FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment
for
The Resolution Process

January 22, 2022

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website[1], which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships. FDIC handles the resolution of failing FDIC-insured financial institutions and provides prompt, responsive, and efficient administration (including asset sales initiatives) to maintain confidence and stability in our financial system, to minimize losses, and to ensure continuity of financial services for financial institution customers. FDIC sells failed financial institutions in whole or in part to other financial institutions. It also sells individual or pools of assets (loan portfolios, real estate, furniture, fixtures, and equipment, etc.) from failed financial institutions to investors or other purchasers.

Prior to closing an institution, FDIC Franchise Marketing staff begins to market the failing institution and some or all of the assets for sale to prospective acquiring institutions (AI). Once an institution fails and FDIC is named as the Receiver, FDIC's Asset Marketing personnel work to sell any remaining assets for the highest value as soon as possible after the closing. Meanwhile, Asset Management assumes responsibility for managing and servicing the loans and other assets received from failed financial institutions until sold or otherwise disposed. To assist with its servicing responsibilities, the FDIC has established contracts with third-party Servicing Companies ("Servicers"). As required by FDIC, Servicers safeguard assets while providing services, such as general loan administration, debt restructuring, billing, collection, and accounting services appropriate to the type of asset being serviced.

This PIA serves to provide public notice regarding the processes and collections utilized as part of FDIC's financial institution resolution responsibilities, including the systems that support those responsibilities. The resolution process includes:

1. Determining a financial institution's insurance status;
2. Monitoring and tracking the status of failing/failed institutions;
3. Managing data flow and ensuring complete capture of all pertinent information from the institution into FDIC systems as well as information from FDIC to applicable third parties;
4. Analyzing and evaluating financial information and assets under control of a failing/failed institution;
5. Tracking personal and transactional information about financial institution customers and borrowers, staff, marketers, bidders, and other third parties where appropriate;
6. Marketing and facilitating the bidding, sales, transfers, and transactions pertaining to assets to other vendors and institutions;
7. Tracking and completing sales agreements, payment transactions in conjunction with asset sales;
8. Maintaining court-related information (defendants, liens, taxes, insurance, etc.);
9. Identifying and separating Loan Securities and Real Estate information; and
10. Tracking environmental reports.

[1] www.fdic.gov/privacy

The FDIC receives most of the PII maintained as part of the resolution process directly from failed or failing institutions. This information, called Customer Information Files (CIF), can contain customer and staff full name, date of birth and death, email address, home address, phone number, social security number (SSN), Taxpayer Identification Number (TIN), financial information (e.g. values and balances of loans or debit accounts, asset purchaser name and address, account numbers), employment information, and claimant identification number. However, PII can be collected by other means, such as:

- system-system interfaces,
- web portal submissions,
- manual input (e.g. FDIC Accounting staff), and
- external partners (e.g. Servicers, other Government agencies).

The following systems, applications, and tools support the resolution process:

- Communication, Capability, Challenge, and Control (4C) — 4C provides the FDIC with an integrated, end-to-end web-based application that supports key Franchise Marketing, Asset Marketing, and Asset Management activities described above. Specifically, the system houses all asset data received from failing and failed financial institutions beginning with pre-close activities, through asset disposition or ongoing management, as applicable. It manages data flow and updates from financial institutions, application service providers (ASPs). 4C maintains data and transactions for centralized historical analysis that can be accessed through the data warehouse. 4C stores information for all asset types, even those that are not included in the system-to-system downloads or processed on a loan system.

- Resolution Information Tracking Application (RITA) — RITA is a an end-to-end solution that supports FDIC's resolution mission responsibilities by streamlining and automating failing financial institution pre-resolution project initiation, consolidating customer relationship management functions related to interactions with financial institutions and asset buyers, centralizing and expanding resolution risk tracking and stakeholder outreach efforts, optimizing workflow for the failing financial institution marketing process, expediting exchanges of information, applications and approvals, automating the bid submission experience with an external facing portal, accessible via FDICConnect,[2] aggregating and sharing bid composition and liquidation and bid costs, and deploying workflow approvals for potential winning bids. RITA also utilizes an electronic signature platform by sending the bid submission to the platform for signature by the bidder. Once the bidder signs, RITA will retrieve the signed bid submission from the electronic signature platform.

- Virtual Data Rooms (VDR) — VDRs are an outsourced secure web site facility and technology used by FDIC to create workspaces for failing or failed institution projects, where confidential documents and information can be rapidly exchanged with specific groups of authorized internal and external users. FDIC uses VDRs as platforms for managing/transferring files and communicating with external entities (e.g., bidders, regulators, AIs, and contractors) involved in the resolution and receivership process.

