FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment

for

Insurance Determinations and Payouts

August 18, 2021

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

During the resolution planning and failure of an insured financial institution, FDIC obtains information about the institution and its assets, and reimburses individuals who have insured deposits with the institution, i.e., individual financial institution customers, brokers (acting as agents for other depositors), and non-depositors, i.e., creditors, businesses, and governments. There is a small window of time available to analyze and process claims from these depositors and creditors, and determine whether these individuals or entities are entitled to receive payouts from FDIC, acting in its receivership capacity. The FDIC Division of Resolutions and Receiverships (DRR) is responsible for managing the resolution of failed insured financial institutions. The scope of this PIA is the FDIC insurance determinations and payouts process and the systems that support it. The insurance determinations and payouts process includes:

1. Determining financial institution depositor's account(s) insurance status;
2. Making determinations and payments in accordance with insurance;
3. Evaluating and processing depositor and non-depositor/creditor claims;
4. Completing payouts and dividend distributions;
5. Compliance testing in accordance with regulation 12 CFR 360.9, Large-Bank Deposit Insurance Determination Modernization (LBDIDM) Rule;
6. Managing account balances, reporting, and reconciliation with the General Ledger;
7. Managing and processing income statements and other tax-related items;
8. Allowing depositors to query status and coverage of failed financial institutions;
9. Searching for unclaimed funds; and
10. Verifying and investigating claims against U.S. Treasury Office of Foreign Assets Controls (OFAC), Credit Bureaus, State Officials, and other investigatory databases prior to issuing payment.

Each of these processes use information technology (IT) that DRR is rationalizing in order to ensure the cost efficiency and effectiveness of these systems. The systems include:

- **Claims Administration System (CAS)**—CAS supports the loading of datasets containing depositor information from financial institutions as part of an overall transfer of depositor information files to FDIC during the financial institution closing process. Any checks that are cut for failed financial institution depositors are completed using the Dividend Processing System (DPS). It should be noted that on occasion, a financial institution may not fail immediately and could be monitored for some time in anticipation of failure, whether or not it actually fails. At some point, FDIC will stop monitoring financial institution if it does not pose a risk of failure. For monitored financial institutions, FDIC can receive multiple loads of data to be used for pre-failure depositor claims insurance determinations. In addition, Congress or the FDIC Chairman identifies high-visibility financial institution for monitoring. The data collected from high-visibility financial institutions' is retained in CAS for use in preparing for potential financial institution failures and reporting historical analysis to Congress and the FDIC Chairman.
    - **DRR Internet Publications: "Is My Account Fully Insured?"**—"Is My Account Fully Insured?"[2] is a public facing website that publishes the insurance status of accounts at failed

[1] www.fdic.gov/privacy

[2] "Is My Account Fully Insured?" is a public facing website available at closedbanks.fdic.gov/drrip/AFI/Search.

financial institutions. The website is designed to promote transparency with the public and provide notice to the depositors of failed institutions while reducing the customer service workload of DRR in the event of financial institution failures. The information that supports the "Am I Fully Insured?" function is extracted from CAS and maintained on the website for 30 days following a financial institution failure.

- **Non-Deposit Claims (NDC)—**During the financial institution closing process, DRR is responsible for processing insured and uninsured depositor claims, as well as other "non-deposit" claims. Non-deposit claims may come from a range of businesses, government agencies, or other entities. In some cases, non-deposit claims may include claims from individuals such as former financial institution officers and financial institution employees that potentially are entitled to payment from the FDIC Receivership for a service or other obligation incurred by the financial institution prior to its failure. Non-deposit claims fall into three claim categories: creditor, stockholder, and subordinated debt. Claims may be filed by the individual or entity, or by an agent on behalf of the claimant**.** NDC supports the collection of creditor claims data submitted to the FDIC acting as the receiver.

  Promptly after the failure of an institution, DRR performs a mailing to all non-deposit creditors on the financial institution's books. The notification package includes the following:

  - A Notice to Creditor to Present Proof of Claim letter ("Notice Letter") notifying them about the financial institution failure, the appointment of FDIC as receiver, and the requirement to file a creditor claim with the receivership by a certain date.
  - A Proof of Claim form (FDIC Form 7200/19) to assist the claimant with filing a claim. The form collects the name of person completing the form, the name of claimant, address, and phone number. The form is optional and not required.
  - Instructions for Completing the Proof of Claim form that contains a description of the claim form fields and supporting documentation related to goods purchased by, or services rendered to, the failed institution, or other types of claims. Documentation may include an invoice, spreadsheet, or other documents that supports the claim.
  - A Fund number, bar code number, and a Claimant ID number specifically assigned to the claimant to facilitate their log-in into the FDIC Claims Portal and the tracking and processing of their claim in the NDC system.

