FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Risk Management Supervision (RMS)

Regional Automated Document Distribution and Imaging System (RADD)

FDIC PRIVACY PROGRAM

Date Approved by Chief Privacy Officer (CPO)/Designee*

date to be inserted after approval by the FDIC Privacy Program Staff in DIT

04/12/2017

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.

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions for safety and soundness and consumer protection, and managing receiverships.

The Regional Document Distribution and Imaging System (RADD) supports the FDIC's examination and supervision mission by providing an electronic document imaging, distribution, and storage system for final

[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.

financial institution correspondence and examination workpaper documents. Correspondence is stored in RADD in PDF format with hard copy documents stored temporarily in the FDIC Regional Offices. Long-term storage of hard copy documents (correspondence only) is offsite at Iron Mountain . Examination workpapers are also stored in RADD in Word, Excel, PowerPoint, and PDF format, but hard copy workpapers are no longer retained.

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.

RADD contains copies of examination workpapers, reports of examination, correspondence, and various other information[3] related to financial institution (FI) examinations, applications[4], and enforcement and supervisory actions. These documents may include the following types of PII: full name; date of birth; Social Security Number (SSN); photographic identifiers; driver's license/state identification number; biometric identifiers; employee identification number; vehicle identifiers; home address; non-work phone numbers; financial information or numbers; certificates of birth, death, marriage, naturalization, or marriage; legal documents or records, such as divorce records or criminal records; investigation reports; Web URLs; non-work email addresses; education records; military status and/or records; employment status and/or records; and foreign activity or interest reports. The aforementioned PII may pertain to the following categories of individuals: persons of interest (POIs)[5]; FI officials; FI applicants for insurance, re-instatement, management control, etc. (the aforementioned PII is most likely to pertain to this category of individuals); and FI customers[6].

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

The information specified in Question 3.1 is necessary to support the examination and oversight functions of the FDIC. More specifically, the information is used to assess the FI and/or FI staff viability, conformance with regulations, applications, etc., in order to avoid a negative impact to the insurance fund. Loan, deposit, and other FI records are reviewed directly to help determine the viability of an institution's underlying assets as well as compliance with consumer regulations. Additionally, information is provided to support bank applications, identify suspicious activity, and various other oversight functions. While the PII obtained from applicants is used to determine their worthiness, most other PII contained within RADD is typically non-sensitive and/or part of broader documentation used to supervise the institution (e.g. a loan agreement has a borrower's address on it, but the agreement is used to support the borrower's obligation to the bank). Sensitive PII, such as a SSN, is used to run credit checks for applicants and POIs (i.e., persons under investigation).

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

a) Explain the business purpose requiring the collection of SSNs. As part of the FDIC's examination and supervision mission, RADD facilitates the document imaging, distribution, and storage for examination

[3] This description may not be all inclusive due to the nature of the documents being processed. Document content is subject to author discretion unless covered by a specific examination or supervisory related policy.
[4] Applications for insurance, re-instatement, management control, etc.
[5] Individuals who are considered to be possible suspects in investigations.
[6] PII pertaining to FI customers is generally limited to contact information, such as home address, email address, and phone number, if collected at all.

documents, some of which may contain SSNs. SSNs are not commonly obtained, but if needed directly (or if embedded in more important information), they are used to obtain credit reports or for other investigatory purposes. The collection of SSNs is incidental to the document imaging, distribution, and storage for examination documents, and is not required for the scope of work being conducted.

b) Provide the legal authority which permits the collection of SSNs. 12 U.S.C. § 1820, et. seq. The collection of SSNs is incidental to the document imaging, distribution, and storage for examination documents, and is not required for the scope of work being conducted.

c) Identify whether the SSN is masked or otherwise truncated within the system: The electronic documents uploaded to RADD are not altered as they represent official correspondence or workpapers that support FDIC's position if any eventual legal actions are brought forth.

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

RADD receives non-sensitive institution structure and examination data from the following FDIC systems: Virtual Supervisory Information On the Net (ViSION) and System of Uniform Reporting of Compliance and Community Reinvestment Act (CRA) Exams (SOURCE). In addition, documents contained in RADD are either generated by FDIC staff or provided directly to FDIC by another agency, institution, or persons (e.g., attorneys, auditors, etc.). FDIC-generated documents, such as memorandums to file, letters to bank, reports of examination, etc. are derived from layers of analysis and review. Correspondence files are obtained in electronic or hard copy format. All correspondence is scanned by administrative staff and is stored in RADD in PDF format with hard copy documents stored temporarily in the FDIC Regional Offices. Long-term storage of hard copy documents (correspondence only) is offsite. Examination workpapers are also stored in RADD in Word, Excel, PowerPoint, and PDF format, but hard copy workpapers are no longer retained. Examination workpapers are created internally (templates, analysis, etc.) by FDIC staff, provided electronically by the institution (or person), or obtained directly onsite at the FI. Documents received electronically are imported directly by examination staff and remain in their electronic form (stored in Word, Excel, PowerPoint, or PDF formats). Hard copy workpaper documents are scanned to PDF by examination staff using FDIC-provided scanners. These scanners create a PDF on the examiner's desktop, which is imported/moved into RADD by the examiner.

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?