    - Specifically, prior to a financial institution closing, Franchise Marketing staff use the VDRs to:
        - Announce the marketing of a potentially failing institution to qualified potential bidders (generally financial institutions or their designated authorized representatives). These eligible financial institutions can review certain documents about the potentially failing institution, including financial information, legal documents, etc.;
        - Communicate with regulators and exchange reports for approving potential bidders and reviewing bidder activity;
        - Provide data to third party loan valuation contractors who are responsible for reviewing and valuing pools of loans and individual assets in support of the sale of an institution;
        - Maintain and manage data on potential bidders, or their designees, who have been invited to view marketing information for a specific project; and
        - Provide potential bidders access to electronic images of complete loan and other files for due diligence.

[2] https://www.fdicconnect.gov/index.asp

- After a financial institution has closed, Asset Marketing staff generally use the VDR to:
  - Conduct Structured Sales transactions;
  - Provide asset data to third party Financial Advisors; and
  - Provide documents to potential corporate bidders for inspection and due diligence.

- Also after a financial institution has closed, staff use a separate workspace on their VDR to:
  - Obtain monthly and quarterly "certificates for payment" reports from AIs that purchase failed financial institution assets and are seeking reimbursement under FDIC's loss-share program;
  - Share data with FDIC contractors responsible for reviewing AI compliance with program reporting requirements and aggregating data for the loss-share program;
  - Perform settlement documentation exchange with AI;
  - Transfer owned real estate and other owned asset documentation from the institution or affiliates into FDIC; and
  - Exchange institution financial data with outside receivership tax return preparers to create and finalize tax returns.

- FDIC uses VDRs for other limited purposes as a means to securely exchange documentation with authorized parties.

- Asset Servicing Provider (ASP) — FDIC generally uses contractors and loan servicers to help manage many of the assets until they can be sold or otherwise resolved. Under certain circumstances, loans may need to be managed in-house by FDIC Staff, rather than being transferred to external loan servicers for management. To manage assets internally, FDIC contracts the use of an asset servicing application (ASA). Each ASP provides FDIC interrelated subsystems and reporting tools that FDIC uses to track, manage and apply adjustments, payments and proceeds for assets.

- Mortgage Electronic Registration System (MERS)[3] — MERS is an electronic registry designed to track servicing rights and ownership of mortgage loans in the United States. MERS streamlines the mortgage process by eliminating the need to prepare and record paper assignments when trading residential and commercial mortgage loans. MERS serves as the mortgagee of record for lenders, investors and their loan servicers in the county land records. The mortgage or deed of trust is held in the name of MERS as nominee for the beneficial owner and is recorded in the applicable county land records. The mortgage information is entered into MERS at the time of origination. Data in MERS is then updated when the loans are transferred and sold by the originator, eliminating the cost and expense of filing significant amounts of paper document transactions. As Receiver, the FDIC is charged with disposing of the failed financial institution's assets and liabilities in an efficient and expedient manner, including the sale and transfer of MERS registered mortgages and related servicing. As such, FDIC employees and contractors, as well as failed financial institution employees retained by the FDIC, must be able to access, review, and update the data in MERS.

- Owned Real Estate (ORE) Tracker – ORETracker is a web-based application used by FDIC to support the tracking, management, marketing and reporting of assets owned by the FDIC. The system houses both external vendor and FDIC in-house data assets.

- Post-Closing Automation and Monitoring (PCAM) — PCAM is used to assign FDIC employees and Contractor personnel to manage loans that will be inventoried when a failed institution goes into receivership. The system monitors and tracks these loans until the inventory process is complete. Most of the unsold assets retained by the FDIC after a financial institution failure are loans. The FDIC assumes responsibility for servicing these loans, including collecting payments, managing escrow accounts, monitoring delinquencies, managing defaulted loans, approving loan or line of credit disbursements, and meeting statutory and regulatory requirements that set standards for loan servicing tasks. Retained loan assets are managed and serviced on-site at the failed institution's facilities until they are transferred to a national loan servicer. PCAM established an automated, centralized and consistent business process and provides tools for internal and external stakeholders

[3] https://www.mersinc.org/products-services/mers-esuite/eregistry

executing and monitoring associated tasks. The system allows stakeholders to enter, track, monitor, and update loan servicing status, requests, communications, tasks, approvals, and deliverables, compile and submit required reports, and visually track, analyze, and display progress toward goals or key performance indicators (KPIs) and metrics.

