FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)

for

Division of Resolutions and Receiverships (DRR)

Warranties and Representations Accounts Processing System (WRAPS)

FDIC PRIVACY PROGRAM

Redress • Notice • Awareness • Choice • Consent • Access • Participation • Integrity • Security • Enforcement

Date Approved by Chief Privacy Officer (CPO)/Designee

8/4/2016

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.

WRAPS is used by DRR to process and maintain data on claims made by asset purchasers under the terms of loan sales agreements.

The primary input to WRAPS is Asset Sale information, claim information, and payment information. Asset Sale data is received from DRR Asset Sales. Claims information is received in hard copy from a claimant. Payment information is exchanged with NFE accounts payable.

[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 output of WRAPS includes Asset Repurchase data provided to 4C, Payment data exchanged with NFE accounts payable, and various reports.

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.

WRAPS was not designed to carry specific fields containing personal identification information on borrowers. The comments field in WRAPS may contain this information. Generally, this is limited to the borrower's name and address.

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

The name and address identifiers in WRAPS are used to maintain a level of accuracy in researching and processing claims for the correct customers. These data support data located on 4C and assure that system is updated subsequent to a claim being settled and an asset reacquired.

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

WRAPS is designed to support the DRR Claims Office's processing and tracking of claims made by asset purchasers under the terms of loan sales agreements. The data in this system is derived from those claims and from loan sales agreements. Additional data may be acquired from other sources, such as accounting and payment data from NFE and legal opinions regarding claims and payment from FACTS. WRAPS receives data from the following sources:

Table 3.3.1 – FDIC Systems/Applications That Provide Data to WRAPS

System/ Application Name	FDIC Division Sponsor	Description of Data Imported	Is PII Included?
New Financial Environment (NFE)	DRR	In the latest version of WRAPS that interfaces with NFE, users in WRAPS can create vendor and payment (invoice) records which are submitted to NFE by nightly batch jobs for processing. The data received by NFE is first validated and then loaded into proper modules for processing. Once the vendor and invoice records are processed in NFE, the updated information is retrieved by WRAPS nightly batch jobs.	No
FDIC Automated Corporate Tracking System (FACTS)	DRR	FACTS reference number is manually input into the field in WRAPS, with a hyperlink to the FACTS application. Information associated with the FACTS reference number is displayed to the authorized FACTS user. FACTS data is viewable only and is not transferred to WRAPS. Viewable data may include legal opinions regarding claims and payment.	Yes

Table 3.3.2 – FDIC Manual Entry and Other Sources That Provide Data to WRAPS

Data Source	FDIC Division Sponsor	Description of Data Imported	Is PII Included?
Manual Entry	DRR	Authorized FDIC/DRR personnel manually enter or update information into editable data fields in WRAPS.	Yes

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? Explain.

No Federal, state or local agencies provide scheduled data for use in the 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.

FDIC DOF provides payment data from NFE to update WRAPS. These updates reflect the amount and date of payment of claims. The 4C Asset ID is used in WRAPS to support users' ability to locate assets on 4C if needed.

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: As WRAPS was not designed to specifically carry personal identification; it is not possible to opt-out. The comments field in WRAPS may, from time to time, contain personal identifiers on borrowers including customer name and full address. The name and address identifiers in WRAPS are used to maintain a level of accuracy in researching and processing claims for the correct customers.

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. Users of the system include: authorized FDIC DRR staff, supervisory personnel, management officials, system administrators and other employees of the Corporation who have a need-to-know of the information contained in this system to carry out their duties. In certain instances, contractors performing work on the Corporation's behalf may have access to records in the system. Developers have access to the data in the non-Production environments. They use this data to test application corrections and changes. Developers have access to the data in the Production environment through the use of an on-call ID. Access to this ID is tracked and reviewed and its use is justified each time it is activated. This access is used to research and resolve production processing problems. All contracted users must sign a Contractor Confidentiality Agreement.

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 by a user (i.e.; FDIC employee or contractor who is responsible to update WRAPS data or respond to inquiries regarding the data) is determined by the "need-to-know" requirements of the Privacy Act. The user's profile is based on their job requirements and managerial position. The FDIC's Computer Access procedures (Form 1370/02), as well as the individual Application Access Control Procedures that are implemented and enforced by the Information Security Administrator, comply with the intent of the Computer Security Act of 1987 (Public Law 100-235) for standards and guidelines on security and privacy.

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. Data in WRAPS is exported or provided to the following FDIC systems/applications (specified in Table 4.3.1).

Table 4.3.1 – FDIC Systems/Applications that Receive WRAPS Data

Application Name & Acronym	FDIC Division Sponsor	Description of Data Exported	PII Included in Data?
New Financial Environment (NFE)	DRR	In the latest version of WRAPS that interfaces with NFE, users in WRAPS can create vendor and payment (invoice) records which are submitted to NFE by nightly batch jobs for processing. The data received by NFE is first validated and then loaded into proper modules for processing. Once the vendor and invoice records are processed in NFE, the updated information is retrieved by WRAPS nightly batch jobs.	No

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.**

Not applicable.

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.**

Although all employees who have access to information in a Privacy Act System of Record bear some responsibility for protecting personal information covered by Privacy Act, the information owner and system manager share overall responsibility for protecting the privacy rights of individuals by developing data access guidelines and standards which must be followed.

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?**

Contracted developers have the primary responsibility for design, enhancement and maintenance of the WRAPS system. All individuals that have access to the application complete a Contractor Confidentiality Agreement and Non-Disclosure Agreement on an annual basis.

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 is verified by users while providing support to customers. The FDIC has controls in place to ensure that any data input to WRAPS is free from viruses and the software controls ensure that the data complies with processing requirements before it is introduced to WRAPS. Data entry screens include edit checks to ensure that business rules and data relationships are maintained. Data validation has been incorporated within the application (front-end) and the database (back-end) to ensure data is entered in the required format. There are validations at the data field level (e.g. monetary fields must be numeric).

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

In accordance with OMB Circulars A-123 and A-130, WRAPS has controls in place to prevent the misuse of the data by having access to the data. Such security measures and controls consist of passwords, user identification, user profiles and software controls. All users, including contractors, must meet the requirements for securing Privacy Act protected information. See FDIC Privacy Act regulations. Users that are approved for access to WRAPS are deemed to have the authorization to access and review any data maintained. The controls are applied during the process of approving a user for access. In addition, if an authorized user does not utilize their access on a regular basis, the login is inactivated and no access is available. Users who are inactivated must reapply for 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.

Data in WRAPS can be retrieved by search, using a variety of fields. SSN is not included in WRAPS. It cannot be retrieved by a personal identifier.

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?

WRAPS cannot be used to create reports 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.

The retention periods of data/records are covered by FDIC Records Schedules. The Corporation also follows guidance on permanent and temporary records disposition issued by the National Archives and Records Administrations (NARA).

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

WRAPS is affiliated with 30-64-0013, Insured Bank Liquidation Records SOR.

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

Changes to the application may affect functionality but will not impact the overall business processes that the system supports so the Privacy Act system of records notice will 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 data in WRAPS is not being consolidated.

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, the system is not using technologies in ways that the Corporation has not previously employed, so there is no effect on privacy.

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. Monitoring is not being performed. The system is only accessible by those individuals who have been authorized to access the system.

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 of the corporation would not be materially affected by disclosure, intentional or unintentional, of data contained within WRAPS.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain. No.

No changes to business processes or technology are required.