  At the same time, FDIC publishes a notice in the local newspaper(s) about the financial institution failure and opportunity for creditors to file a claim. Any "discovered" creditor claimants are directed to the main FDIC website (www.fdic.gov) or the DRR Claims Department to obtain further information on how to submit a claim. The website also includes an e-mail link to the DRR Claims Department NonDepClaimsDal@fdic.gov and a link to the FDIC Claims Portal to register and set up a claimant record in NDC. The link to register electronically asks for the claimant's email address to facilitate the electronic delivery of the Creditor Notice to the claimant's email and provides a Claimant ID, Fund number, and Barcode number.

  Creditor claimants may use one of the following methods to file a claim:
  - Utilize the FDIC Claims Portal by completing an electronic claim form and uploading their required supporting documentation.
  - Mail the form and supporting documentation to a specific office location identified by the FDIC as receiver.
  - Email the form and supporting documentation to NonDepClaimsDal@fdic.gov.

- **Dividend Processing System (DPS)**— The purpose of DPS is to calculate and issue the appropriate payments to proven claimants, as well as reconciling those payments with the FDIC's New Financial Environment (NFE) General Ledger. In accordance with federal law, DRR pays claims in the following order of priority (after the administrative expenses of the receiver are taken care of): depositors, general unsecured creditors, subordinated debt, and stockholders. DPS processes the following types of payments:

- Payout Checks: DPS is used to print "payout checks" for distribution to insured depositors either onsite during financial institution closings or by mail. "Payout checks" are distributed to insured depositors in instances when no acquiring institution is found.
- Receivership Certificate & Dividend Payments: DPS generates "Receivership Certificates" (RCs) and distributes several types of "dividend payments" for these RCs to uninsured depositors and non-deposit claimants whose claims have been approved by DRR Claims Department. RCs are issued when funds are not immediately available to pay claimants; RCs show that claimants are entitled to receive money from the receiver once cash becomes available. As assets of the failed financial institution are sold and cash is accumulated, a portion of the cash is used to pay claimants who hold RCs. This distribution of cash to qualified claimants who hold RCs is known as "dividend payments".
- Unratified Deposits: DPS is used to log and process "unratified (or unclaimed) deposit payments", which are insured deposit accounts that remain unclaimed 18 months after a financial institution closing and are returned to the FDIC by the acquiring institution, as appropriate. The DRR Claims Department receives a check for the deposits from the acquiring institution and verifies that the check amount matches the unratified total. DPS imports the claimant and claim data from the acquiring institution so that the funds can be sent to the appropriate state treasuries, as required by law and described under Escheated Funds below.
- Escheated Funds: DRR uses DPS to escheat (i.e. send) unclaimed deposits, both insured and uninsured, to the appropriate state treasury offices, and track the timing of these funds and when they should be returned to the FDIC. In some instances, deposit funds remain unclaimed by the owners. Following a financial institution closing, the FDIC or the acquiring institution's attempt to locate the owners of insured deposit accounts for 18 months, after which any remaining funds are escheated by FDIC to the state treasury offices as required by law. These "escheated" funds are held by the states as a custodian for the depositor for up to 10 years. Funds unclaimed after 10 years are returned to the FDIC.
- Federal & State Tax Payments: DPS is used to send tax payments to the appropriate federal and state tax offices when funds are withheld from wage dividends.
- Billings & Borrowings: DPS helps generate billings and borrowings payments to transfer funds owed to the FDIC from the receivership accounts.
- Provisional Hold Reconciliation: DPS identifies provisional holds placed on deposit accounts in the resolution of a financial institution to allow time for an insurance determination to be completed. DPS tracks balance updates and provisional holds that may have caused balances to change since closing in order to allocate insured and uninsured amounts per account based on updated bank balances. DPS tracks the repayment of any accounts that are determined to be over-insured. An automated reconciliation is performed to compare results of the insurance determinations to a post-closing deposit file to assure holds and uninsured debits can be placed on the institutions' deposit subsystem.
- Acquiring Institution Settlement Activity: DPS automates the corporate settlement with the Acquiring Institution by providing and receiving data for the Purchase Assumption Settlement System (PASS) to allow the Acquiring Institution to view and update settlement information sourced from DPS. DPS also exchanges settlement transaction, invoice, and ACH details in addition to supporting receivership settlement reconciliations reporting.