- Resolution Transaction Submission Portal (RTSP) — RTSP is an out-sourced contractor system used for data collations, aggregation, storage and data management and reporting services for Loss Share, LLC/Joint Venture (JV) Securitizations transaction and other related programs at the FDIC's instructions. Loss Share is a feature that FDIC first introduced into selected Purchase and Assumption (P&A) transactions. These P&A agreements are contractual agreements between the FDIC and an AI where assets are covered under a loss share, the FDIC absorbs a portion of the loss on a specified pool of assets which maximizes asset recoveries and minimizes FDIC losses. Loss Share also reduces the FDIC's immediate cash needs, is operationally simpler, is easier for failed financial institution customers, and moves assets quickly into the private sector. Depending on the AI agreement, Loss Share submissions are uploaded to RTSP on a monthly or quarterly basis. Included within these Loss Share submissions is account information on single-family financial and commercial portfolios.

- Receivership Assets Data Repository (RADR) — RADR is a datamart used to store Receivership data sent to the FDIC from third-party vendors that process and report on asset transactions. The Receivership data that is stored in this database is aggregate Loss Share submissions from AIs of failed financial institutions. On a recurring basis, Loss Share submissions are uploaded to RTSP and then to RADR. Included within these Loss Share submissions is information on single-family financial portfolios.

- The Warranties Representation Accounts Processing System (WRAPS) — WRAPS supports FDIC in monitoring contractual obligations between sellers and purchasers of receivership loans and related assets. These obligations are based on the Representation and Warranties (R&W) offered to the purchaser as documented in the Sales Agreement. Upon receipt of the claim, a Sales Agreement record is created in WRAPS and used to track the progress of a claim through its review lifecycle. If the review process results in FDIC having a financial liability, then a payment will be generated for the claimant. A claimant is the purchaser of a loan pool, and is typically a financial institution, but on rare occasions a claimant may be an individual attorney representing the financial institution.

- Closed Loan Sales and Closed Real Estate (CSCRE) — CSCRE is web-based application that FDIC uses to publish information on the internet relating to the sale of loans[4] and real estate[5] by the FDIC. This information is used by the FDIC and the public to perform trend analysis. Additionally, the application serves to provide access to the public without requiring the submission of a formal Freedom of Information Act (FOIA) request.

- Proforma – At institution failure, FDIC reconciles the general ledger of the institution and converts the information to the FDIC's standardized accounting system. Additional capabilities include recording necessary adjustments to the general ledger, reconciling differences, adding narrative, and generating reports and statements which when final document the inception balance entries for the Receivership, and the initial balances for any acquiring institution (AI).

- Bank Collaboration Sites – FDIC uses internal collaborations sites data repositories for pre- and post-failure financial institution documentation not otherwise stored by FDIC. This may include financial, asset, liability, and supporting data, plus loan, insurance, employee, or similar data for any FDIC purpose obtained from the institution, its affiliates, vendors, or customers.

- Valuation – FDIC obtains appraisals and other valuation products and services for both residential and commercial real estate based on state and federal guidelines and laws that apply to the banking industry to ensure the value estimates used by FDIC are a reasonable reflection of market value.

[4] https://sales.fdic.gov/closedsales/

[5] https://sales.fdic.gov/closedrealestate/

Unclaimed Property System – Property that has been abandoned lost or inactive is referred to as unclaimed properties, which are assets such as cash, stocks, and bonds. FDIC's Unclaimed Property Group (UPG) is responsible for recovering unclaimed property belonging to the FDIC that has been turned over to the state by multiple entities such as title companies, financial institutions, insurance companies, municipalities, stock, and brokerage institutions. It can also include property held by bankruptcy courts or various government entities. UPS is a system used to track claims and recoveries of unclaimed property being held by others and belonging to FDIC. The type of data that is stored in UPS includes failed financial institution information consisting of information listed on a state's publicly available unclaimed property website, the state's application login IDs and passwords to access the state's unclaimed property website, and the names of joint owners of assets and bankruptcy filers in certain cases. FDIC personnel's name may be also listed in reports run in UPS to represent the individual that has been assigned the claim.

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency
- Access and Amendment
- Data Minimization
- Data Quality and Integrity
- Individual Participation

Transparency
Privacy Risk: Although FDIC makes System of Record Notices and PIAs publicly available on the FDIC.gov website, impacted customers and borrowers may not realize their data is being provided to FDIC in conjunction with the failure of their financial institution.

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure. Insured financial institutions display the FDIC logo at their physical locations and on their websites. In addition, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. For example, loan servicers are required by law to provide borrowers with a notice of transfer for any mortgage loan that includes the date of transfer and contact information for both the transferor and transferee.[6]

Access and Amendment
Privacy Risk: The systems involved in the resolution process do not have procedures or provide notification to individuals about how to access or amend their information when PII is collected/obtained from the institution or other third parties.

