYERID, however there is no way to know if it either a TIN or a SSN. The TIN is collected from the borrower as part of the loan application process and used to verify credit worthiness and for possible collection efforts if required. It is included in RADR to help find related loans.

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: 12 U.S.C. § 1820
☐ No

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

☒ Yes. Explain: The RTSP data is masked when placed in RADR and is not visible to the RADR users.
☐ 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:

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

☒ Yes. Explain: It is stored only the database is not viewable to end-user
☐ 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?
When a financial institution is placed into receivership and the FDIC is named receiver, data is extracted from the failed institution's loan and asset files. After the Purchase and Assumption (P&A) agreement has been executed, the loan and asset data covered by the loss share agreement is segmented out from data not covered by the P&A agreement and it is transmitted to the RDA where it is managed and stored. When an AI files a claim for losses incurred on assets, the data provided by the AI is compared against data loaded into the RDA to ensure claims are accurate. That data is then transmitted to RADR and made available to FDIC staff and contractors for reporting and analysis.

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 will not have access RADR data.

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.

Not applicable. No, other third-party sources will be providing data to RADR.

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)?

☒ No Explain: The information in RADR is not obtained from individuals, but instead through a download of the data from the failing institution to the RDA during the closing process and then sent to RADR; therefore, there is no opt-out option for individuals.
☐ Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

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.

No external parties will have access to the data. The FDIC's Division of Information Technology (DIT) Staff members will have access to the data for the sole purpose of formatting the data for viewing in RADR. FDIC Executives, Senior Managers, and other staff members will have access to the data to view Loss Share Agreements status.

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

Access to the data is completed via an online process through FDIC's automated access management system. All access requests must specify the business reason for access to the RADR DataMart or Operational Data Store. RADR contains two access levels/roles which separate functions that can be performed and information that can be viewed in the DataMart. Users who request access must specify an access level or role relevant to their specific job tasks. Requests for access to the DataMart are granted on a "need to know" basis and must be approved by the user's Manager and the Data Owner before access can be granted.

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. There are several internal downstream applications that have access to RADR data. These are Receivership Oversight Management Systems (ROMS), ReALM, Shared Loss Monitoring Tool and the Risk Sharing Asset Management (RSAM) Dashboard.

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.

Other agencies or entities do not have access to data in RADR.

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.

The FDIC/DRR Program Manager is responsible for protecting the privacy rights of individuals by developing data access guidelines and standards which must be followed and customizing RADR to meet those standards. In addition, it is every user's responsibility to abide by FDIC data protection rules that are outlined in the Corporate Information Security and Privacy Awareness training which all employees must 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.

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?

DIT utilizes contracted developers who have the primary responsibility for design, enhancement, and maintenance of the RADR DataMart. All individuals who have access to RADR 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 DataMart Owner or the Project Manager.

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?

Control totals are sent with the RADR files on a weekly basis and an automated process is in place to verify the data transmitted from the RDA is the same that is loaded into the RADR database.

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

RADR adheres to the Office of Management and Budget (OMB) Circulars A-123 and A-130, which notes that every system or process that stores or maintains government data must have controls in place to prevent the misuse by those having access to the data. RADR has the following controls:

• Access to the data is completed via an online process through FDIC's automated access management application. Requests for access to the DataMart are granted on a "need to know" basis and must be approved by the user's manager and the DataMart Owner before access can be granted.

• RADR users undergo a Supervisor Access Review on an annual basis. This review includes contacting the user's manager to determine if the user still requires access to the DataMart and if they have the appropriate access levels/roles to perform their assigned job tasks. If access is no

longer required or if changes to a user's access level/roles is needed, the user will either be removed or their access level/roles will be updated accordingly.

• When users leave DRR or the Corporation, the RADR Administrator receives a request from the Corporation's automated access control application and the user's access to the DataMart is removed immediately.

As of December 2016, only users that require PII data will be able to access fields containing PII.

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.

Data can be retrieved by personal identifiers such as name, TIN/SSN, or account numbers. This data can only be viewed by a limited number of users who has access to the RADR Universe in Business Objects and has the ability to search and create reports on any field that is in the RADR Universe. There are no canned or standard reports for RADR.

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 canned reports for RADR. Reports on individuals can be created and pulled by any identifier listed in RADR Universe which includes Name, TIN/SSN and account number. The reports are used to monitor the Acquiring Institution's agreement with the FDIC, Loss Share submissions in their portfolio. Reports are maintained on a quarterly basis which is the next time the Acquiring Institutions sends their updated Loss Share Agreement information at which time the old reports are no longer accurate and can be deleted. New reports may be produced using the new data received from the Accruing Institutions.

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.

There are two Retention Periods for this application:

RAR2000 Resolutions and Receiverships Failed Financial Institution Records 10 Years Old or Older

- Description - Records created by and/or acquired from a failed financial institution that become the property of the FDIC as a result of receivership proceedings. Includes all records at least 10 years old at the time of appointment as receiver that are not relevant to any pending or probable future litigation.
- Retention Timeframe – Upon Appointment as Receiver

RAR2010 Resolutions and Receiverships Failed Financial Institution Records Less Than 10 Years Old

- Records created by and/or acquired from a failed financial institution that become the property of the FDIC as a result of receivership proceedings. Includes all records less than 10 years old at the time appointment as a receiver, or that may be relevant to any pending or probable future litigation.
- Upon Appointment as Receiver + 6 years

The data is being overwritten. The Loss Share Program will be ending within the next 4 or 5 years and at that time the information will be maintained or disposed of as noted in the FDIC retention requirements.

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

RADR operates under FDIC SORN #30-64-0013, *Insured Financial Institution Liquidation Records.*

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

Not applicable.

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. RADR 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. RADR 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. RADR 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 in RADR could have a serious adverse effect impact on FDIC's reputation and is deemed to be a moderate risk. Also, there is a high risk of harm if the data in RADR is misused or if unauthorized access is obtained. Since RADR is used to track loss share agreements which include 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 Corporation.

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.