Additionally, DPS performs a number of other functions including creating over 50 journal entries; reconciling receivership accounts between DPS, the CAS, and the NFE General Ledger; and maintaining records for a number of receivership-related transactions.

DPS also has added investment and distribution processing capabilities that allow the system to: (a) allocate excess funds from receiverships for investment purposes; (b) maintain investment records as a separate receivership function; (c) print investment reports; and (d) distribute the principal and interest at investment maturity.

- **Dividends Unclaimed Fund (DIV_FUNDS)—**DIV_FUNDS is a publicly accessible web page[3] that allows the public to search for their unclaimed insured deposits or for dividend checks issued which were undeliverable or never cashed. Data within DIV_FUNDS is transmitted from DPS via a query from the DPS database and synchronized nightly. This data includes a

[3] DIV_FUNDS is available at https://closedbanks.fdic.gov/funds/.

reference number for each record, unclaimed dividend payment information (check number and date), unclaimed deposit information (depositor name and deposit amount), and receivership information (failed institution name, city, and state).

- **Provisional Hold System (PHS) and Associated Statistical Analysis System (SAS) Applications**—FDIC uses the PHS and SAS applications to verify and validate the data format and relationship of the Deposit, Hold, and Sweep files sent to the FDIC, and to validate the accuracy of provisional holds placed by the financial institution before and after it closes. To support this process, DRR requests standardized, formatted deposit files from the financial institution or its servicer. The financial institution or servicer is requested to transmit the files via their secured FTP file transfer tool or via SFTP. FDIC reviews the dataset to ensure compatibility with its systems. Occasionally, the financial institution may insist that files be provided via read-only encrypted USB drive or CD/DVD disk that are owned by the financial institution and remain at the financial institution site. When an institution fails, FDIC facilitates the transfer of the institution's deposits to an acquiring institution or pays insured depositors directly. Together with CAS and DPS, the FDIC uses PHS to ensure that the FDIC can fulfill its legal obligation to resolve failed insured institutions and provide liquidity to depositors in a timely matter, usually within 48 business hours.

- **Receivership Request Management Portal (RRMP)** – FDIC uses RRMP to track and manage requests, inquiries, and updates submitted by failed financial institution depositors, non-deposit claimants, and deposit brokers. Using RRMP, these external claimants are able to: view and edit personal or business information already collected by and stored in CAS, NDC, and DPS; choose payment method preferences for deposit insurance, non-deposit claims, and dividends; supply documentation; and communicate with DRR Claims Agents. Potential claimants will access the FDIC Claims Portal[4] and be required to perform identity verification using Login.gov.[5] Once the claimant's identity is confirmed using Login.gov, attributes linked to the identity are passed via RRMP to the appropriate FDIC systems to match the identity to the correct records in those systems. Once this connection is made, claimants will be able to view their records, and submit proposed changes to certain parts of their records as needed during the resolution process.

The FDIC receives most of the PII maintained as part of the insurance determinations and payouts process directly from failed or failing financial institutions. Data from open financial institutions, including data from large and complex financial institutions, is collected and evaluated for resolution planning and compliance testing. Data files can contain depositor 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, account numbers), employment information, and claimant identification number. However, PII can be collected by other means, such as:

- forms (e.g. FDIC Form 7200/19, Proof of Claim),
- system-system interfaces,
- web portal submissions (e.g. FDIC Claims Portal),
- mail,
- manual input (e.g. DRR Accounting personnel), and
- external partners (e.g. Department of Treasury, State and Federal Tax authority).

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:

[4] https://resolutions.fdic.gov/claimsportal/s/.
[5] For additional information about the privacy implications of the General Services Administration's (GSA) Login.gov service, please see https://www.gsa.gov/cdnstatic/20200911_-_logingov_PIA_signeddocx.pdf.