Mitigation: Financial institutions provide FDIC with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for access to their personal information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Data Minimization

[6] 12. C.F.R. § 1024.33

Privacy Risk: A number of FDIC systems supporting the resolution process do not yet have established records retention schedules. Additionally, some systems receive batch files and may receive more than the minimum elements necessary.

Mitigation: FDIC takes steps to ensure that duplicate data sets are overwritten and that the records retention schedules are followed. FDIC RIMU is currently engaged in a large effort to establish formal retention schedules for all systems. Also, FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

Data Quality and Integrity
Privacy Risk: The FDIC collects information from failed and failing financial institutions and cannot attest directly to the data quality of the information received. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and the failed or failing financial institutions.

Mitigation: To the extent possible, the FDIC uses system-to-system transfers to reduce the inadvertent alteration of data. For data that is manually uploaded by FDIC employees, there are a number of validation points and safeguards to avoid the alteration of data uploaded from the failed financial institutions. See Section 7.1 for more information. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate. See Section 3.0 for more information.

Individual Participation
Privacy Risk: Since most data in the system is not collected directly from individuals, there is a risk that these individuals will not know how their data is being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: In cases where FDIC does collect PII directly from individuals, Privacy Act Statements are provided where appropriate. Additionally, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Section 1.0: Information System

1.1 What information about individuals, including personally identifiable information (PII) (e.g., name, Social Security number, date of birth, address, etc.) and non-PII, will be collected, used or maintained in the information system or project?

While there are a number of systems covered under this PIA, there are a handful of key systems where all PII is collected and stored, detailed below:

System	Information Summary
4C	• Full Name of the financial institution customer (including primary account holder and trustees or beneficiaries). • Social Security Number (SSN) and Tax Identification Number (TIN) • Home Address. • Non-work Phone Numbers. • Financial Information (e.g., checking and savings account numbers and balances, loan balances, loan number). • Criminal History Information. • Court Record/Restitution Information.

System	Information Summary	
RITA	• Full Name • Phone Number • Email address • Legal documents, records, or notes (as related to the bid submission)	
VDR	*Customer/Failed Institution* • Full name • Address • Phone Number • Date of Birth • SSN (after closing) • Driver's License (after closing) • Tax Returns (after closing) • Previous credit reports (after closing) • Loan account number and balance, interest rate, term • Other relevant customer account information (e.g., name of co-borrower; name of guarantor) • Loan to value data • Property description • Borrower net worth • Criminal Information (Restitution)	*Potential Bidder/Regulator/Acquiring Institution* • Organization name • Full name of point of contact • Work phone number • Work email • Size of bidding organization/ total assets • Holding company name and other qualifying information (e.g., supervisory rating)
ORETracker	• Account Manager full name • Contractor Asset Manager full name • Listing Agent full name • FDIC Legal Counsel full name • Protested By full name • Purchaser full name • Environmental Specialist full name • Inspector full name • Consolidated address of asset name (ORE property address to be sold).	
PCAM	• Full Name • SSN • Home Address • Phone Number • Email Address • Financial Information	
RTSP	• Full Name • SSN • Home Address • Email Address • Financial Information • Asset Names • Vehicle Identifiers • Legal Documents • Investigative Report/Database	
RADR	• Full Name • SSN or TIN • Home Address • Phone Number • Email Address • Financial Information	
WRAPS	• Full Name • Home Address • Financial Information	
CSCRE	*Loan Sales*	*Real Estate Sales*

System	Information Summary	
	• Purchaser Name • Purchaser Address • Date of Sale • Property Type • Purchase Price	• Property Name (typically property address) • Property Type • Purchase Price • Date of Sale
ASPs	• Full Name • SSN or TIN • Home Address • Phone Number • Financial Information • Criminal Information • Property Name • Property Type • Purchase Price • Date of Purchase/Sale • Purchaser Name • Purchaser Addresses	

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s)	☒	☐
Email Address	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☒	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☐	☒
Criminal Information	☒	☐
Military Status and/or Records	☐	☒
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: See table above in 1.1)	☒	☐

1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Failing/Failed Financial Institutions	Using secure methodologies, the FDIC obtains the Customer Information Files and Depositor Information Files from the failing or failed institution. FDIC then extracts/prepares the required asset and transaction data elements for upload to the appropriate system. FDIC is responsible for ensuring the completeness of the downloaded/uploaded data.

