FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA) For Division of Resolutions and Receiverships

BIS SQL SERVER

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

3/25/19

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 BIS SQL Server is not a system, it is a database server used to store, analyze, transform, and distribute resolution and receivership data. The primary purpose for these databases is to process asset data for near failure and failed financial institutions. A separate database is created for each institution that is processed on this server and access is controlled at the database level. These databases are used to take data in varying formats from each individual institution and transform the data down to an FDIC standard format. Once this data is standardized it is used to create deliverables that are used to support the resolution and receivership process. These deliverables are then posted to the corresponding SharePoint site for each institution so that authorized users can access this information.

[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.

In addition to the primary purpose of processing asset data from financial institutions this server also used to store and maintain additional reference information including access request tracking, logging data, project status data, data validation rules, codes tables, audit data, and cross-reference data.

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 data below is collected from failing/failed institutions for bank closing purposes and used to capture the depositor and customer's data which DRR uses to liquidate the bank's assets and distributes payment to bank customers. In addition, asset servicers that are contracted by DRR to liquidate or service assets provide current status of all assets and are sent via various secure FTP (FDIC GlobalScape the majority of the time) processes and placed on this server for data manipulation for downloads to various DRR applications to assist with the liquidation of failed banks assets.

- Full Name
- Date of Birth
- Social Security Number
- Employee Identification Number
- Mother's Maiden Name
- Home Address
- Non-work Phone Numbers
- Financial Information and/or Bank Account Numbers
- Legal Documents, Records or Notes
- Non-work E-mail Address
- Military Status and/or Records

3.2 What is the purpose and intended use of the information you described above in Question 3.1?
DRR BIS **-** Uses this server to load data from failing banks and servicers and to perform various closing tasks.
DRR BOS **-** Converts invoice files of ORE fees from the ORE contractors into a NFE upload template format.
DRR Franchise and Reporting **-** Produces the WebFocus version of the ATR Executive summary report.
FDIC Legal Division and DRR Franchise Marketing and Sales Section **-** Reviews litigation matters for failed institutions, which are used by Legal in support of court cases and legal matter resolution.

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 SSN and litigation information is received from failing or failed financial institutions or servicers via a file to load into the following applications so business users can perform their job tasks.

- 4C **-** Failed or failing bank loan and asset information files – Collected and placed in 4C[3] so DRR can monitor payment and sale assets and loans

b) CAS **-** Failed or failing bank deposit information files – Collected and placed in CAS[4] to create deliverables from the insurance determinations for failed bank depositors. **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?**

[3] The FDIC's Communication, Capability, Challenge, and Control (4C) system is an umbrella application that provides an integrated solutions that meets the FDIC's current and future asset servicing responsibilities. Users access the DRR asset management and servicing functions in the system. Each asset within 4C is assigned a number for identification purposes. For additional information, refer to the FDIC's 4C Privacy Impact Assessment.

[4] Claims Administration System is used to identify depositors' insured and uninsured funds in failing and failed financial institutions. For additional information, refer to the FDIC's CAS Privacy Impact Assessment.

☐ Yes List any additional legal authorities:
☒ 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: Truncating the SSNs will not allow the DRR staff to identify the correct bank depositor, loans and asset accounts holder or litigant for legal matters as the last 4 digits of a SSN can be the same for numerous persons.

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

☒ Yes. Explain: The raw data files are on the BPM BIS SQL Server and are only available to BIS Staff who request access via ARCS.
☐ 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?

- **VARIOUS BANKS & SERVICERS -** Data is provided through FDIC approved secure file transfer protocol methods including GlobalScape and FDIC Connect. If these options are not available the FDIC will work with the data provider to find another secure method for delivering the required data. The data provided includes failed and failing bank loan and deposit files. This may include full name, home address, SSN, EIN, mother's maiden name, e-Mail address, military status and records, and financial information.
- **ACQUIRING FINANCIAL INSTITUTIONS -** Loss Share adjustment information is received and used to demonstrate that the sale maximizes collections on an asset by asset basis. The data is provided through GlobalScape and other FDIC approved secure file transfer methods.
- **FDIC SERVICERS -** Loan information is received from various Servicers contracted with FDIC. The data may include full name, home address, loan amounts, SSN, phone numbers, and other information related to a sale of an institution. Data is provided through GlobalScape secure connections.
- **INTERNAL APPLICATIONS & TOOLS –** Various reference data including valid codes & descriptions, request tracking, audit logs, and project status data is received from desktop applications and internal tools so that it can be securely stored on the database server.