- Transparency
- Data Minimization
- Data Quality and Integrity

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

Mitigation: When a financial institution is insured by the FDIC, it must display the FDIC logo at their physical locations and on their websites. This public association between the insured financial institution and the FDIC provides public transparency that there is an established relationship between the FDIC and the insured financial institution. Moreover, financial institutions are legally obligated to provide notice to individuals regarding the FDIC role as regulator and insurer of deposits. The access that the FDIC obtains to data from an insured financial institution is authorized and necessary under the Federal Deposit Insurance (FDI) Act to identify failing financial institutions and to resolve failed financial institutions.

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

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure and information relating to the opportunity for creditors to file a claim. If there are any "discovered" creditor claimants, they are directed to the main FDIC web site (www.fdic.gov) to obtain further information, such as the Proof of Claim form and then directed to the FDIC Claims Portal web site to register and set up a claimant record in NDC.

Privacy Risk: Depositors and creditors may not know that their information will be searched against the U.S. Treasury Office of Foreign Assets Controls (OFAC) Special Designated Nationals (SDN) List in order for FDIC to ensure that it does not disburse insured deposits or debts owed to individuals, entities or countries targeted by OFAC-administered sanctions programs.

Mitigation: The FDIC has published this PIA to provide transparency to the public regarding how their information may be processed as part of the insurance determinations and payouts process. The FDIC must comply with the requirements of 31 CFR 501.603, 604, 606, which define the reports required regarding economic sanctions programs, to ensure that the FDIC does not disburse insured deposits or debts owed to individuals, entities or countries targeted by OFAC-administered sanctions programs. The U.S. Department of Treasury has also published a Privacy Impact Assessment associated with the OFAC SDN List to inform the public how the program is managed.[6] Moreover, the OFAC SDN List is available on the Treasury public website and a search tool is available to allow external parties and the general public the ability to search the list.[7]

Data Minimization
Privacy Risk: To the extent that the FDIC is not explicitly required to publish insurance determinations via DRR Internet Publications: "Is My Account Fully Insured?" or unclaimed funds via DIV_FUNDS, and thus explicit notice regarding such use is not provided, there is a risk that greater PII is disclosed than is required or addressed via notices.

Mitigation: The FDIC publishes information via DRR Internet Publications: "Is My Account Fully Insured?" and DIV_FUNDS to provide better customer service to individuals impacted by the failure of an insured financial institution. It is in the individual's interest to learn about the status of their deposits and unclaimed funds.

[6] The Department of Treasury is responsible for ensuring compliance with privacy requirements associated with the OFAC SDN List. Office of Foreign Asset Control (OFAC) Consolidated Technology Systems (OCTS) Privacy Impact Assessment (PIA), March 15, 2013 available at https://home.treasury.gov/system/files/236/pia_ofac_octs.pdf.
[7] "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists," https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

Privacy Risk: There is a risk that RRMP collects more data from Login.gov than is necessary to correctly link the identity-proofed claimant to the appropriate records in CAS, NDC, and/or DPS.

Mitigation: Data fields in CAS, NDC, and DPS have been established via specific file structures set forth in FDIC Resolution and Receivership Rules.[8] Having reviewed the list of attributes that could be passed from Login.gov to FDIC via RRMP, DRR determined that the attributes collected are the minimum necessary to properly link an identity-proofed claimant to the appropriate records in CAS, NDC, and/or DPS with an appropriate level of certainty. The attributes are only maintained by RRMP for mere moments prior to being purged. As the RRMP claim function matures, DRR and the Privacy Program will continue to review the data necessary to create this link and will update the attributes passed from Login.gov as appropriate.

Data Quality and Integrity
Privacy Risk: Currently, the NDC non-depositor claimants have the ability to electronically file (e-file) information directly into the FDIC Claims Portal or to submit their information to the DRR Claims department via email or U.S. mail in which case the Claims Agent will enter the information into the NDC system. There is a risk that information may be manually entered incorrectly into the FDIC Claims Portal by the claimant or provided incorrectly via email or U.S. mail by the claimant, which could cause the claimant's information to be incorrect and/or cause for non-payment or misdirected payment.

Mitigation:
If there are errors in a non-depositor claim submitted via the FDIC Claims Portal or via email or mail, and a data entry occurs, such errors are typically discovered during a second-level review process for each claim. If an error passes the second level approval process and exists in the determination letter, it is up to the claimant to notify DRR Claims department and have a Claims Agent correct the error. Claim determinations are based on the claim amount submitted by the claimant as the most reliable source of information.

Privacy Risk: The FDIC collects information from failed or failing financial institutions and cannot attest directly to data quality that it receives. 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. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate.