4C	Provides information on bidders, institutions, and asset transactional data to other FDIC systems. Additionally, non-PII information such as financial institution names, asset amounts, holding companies and compliance rating details are provided from 4C to other FDIC systems.
PCAM	Retained loan asset information (including customer demographic information), financial details, and collateral information are shared with National Loan Servicers as well as Loan Purchasers via VDRs.
Manual Input by FDIC	When applicable resolution, marketing, and transaction information is collected and processed, FDIC staff captures some elements manually.
New Financial Environment (NFE) General Ledger, Accounts Payable, and Receivership Asset Accounting	FDIC has an automatic reconciliation with NFE, which imports non-PII, aggregate data such as Real Estate budget information, Also, FDIC automatically imports Chartfield data (i.e. accounting data that does not contain PII) and daily and monthly account balances from GL for account valuation and analysis purposes.
Failed financial institutions/Deposit Insurance National Bank (DINB)	In some instances, when a financial institution fails, the FDIC charters a new national financial institution, referred to as a Deposit Insurance National Bank (DINB), which assumes only the insured deposit liabilities of the failed financial institution, and no other assets. The DINB then proceeds in an orderly fashion to self-liquidate, by paying off depositors. In a DINB scenario, payouts occur over a 30 to 60-day time period, instead of during the closing weekend. DINB data, consisting of insured deposit data, which includes Name, SSN, Account Number, and Account Balance, is automatically and securely fed from the failed financial institution/DINB. This data is necessary to ensure accurate payouts for insured deposits.
RTSP	The FDIC Risk Share Asset Management Staff uses RTSP for the purpose of managing the Loss Share Program. The application is used for data collations, aggregation, storage, and data management; and reporting services for Loss Share, LLC/JV Securitizations transaction, and other related programs at the FDIC's instructions. All data elements from this application are sent to FDIC to be formatted and placed in RADR for senior management (including the Chairman) to review the Loss Share Program information at one glance. The data received may include individual borrower name, SSN/TIN, home address, financial information, e-mail address and phone number.
Structured Information Management System (SIMS)	RITA retrieves financial institution CEO phone number and email from SIMS.
Virtual Supervisory Information on the Net (ViSION)	4C and RITA receive and store the institution's primary contact information (Name, Position, Phone, and Email Address) from ViSION. RITA also receives Case Manager contact information, Case Assistant Regional Director, and Case Supervisor names from ViSION.
Corporate Business Information System (CBIS)	RITA receives and stores financial institution president contact information and information associated with accounts from CBIS.
Enterprise Data Warehouse (EDW) Person Master Database	FDIC employee and contractor staff information including full name, user name, FDIC work phone and FDIC work email.
ASPs	Some asset data in ASPs may be obtained from FDIC-contracted interim servicers or external asset servicers. These sources also use the 4C conversion process since 4C controls the assigned Servicer, including the internal servicer. Specifically, as the Asset Management team identifies a change in Servicer, the change is scheduled and recorded in 4C. BIS staff works directly with the existing servicer or interim servicers to convert asset data to the new ASP.
FDIC Third-Party Contractors	FDIC Contractors produce deliverables that may be exchanged using VDRs.
Potential Bidders	Bidders provide FDIC information about their organization and bid submission documentation as well as other requisite information prior to the bid.
State Unclaimed Property Websites and	UPS processes information related to unclaimed property retrieved from state unclaimed property websites and US Bankruptcy Court websites to recover unclaimed property belonging to the FDIC.

US Bankruptcy Court Websites	

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

All FDIC information systems must achieve an Authority to Operate (ATO) via the Assessment and Authorization process that aligns with the Risk Management Framework. Information systems that process resolution information have been granted ATO or are in the process to achieve ATO. The ATO for each FDIC system is periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

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

The following SORNs apply to the Resolution Process PIA:

- FDIC Privacy Act SORN-013 Insured Financial Institution Liquidation Records;
- FDIC Privacy Act SORN-019, Potential Bidders List; and
- FDIC Privacy Act SORN-024, Unclaimed Deposit Account Records

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

No, the SORNs listed in Question 2.2 do not require amendment or revision. Generally, the FDIC conducts a review of its SORNs every three years or as needed.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

Information collected from third parties: FDIC systems store and process data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Given that the FDIC is not the initial collector of the PII, a Privacy Act Statement is not required to explain the purpose for collection and the intended uses of the information.

Information collected by FDIC: When information is collected directly from the individual, FDIC provides the individual with a Privacy Act Statement prior to the collection of his or her personal information.

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1, 'FDIC Forms Management Program.'

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, the Privacy Act System of Records Clearance Officer, and the Privacy Program (Privacy@fdic.gov). See https://www.fdic.gov/about/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Although FDIC makes System of Record Notices and PIAs publicly available on the FDIC.gov website, impacted customers and borrowers may not realize their data is being provided to FDIC in conjunction with the failure of their financial institution.