No other federal agencies directly interface with RADD. Final correspondence from other federal agencies may be scanned into a PDF and electronically filed in RADD. Examination workpapers provided electronically by another agency may remain in their original format providing they are Word, Excel, PowerPoint, or PDF. All other documents would be scanned to PDF.

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.

Financial institutions or their representatives (auditor, attorneys, etc.) can submit information in various formats to FDIC. Correspondence is scanned into PDF files. Examination workpapers provided electronically may remain in their original format, providing they are Word, Excel, PowerPoint, or PDF. Other documents would be scanned to PDF. Documents are stored in RADD in the virtual bank file of the institution, mimicking the paper filing of correspondence (Official Bank Files of the regional office file rooms) and examination workpapers. This information is used for analysis, monitoring, examination, ad-hoc reporting and other assignments.

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: RADD does not collect any data directly from individuals. Information is gathered through examination and supervision activities of the FDIC and other institution regulators.

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.

RMS and DCP examiners, analysts, administrative staff and management will have access to information in RADD to support their oversight responsibility (e.g., analyze viability, approve applications, investigate issues, etc.). Certain FDIC Office of Complex Financial Institutions (OCFI), Division of Resolutions and Receiverships (DRR), Division of Insurance and Research (DIR), Office of Inspector General (OIG), and Legal Division staff will have access to information in RADD for similar reasons as mentioned above. Authorized FDIC Division of Information Technology (DIT) system administrators will have access to RADD for purposes of system administration, updates and maintenance. DIT contractors may also have access to RADD in order to administer and maintain associated network resources.

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

All authorized users who have access to the data in RADD must have the approval of their Manager/Supervisor and the RADD Program Manager/Data Owner before access is granted to the system. Access to RADD is limited to defined groups. Access is granted to a specific role structured within RADD that sets systems and data access privileges, which limits a user's access to a specific function and regulates a user's ability to update data for a specific function.

All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

RADD automatically requires each user to complete security awareness training within the system on an annual basis. Failure to do so prevents access to the system. This training has specific information regarding compromise and the prevention of misuse of data.

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. RADD shares document meta data with Interim Bank Contact, which does not contain PII, for the purposes of generating reports.

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 other agency or entity has access to the system. Documents retained in the system are shared with counterpart agencies according to corporate supervision and examination guidelines.

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 RADD Program Manager/Data Owner is responsible for the management and decision authority over a specific area of corporate data. The RADD Program Manager/Data Owner and RMS Information Security Manager (ISM) serve as the sources of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

Although the RADD Program Manager/Data Owner and RMS ISM share overall responsibility for assuring proper use of the data, it is every user's responsibility to abide by FDIC data protection rules, which are outlined in the annual IT Security and Privacy Awareness Certification, that all employees take and certify that 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?

FDIC contractors are involved with the resource server and SQL server maintenance. Such contractors are subject to the FDIC's contract provisions for confidentiality and non-disclosure.

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?

RADD data consists of structure information (institution name, location, supervisory region, etc.) and document information (document name, source, etc.). Structure information comes from other systems such as ViSION and is updated daily with critical fields reviewed/approved for update by RADD administrators as needed. Document information is indexed by specifically designated RADD indexing personnel and reviewed by the assigned case manager or review examiner. Additionally, RADD administrators regularly review indexing to ensure consistency and accuracy.

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

Access to the data in RADD is limited to defined NT groups and system roles. Examination, supervision, and select specific staff in other divisions/offices who are provided access to RADD on a "need to know" basis, are trained in handling and securing sensitive data through an annual security and privacy act awareness training within RADD (section 4.2). Additionally, RADD documents are stored on an encrypted server.

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 is retrieved by FI number (cert), FI name, or by examination date/type (compliance, safety and soundness, etc.). Personal identifiers are not used for organization or retrieval. Text searchability is available within the correspondence-related documents.

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?

N/A – no reports can be 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.

Retention periods are defined by the FDIC Reports and Information Management (RIM) Policy Manual 1210.1, which references the Records Retention Schedule (RRS). Correspondence-related documents are retained for 30 years as identified in Series 6 - Supervision section of the RRS, and are systematically deleted at the end of that period. Workpapers are generally only kept until the next examination unless subject to legal hold, under enforcement action, or other needs. BSA workpapers are kept for at least 5 years. Workpapers are deleted by end users as part of the examination process.

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

RADD is covered by various FDIC SORNs including: 1) FDIC 30-64-0002, Financial Institution Investigative and Enforcement Records; 2) FDIC 30-64-0004, Changes in Financial Institution Control Ownership Records; 3) FDIC 30-64-0005, Consumer Complaint and Inquiry Records; 4) FDIC 30-64-0008, Chain Banking Organizations Identification Records; 5) FDIC 30-64-0016, Professional Qualification Records for Municipal Securities Dealers, Securities Representatives, and U.S. Government Securities Brokers/Dealers; and 6) FDIC 30-64-0025, Beneficial Ownership Filings (Securities Exchange Act).

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

No, the SORN does not require amendment or revision.

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, the system 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, RADD is not using any of these new technologies 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.

All user access attempts to institution correspondence are reviewed systematically to determine permissions to access the document. Data is kept to monitor level of use, track document history, and monitor general activity. Additionally, general FDIC access controls, firewalls and intrusion-detection systems are used to prevent unauthorized monitoring.

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 Corporation would experience significant reputational risk if any information would be inappropriately accessed or obtained from the system.

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

No.