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?

System	Information Summary
CAS	• Full Name of the financial institution customer (including primary account holder and trustees or beneficiaries) • Date of Birth • Social Security number (SSN) and Taxpayer Identification Number (TIN) • Home Address • Non-work Phone Numbers • Financial Information (e.g., checking and savings account numbers and balances) • Type of account (e.g., single/joint account; revocable trust account; corporate, partnership and unincorporated associations account, irrevocable trust account, employee benefit plan account or government account)
Is My Account Fully Insured?	• Account number • Acquiring institution name

[8] 12 C.F.R. Part 360.

System	Information Summary
	• Failed Financial institution name
NDC	• Full Name of financial institution Non-Deposit Creditor • Social Security number (SSN) or Taxpayer Identification Number (TIN) • Claimant Address (non-work) • Claimant Phone Number (non-work) • Claimant E-mail Address (non-work) (serves as username for log-in) and password provides access to the FDIC Claims Portal • Name of Firm (if applicable) • Claim Amount • Claim Description and Date of Claim • Barcode Number (used to access NDC record) (ties the claim to the applicable receivership) • Fund number (or Financial Institution Number (FIN) - manually entered by DRR Claims Agents) • Claimant ID number (tying the claim to the applicable receivership) • Name, title, and company of individual completing the Proof of Claim form on behalf of a claimant (if applicable) • Proof of Claim form with claimant's signature • Required supporting documentation

DPS	• Full Name of Claimant
	• Claimant Social Security number (SSN) or Taxpayer Identification Number (TIN)
	• Claimant Address (Home or Work, depending on whether claimant is an individual or business)
	• Vendor Identification Number (if applicable)
	• Claim Details, such as:
	  ○ Claim type (e.g., Payout Check, Dividend Check, Unratified Deposit, Receivership Certificate) and priority
	  ○ Financial Institution Number (FIN) and Financial Institution Name associated with claim
	  ○ Total claim amount
	  ○ Total amount paid by receivership, total amount to be paid by receivership and instructions for dividend payments (if Receivership Certificate), payment type (wire or check), date of payment, check number, check status (e.g., Void), whether payment is tax reportable, state/federal income tax withheld for claim payment (if applicable)
	  ○ Escheatment payment number and the state to which an escheated payment is made (if applicable)
	  ○ Date and amount state paid to claimant for escheated payout or unratified deposit
	• Claimant Financial Information [i.e. individual financial institution account data required to make Electronic Funds Transfers (EFT) for the payout or unratified deposit liability. This is used to return funds to the financial institution's customers.]
	• Settlement asset or liability reference and claim amount.

DIV_FUNDS	• Full name of depositor
	• Claim details, such as official item check number
	• Business name
	• Failed institution information, such as:
	  ○ Name
	  ○ City or State

PHS	• Full Name • Social Security number (SSN) • Home Address • Financial Information (account number, account balance, and account type)
RRMP	• Full Name • Date of Birth • Social Security number (SSN) • Financial Information • Home address • Phone number • Email address • Driver's License/ State ID • Gender • Supporting documentation

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: beneficiary name, date of death, gender)	☒	☐

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 (CAS, NDC, PHS, RRMP)	DRR obtains depositor information files from the failing or failed institution. DRR then extracts/prepares the required depositor and existing creditor data elements for upload to the appropriate system.
Discovered Individual Creditors (NDC, RRMP)	As these entities are not known to the FDIC receivership at the time of the financial institution failure, they may register on the FDIC Claims Portal or call a DRR Claims Agent. If they register on the FDIC Claims Portal, they must create a Claimant Record (providing email, name, address, telephone number). The system then generates an e-mail to the individual containing a Notice Letter and Proof of Claim form. They can submit a claim during the same FDIC Claims Portal session.
Individual Financial Institution Depositor (CAS, RRMP)	On occasion, the FDIC Claims Agent requires additional support data or documentation from depositors to make insurance determinations. This occurs when there are questions about the ownership status of the account. This collection typically occurs during an in-person meeting. The required information is entered by authorized Claims Agents.
Known Individual Creditors (NDC, RRMP)	Existing Individual Creditors must complete the Proof of Claim form that was mailed to them after the financial institution closing and return the form, along with required supporting documentation, to DRR via U.S. mail, email, or e-file (FDIC Claims Portal). For those using the FDIC Claims Portal, the claimant is required to log into the site using their email address and password, and barcode number. They can select the name of the financial institution for which they are creating a claim and complete the Proof of Claim by entering their SSN/EIN, Claim Description and Claim Amount, certify that the information is correct and accurate, and upload required supporting documentation.
Manual Input by DRR-Accounting Unit (CAS, NDC, DPS	When approved Receivership Certificate (RC)/dividend cases are processed, DRR-Accounting Unit captures dividend payment instructions for uninsured deposit and non-deposit claims manually. DRR Accounting Unit reviews data received from PASS and RRMP, plus payment method changes received from RRMP. Also, wire transfer data may

