FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Risk Management Supervision (RMS)

Regional Report Repository (R3)

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

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

8/30/2016

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 Division of Risk Management Supervision (RMS) within the FDIC promotes stability and public confidence in the nation's financial system through examining and supervising insured financial institutions, and monitoring and mitigating systemic risks.

[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 Regional Report Repository (R3) is an Oracle Application Express (APEX) application used to facilitate reporting by the various FDIC Regional Offices to the FDIC Washington examination specialists and senior management within RMS and the Division of Depositor and Consumer Protection (DCP). Case managers and other regional personnel enter data and narrative comments into R3 regarding financial institutions within their supervisory caseloads. Additional data is queried from the Reporting Data Mart Migration (RDMM) system and combined with R3 data to satisfy regional reporting requirements to the FDIC Washington office. Reports are transmitted either electronically within R3 or exported as a Word, Excel, or PDF file and submitted to recipients as an encrypted email attachment.

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.

Of the reports produced by R3, only the Pending Enforcement Actions Against Individuals Report, commonly known as the "Pink Report", captures and reports any data pertaining to individuals. The purpose of the Pink Report is to summarize cases in which current or former bank employees or directors are suspected of causing harm to a financial institution. Individuals' names and titles, and the names of financial institutions at which they are currently or were formerly employed, are stored in the R3 database. The R3 system allows for free form narrative comments, enabling the user to potentially enter additional data elements if necessary. This may include contextually sensitive information pertaining to the subject of interest (i.e., information that may be used in a pending court case). For example, narrative comments may capture an individual's year of birth, but not the entire date of birth, and the status of pending criminal investigations. Most data collected and reported through R3 pertains to the financial condition and regulatory compliance of financial institutions.

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

FDIC Regional Offices are required to report their special examination activities to the Washington Office on a quarterly basis. The R3 system has been developed to streamline the reporting process and reduce the reporting burden. The data collected in the R3 system is used for the ongoing review and tracking of enforcement cases being processed within FDIC Regional Offices for the purposes of reporting to the Washington Office. Pink Reports including the information specified in Question 3.1 are provided to senior RMS management and the FDIC Board of Directors as Word documents exported from R3.

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

Data in the R3 system is primarily obtained from Suspicious Activity Reports[3] (SARs) filed through the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), as well as from observations reported by FDIC's financial institution examiners and investigators in the course of conducting bank examinations. Data is not collected directly from individuals. All information about individuals is input manually into R3 by case managers working in regional offices.

[3] A Suspicious Activity Report (SAR) is a confidential report filed by a financial institution about suspicious or potentially suspicious activity noted within that financial institution. Generally, if a financial transaction appears suspicious or is unusual for a particular individual affiliated with that institution, the financial institution (or the FDIC on its behalf) is required to file a SAR with the Financial Crimes Enforcement Network (FinCEN), an agency of the U.S. Department of the Treasury.

3.4 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?

The are no Federal, state, or local agencies that provide data for use in the R3 system.

3.5 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.

There are no third-party sources that provide data to the R3 system.

3.6 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: Data is collected from Suspicious Activity Report filings and observations made by FDIC examiners and investigators. As such, individuals do not have the opportunity to decline to provide their information or consent to specified uses.

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.

Data in the system is only available to authorized FDIC staff within RMS, DCP, and the Legal Division. Users are primarily case managers, attorneys, and management within FDIC Regional Offices, examination specialists and section chiefs, associate directors, deputy directors, and division directors in the Washington Office. The case managers must have access in order to input their reports. Management and directors have access to R3 in order to review information from the case manager for accuracy, as they are ultimately responsible for monitoring the risk in the financial institutions and issuing enforcement actions against individuals.

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

To gain access to R3, users must submit a request through the Identity Access Management System (IAMS). To access the Pink Report, users must select a specific role within the IAMS application access form. IAMS requests are first approved by the user's manager, and subsequently reviewed and approved by the Chief of the RMS Business Analysis and Decision Support (BADS) section, or a delegated authorized member of the BADS staff. Requests for access must include reasonable justification.