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure. Insured financial institutions display the FDIC logo at their physical locations and on their websites. In addition, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. For example, loan servicers are required by law to provide borrowers with a notice of transfer for any mortgage loan that includes the date of transfer and contact information for both the transferor and transferee.[7]

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

Information collected via third parties: The systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. This snapshot is an instance of what is on file with the institution(s) at that time. No changes are allowed after the financial institution has closed. The information is not directly collected from individuals. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. PII obtained from financial institution records is necessary to ensure FDIC issues accurate transfers of assets, markets loans and real estate appropriately, and properly handles payment processing. The FDIC does not have the ability to implement procedures for individual access in these cases. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for access to their personal information.

Information collected by FDIC:

Shortly after the failure of an institution, FDIC will utilize marketing staff to work with other third parties (e.g. Loan Servicers, Potential bidders) to in an attempt to sell or transfer assets obtained. PII is collected in multiple FDIC systems pertaining to third parties as a part of the marketing process.

[7] 12. C.F.R. § 1024.33

In cases where FDIC has collected PII directly, access procedures are detailed in the SORNs listed in Question 2.2 of this PIA. . The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 12 C.F.R. § 310.3 and 310.4. FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

3.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Information collected via third parties: Many of the systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. The FDIC does not have procedures to correct inaccurate or erroneous information in these cases. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for corrections to their personal information.

Information collected by FDIC:
In cases where FDIC has collected PII directly as described in Question 3.1, amendment procedures are detailed in the SORNs listed in Question 2.2 of this PIA. . The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 12 C.F.R. § 310.3 and 310.4. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

Information collected via third parties: Most systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. The FDIC does not have procedures to correct inaccurate or erroneous information in these cases. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for access to their personal information.

Information collected by FDIC:
In cases where FDIC has collected PII directly, notifications occur as described in Question 3.1. Additionally, notification procedures are detailed in the SORNs listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 12 C.F.R. § 310.3 and 310.4. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. Additionally, the FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users, the procedures for which are published in the SORNs listed in Section 2.2 of this PIA. This is in accordance with the Privacy Act and 12 C.F.R. § 310.3 and 310.4.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: The systems involved in the resolution process do not have procedures or provide notification to individuals about how to access or amend their information when PII is collected/obtained from the institution or other third parties.

Mitigation: Financial institutions provide FDIC with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does

not have the ability to provide privacy notices prior to the agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for access to their personal information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002, Section 522 of the 2005 Consolidated Appropriations Act, Federal Information Security Modernization Act of 2014, Office of Management and Budget (OMB) privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes personally identifiable information (PII); (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Privacy risks posed by the resolution process are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program"). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/about/privacy/index.html.

4.4 What roles, responsibilities and access will a contractor have with the design and maintenance of the information system or project?

Contractors are responsible for designing, developing, troubleshooting, applying corrections, and implementing enhancements to systems maintained by FDIC based on evolving business requirements and discovery of security vulnerabilities and system functionality defects. Contractor access is typically limited to the Development and Quality Assurance (QA) versions of most systems; however, if there is a need for contractor administrator-level support, some contractors may be granted access to the production versions and data contained within.

All individuals that have access to applications complete a Contractor Confidentiality Agreement and Non-Disclosure Agreement appropriately. All contractors must also pass a background check.

Due to the contractors' access to PII, contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Yes, Contractor Confidentiality Agreements have been completed by contractors who work on applications pertaining to the resolution process. Additionally, privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program is currently in the process of implementing a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

FDIC personnel and system users involved in the resolution process are required to take specific security and privacy awareness training. The user roles, responsibilities, and expected behavior with regard to information and information system usage are defined in accordance with NIST SP 800-53. Signed acknowledgments are obtained from users.

In addition, the FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; Information Security Manager's Monthly meetings.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls, if possible. Additionally, FDIC has implemented technologies to track, respond, remediate and report on breaches, as well as to track and manage PII inventories.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program." Disclosures are tracked and managed using the FDIC's FOIA solution.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program."

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program."

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with Accountability.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of personally identifiable information (PII) are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of SORNs. FDIC Circular 1360.20, "FDIC Privacy Program" mandates that the collection of

PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws:

- Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).
- 12 U.S.C. 1821: deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving financial institutions. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 U.S.C. 1822: deals with FDIC as a receiver of failed financial institutions.
- Executive Order 9397: pertaining to the requirement for the use of SSNs
- 12 CFR 330: clarifies the rules and defines the terms necessary to afford deposit insurance coverage under the Act and provides rules for the recognition of deposit ownership in various circumstances.
- 12 CFR 360.9: pertains to allowing large financial institutions to continue function on the day of closing to permit FDIC meeting legal mandates and perform required functions
- 12 CFR 366: deals with FDIC contractors

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority, as FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIA and the development and review of SORNs.

Mitigation: No mitigation actions are recommended.