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.

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

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 is not obtained directly from individuals, but instead through a download of the data from the failing or failed institution to be used for various bank closing tasks; 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.** Only the DRR BPM BIS has access to this server to load data from failing banks and servicers for the purpose of transforming the data and uploading the data via an Infosphere (an Extract Transform and Load tool) to various systems and tools so DRR can perform various job tasks related to bank closing and continuous monitoring of assets, loans, and litigations.

4.2

How is access to the data determined and by whom? Explain the criteria, procedures, controls, and responsibilities for granting access. The databases on the serve are categorized as either Bank Databases or Non-Bank Databases. Access to Bank Databases is granted automatically upon the creation of the database via an Active Directory (AD) group which has been created/set-up for the database. This AD group gets recertified annually via by BIS Management via ARCS. Individual users who are not members of the AD group must get BIS Management approval before being granted access to the database. Non-Bank databases have their own specific AD groups set up. Users must submit an ARCS request to get added to these AD groups which will provide access to the appropriate database. On occasions individual users may request access, which will require BIS Management approval.

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.

The following applications and tools receive data from the BIS SQL Server:

- 4C - Failed or failing bank loan information files
- CAS - Failed or failing bank deposit information files

FDIC SharePoint - BIS-produced reports for FDIC Management, Franchise Marketing, Claims and other internal groups. The BIS Deposit & Loan Teams create reports from the Bank download data. There is a separate SharePoint document library for BIS report deliverables that has different restricted access from the main shared documents library on the bank site. The reports are copied to the Bank's SharePoint site so that the various groups that require access to the reports can retrieve them. Some reports may contain PII.

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 or entities. The bank Servicers already have the data from the bank as they were the bank's Servicer prior to the bank failing so DRR does not need to send information to them. DRR only receives updates from the Servicers.

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 Manager of DRR BPM BIS is responsible for the data on the server. The collection and maintenance of the data falls under DRR's overall bank closing processes. Without this data, DRR could not perform various bank closing tasks and monitor tasks for bank liquidations. .

4.4 **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 DIT maintains the Server hardware and operating system. BIS contractors, upon BIS Management approval, can access databases and work with data within them, but cannot create or delete databases. BIS contractors have to pass the high-level security background check, and they sign a confidentiality agreement (FDIC 3700/46A) for each bank they work on before being granted access.

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?** The BIS Download Specialists, who import the data, transform and export to 4C input files have checks throughout their process to ensure record counts, data formats, and content are accurate and expected so that the load into 4C will be without errors.

5.2 **What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.** Only users (FDIC employees and contractors) who have BIS Management approval can access the data. Once a bank fails, the FDIC DRR BIS Post Close and Interim Servicing team is granted access so they can process changes to 4C until such time as all FDIC retained assets are moved off the Assuming Institution's systems to an FDIC external servicer. BIS SQL Administrators check quarterly with BIS Management to assure no more work is required and then they backup and archive the data to a location where only the BIS administrators have access.

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. Bank data is accessed via SQL applications such as Microsoft Management Studio or Advanced Query Tool. Bank data is viewed for balancing by account numbers and accounting categories, not by individual names or identifiers.

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? Bank data is viewed for balancing by account numbers and accounting categories, not by individual names or identifiers. Reports derived from bank data are copied to the bank's SharePoint site. Individual SharePoint sites and BIS SQL bank databases are deleted 10 years after the bank/receivership enters Termination Status.

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 records in this system are retained by the FDIC for ten years after termination of the bank/receivership or as established by state or Federal law or court order, if longer, in accordance with FDIC's records and disposition schedule A BIS staff members access the SharePoint Site and the BIS SQL Database and manually deletes them once notified by the appropriate DRR staff member.

In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name. This server operates under the "30-64-0013 Insured Bank Liquidation Records."

6.4 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain. This server is not being modified.

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?** The BIS SQL Server is not used to make privacy determinations or derive new data.

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 server is not using 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.** The only monitoring currently enabled is logging of user connections date and times on the SQL Server logs. Only DIT Server Administrators and DIT SQL Server Administrators can modify logging settings.

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 reputation to the Corporation could potentially be affected as the BIS SQL Server contains open and closed bank data that includes the bank's customer's personal information such as SSN, full name, home address, bank account information, and other information as noted above in section 3.

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.