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

☒ No. R3 reads data from RDMM, but does not share data with that or any other systems.
☐ Yes

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.

The FDIC, and other Federal banking regulators, and various other agencies cooperate and exchange information when necessary to address suspicious activity affecting insured financial institutions. Authorized FDIC officials may communicate details of a SAR directly to Federal law enforcement agents of the U.S. Attorney's Office. However, no other agencies or non-FDIC entities have access to or share the data in the R3 system.

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 R3 database schema is only accessible to developers within RMS/BADS and Division of Information Technology (DIT) database administrators. The R3 system security plan does not permit developers or database administrators to grant access to Pink Report tables to other users or to external applications.

Each RMS regional office designates one or more coordinators to review case manager entries and to submit data to the Washington Office. The coordinator role is assigned to users by R3 administrators. Washington Office examination specialists further review data before it is exported as a Word document report within R3, printed, and distributed to senior RMS management.

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?

No contractors are involved in the design, development, or maintenance of R3; however, DIT may employ contractors to serve as database administrators. Contractors employed on behalf of the FDIC are required to execute a Confidentiality Agreement and a Non-Disclosure Agreement at the time of hiring.

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?

Data in the R3 system is received from RDMM. The RDMM system extracts data from other FDIC systems, such as Virtual Supervisory Information on the Net (ViSION), System of Uniform Reporting of Compliance and CRA Exams (SOURCE), Structure Information Management System (SIMS), and Call Reports. DIT manages Extract, Transform, and Load (ETL) processes to refresh the data received in the R3 system from RDMM. User-entered data in R3 is reviewed by region coordinators and assistant directors within each FDIC Regional Office for timeliness and completeness prior to submission to the Washington Office. In addition, form-level validation rules within the application ensure that the certificate number, region reviewer, region attorney, case type, date sent to Washington Office, pre-review indicator, pre-review complete date, and case complete date are populated with valid data. Database triggers are used to populate audit fields within R3 data tables.

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

Login procedures employ a DIT-built authentication scheme to authenticate each user's FDIC Network ID (NTID) and password. Additionally, authorization schemes based on the user's

membership in R3-specific NT groups grant access to specific modules, pages, and controls within the application.

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.

Yes, data in R3 is retrieved using a personal identifier. Data pertaining to individuals included on the Pink Report can be retrieved within the application through a name search.

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?

Data collected for the Pink Report may describe alleged actions taken by an individual that resulted in harm to FDIC-supervised financial institutions. The report can only be accessed by authorized FDIC personnel. FDIC Records Management Policy will apply. Retention and disposition of the records are governed by FDIC's Directive 1210.1 Records and Information Management Policy Manual.

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.

The retention periods and disposition procedures for data/records that the FDIC manages are contained in the FDIC Records Retention Schedule and guidance from the National Archives and Records Administration (NARA). Disposal is completed by electronic purging and removal of records.

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

R3 does not operate as a Privacy Act System of Records. For a listing of current FDIC Privacy Act Systems of Records, please visit: http://www.fdic.gov/regulations/laws/rules/2000-4000.html.

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

No, the system primarily captures narrative analysis of case details that are already present in other FDIC applications, such as ViSION. R3 merely moves the analysis from less-secure formats, such as Microsoft Word documents, to a secure Oracle database environment. As such, the system does not require a Privacy Act SORN 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?

Not applicable.

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.

Not applicable.

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.

R3 captures the timestamp and user ID when a record is modified. In addition, data is archived after each bi-monthly reporting cycle.

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?

Disclosure of privacy-related data from this system could potentially undermine criminal and civil investigations and actions the FDIC is pursuing against individuals, expose the Corporation to charges of defamation by those individuals, and threaten the Corporation's reputation.

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

No. The system is not being modified.