Section 6.0: Data Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

Financial institution customer PII is obtained directly from the institution by FDIC, as part of an overall transfer of the depositor information files and customer information files to FDIC during the financial institution closing process. FDIC extracts the minimum data elements needed and prepares the data for use for FDIC Staff. FDIC resolution applications utilize data sharing wherever possible to ensure that the data exchanged maintains a high level of accuracy and only import required data elements wherever possible.

Additionally, through the conduct, evaluation, and review of privacy artifacts,[8] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

Financial institution customer PII is obtained directly from the institution by FDIC, as part of an overall transfer of the depositor information files and customer information files to FDIC during the financial institution closing process. FDIC extracts the minimum data elements needed and prepares the data

[8] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

for use for FDIC Staff. FDIC resolution applications utilize data sharing wherever possible to ensure that the data exchanged maintains a high level of accuracy and only import required data elements wherever possible. Additionally, systems are analyzed by FDIC Records and Information Management Unit (RIMU) to establish retention and disposition schedules to reduce privacy risk.

Additionally, through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that the FDIC has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of data in this information system or project? 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 with established schedules are retained in accordance with approved records retention schedules. Information related to the retention and disposition of data are captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Directives 1210.01, "Records and Information Management Program" and 1360.9, "Protecting Sensitive Information."

FDIC is in the process of developing formal retention schedules for all systems, and some systems involved in the resolution process do not yet have formal retention schedules. Records maintained in WRAPS are destroyed ten years after the termination for the receivership. In 4C, records related to institutions that do not fail are destroyed two years after the discontinuance of the case and records related to institutions that do fail are destroyed ten years after the termination of the receivership. Data related to corporate purchases in 4C is destroyed seven years after the final disposition of an asset. FDIC has determined that CSCRE does not require a retention schedule because it consists of a duplication of existing agency records.

6.5 What are the policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. The project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Privacy Risk Analysis: Related to Data Minimization

Privacy Risk: A number of FDIC systems supporting the resolution process do not yet have established records retention schedules. Additionally, some systems receive batch files and may receive more than the minimum elements necessary.

Mitigation: FDIC takes steps to ensure that duplicate data sets are overwritten and that the records retention schedules are followed. FDIC RIMU is currently engaged in a large effort to establish formal retention schedules for all systems. Also, FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond what is necessary.

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or utilize synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system. Additionally, the project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

The FDIC reviews privacy artifacts for adequate measures to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation. Most systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. The responsibility for quality, utility, and objectivity of that point-in-time snapshot of data belongs to the failed or failing financial institutions. FDIC systems involved in resolutions have processes and controls in place to ensure that data fields have appropriate formatting and required fields are completed. Where manual data entry is used, there is a second-level review process, data validation checks for certain fields to confirm formatting, and calculated fields to avoid manual entry error. These controls, as well as collecting information directly from the individual as the most reliable source of information, where practicable, help promote data quality, utility and objectivity.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

Information collected via third parties: Many systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. The FDIC does not have the ability to collect information from the individuals who the records pertain to directly in these cases. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for corrections to their personal information.

Information collected by FDIC:
In cases where FDIC collects PII directly, processes are in place to ensure that the individual directly provides PII wherever possible. Generally, DRR staff are directly in contact with the individual for these purposes.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

The FDIC reviews privacy artifacts to ensure adequate measures to check for and correct any inaccurate or outdated PII in its holdings.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of PII. The Office of the Chief Information Security Officer validates the configuration of administrative and technical controls for the system or project based on the FIPS 199 determination.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: The FDIC collects information from failed and failing financial institutions and cannot attest directly to the data quality of the information received. There is a risk that the information provided to the FDIC lacks sufficient data quality, and that there is a risk to data integrity in the transfer of the data between the FDIC and the failed or failing financial institutions.

Mitigation: To the extent possible, the FDIC uses system-to-system transfers to reduce the inadvertent alteration of data. For data that is manually uploaded by FDIC employees, there are a number of validation points and safeguards to avoid the alteration of data uploaded from the failed financial institutions. See Section 7.1 for more information. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate. See Section 3.0 for more information.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. FDIC only collects PII that it is legally authorized to collect. Additionally, this PIA and the SORNs listed in Section 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

Information collected via third parties: Most systems involved in the FDIC resolution process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the closing activities. The responsibility for providing authorizing the collection of PII and providing adequate consequence belongs to the third-party in these cases. Financial institutions are required by

law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their financial institution directly for questions pertaining to their personal information.

Information collected by FDIC: When the FDIC collects information directly from individuals, it describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

8.3 Explain how the information system or project obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. Refer to Section 8.1 for additional information. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORNs as well as the relevant PIA.

8.4 Explain how the information system or project ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

PII collected as part of the resolution process is only used for the purposes listed in Section 9.1. As described in Question 8.2, in cases where data is received from third parties, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals should review the relevant third party's privacy notices.

In cases where FDIC collects PII directly from the individual, FDIC uses Privacy Act Statements to detail all potential uses and sharing of PII. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, https://www.fdic.gov/about/privacy/index.html, instructs viewers to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Since most data in the system is not collected directly from individuals, there is a risk that these individuals will not know how their data is being used or shared, nor be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: In cases where FDIC does collect PII directly from individuals, Privacy Act Statements are provided where appropriate. Additionally, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

The FDIC Resolutions Standard Operating Procedures (SOP) detail how all PII is collected, used, and maintained as part of the FDIC resolution process, to perform the following functions:

1. Determining a financial institution's insurance status;
2. Monitoring and tracking the status of failing/failed institutions;
3. Managing data flow and ensuring complete capture of all pertinent information from the institution into FDIC systems, as well as, information from FDIC to applicable third parties;
4. Analyzing and evaluating financial information and assets under control of a failing/failed institution;
5. Tracking personal and transactional information about financial institution customers and borrowers, staff, marketers, bidders, and other third parties where appropriate;
6. Marketing and facilitating the bidding, sales, transfer, and transactions pertaining to assets to other vendors and institutions;
7. Tracking and completing sales agreements, payment transactions in conjunction with asset sales;
8. Maintaining court-related information (defendants, liens, taxes, insurance etc.);
9. Identifying and separating Loan, Securities and Real Estate information; and
10. Tracking environmental reports.

9.2 Describe how the information system or project uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

FDIC application Program Managers and Data Owners are responsible for the management and decision authority over a specific area of corporate data. Program Managers/Data Owners have overall responsibility for protecting the privacy rights of individuals by developing data access guidelines and standards which must be followed. Additionally, Program Managers/Data Owners and Information Security Managers serve as the source of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing.

Although the Program Managers/Data Owners and Information Security Managers share this data responsibility, it is every user's responsibility to abide by FDIC data protection rules that are outlined in the Division Security and Privacy Awareness Training and the Corporate Security and Privacy Awareness Training, which all employees 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.

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

All users that require access to applications involved in the resolution process must submit a request using the FDIC's Access Request and Certification System (ARCS) and have the approval of their Manager and the application Access Approver prior to being granted authority to use the system. Users are provided a role that limits their view of data only to the data needed to complete their job task. Per FDIC Circular 1360.15, user access levels are reviewed periodically to ensure they reflect current business needs.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☐ No
☒ Yes Explain.

Source	Destination
Customer Information File (CIF) and Depositor Information File (DIF) from Failing/Failed Financial Institutions/ Loan Detail File	-4C -VDR
4C	-FMS -TRAC -NFE/RAA -DRR Locating and Reporting System (DOLLARS) -Identity Management Solution -EDW -ASA -CSCRE -ORETracker
RITA	-EDW
Track and Route Authorization Cases (TRAC)	-4C -DOLLARS
SIMS	-RITA
ViSION	-RITA
RTSP	-RADR
EDW	-PCAM - RITA - EDW provides view in RITA from the following applications: • CBIS • SIMS • Regional Report Repository (R3) • ViSION • Large Insured Depository Institutions (LIDI) • System of Uniform Reporting of Compliance and CRA Examinations (SOURCE)
WRAPS	-NFE
VDR	-RITA

9.5 Will the information system or project aggregate or consolidate data in order to make 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, FDIC does not aggregate data to make programmatic level decisions.

9.6 Does the information system or project share personally identifiable information (PII) externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum

of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used. Please explain.

Source	Destination
4C	-National Information Services (Contract Vendor) -Acquiring Institutions -External Servicers -Owned Real Estate Management and Marketing Vendors (Contract Vendor)
VDR	-Bidders -Regulators -Acquiring Institutions - FDIC Contractors
State Unclaimed Property Websites	UPS
US Bankruptcy Court Websites	UPS

Information is shared externally pursuant to the routine uses described in the SORNs referenced in Section 2.2.

Additionally, through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act, FDIC Circular 1360.20, "The Federal Deposit Insurance Corporation (FDIC) Privacy Program" and FDIC Circular 1360.17, "Information Technology Security Guidance for FDIC Procurements/Third Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17, "Information Technology Security Guidance for FDIC Procurements/Third Party Products" and FDIC Circular 1360.9, "Protecting Sensitive Information."

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There are no identifiable risks associated with use limitation. Through role-based access, employee training and the review of privacy artifacts, FDIC ensures that PII is used only for authorized purposes.

Mitigation: No mitigation actions are recommended.

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the CISO on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system's or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks associated with Security.

Mitigation: No mitigation actions are recommended.