Data Source	Description of Information Provided by Source
	be manually input into DPS by DRR-Accounting Unit when the claimant requests this form of payment.
NFE General Ledger and Accounts Payable (DPS)	DRR has an automatic reconciliation with NFE, which imports non-PII, aggregate data such as the check number of paid/voided dividend checks, Vendor Identification Numbers, Journal Entry error files, and invoice error files from NFE AP for payment reconciliation purposes. Also, DRR automatically imports Chartfield data (i.e. accounting data that does not contain PII) and daily and monthly account balances from the NFE General Ledger for account/payment reconciliation purposes.
Failed financial institutions/Deposit Insurance National Bank (DINB) (DPS)	In some instances, when a financial institution fails, the FDIC charters a new national bank, 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 to DPS. These data are necessary to ensure accurate payouts for insured deposits.
Acquiring Institutions (DPS)	Updated data for insured depositors is imported from the acquiring institution in instances when insured depositors have not claimed their funds from the acquiring institution for 18 months following the financial institution closing. These unclaimed funds are referred to as unratified deposit payments. DRR Claims Department receives the unratified deposit data, including the name and check information, from the acquiring institution and verifies that the check amount matches the unclaimed/unratified total. The unclaimed funds are then escheated to the appropriate state treasuries.
Department of Treasury, Office of Foreign Assets Control (OFAC) (SDN List)	The Department of Treasury, Office of Foreign Assets Control maintains the Specially Designated Nationals (SDN) List, against which the FDIC screens the names of depositors (their agents or lawful successors) prior to making insured deposits available in order to ensure that the FDIC does not disburse insured deposits to individuals, entities or countries targeted by OFAC-administered sanctions programs. FDIC compliance with OFAC-administered sanctions is required by 31 CFR 501.603, 604, 606. The SDN List consists of five (5) watch lists: 1. SDN-OFAC - Specially Designated Nationals 2. NON-SDN - OFAC Non-SDN Entity List 3. COUNTRY - OFAC Sanctioned Countries 4. BIS - The Bureau of Industry and Security of the U.S. Department of Commerce 5. DTC - The list of debarred parties administered by the Department of State At any given time, approximately 40 to 50 percent of the names on the list constitute the names of persons. 95 percent of these listings are non-US persons. The identifier information associated with these persons can be extensive, ranging from address and date of birth to social security numbers and passport numbers. FDIC screens claimant names, addresses and TIN/SSN against the OFAC list of terrorists, drug traffickers, and other "specially designated nationals". OFAC marks any matches and sends the marked file back to DRR. A hold is placed on any payments for those records that are marked by OFAC. This screening against the OFAC list is necessary for purposes of compliance with economic sanctions programs. In the event that OFAC-administered sanctions have been lifted, the FDIC will consult with OFAC as to the disbursement of the funds to the appropriate party. When the receivership with which the insured deposit is associated terminates, the FDIC coordinates with OFAC to determine further disposition of the funds.
State Treasury Offices (DPS)	State treasury offices provide data about payments of previously unclaimed funds; the date and amount are collected and entered by authorized DRR Accounting personnel. Following a financial institution closing, the FDIC will attempt to locate owners of insured deposit accounts for 18 months by publishing data on DIV_FUNDS, after which any remaining funds are escheated to the state treasury offices. The escheatment process consists of the FDIC transmitting the financial institution account data to the state where the depositor was last known to have resided along with a check for the unclaimed amount. The escheated funds are held by the states as a custodian for the depositor for up to ten years. If the funds are unclaimed at the end of this time, they are returned to the FDIC. For each insured deposit account escheated to the states, the FDIC expects either a notification of the payment date or a return of the funds, in either case whether paid or returned by state, data are captured.

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

CAS, NDC, and DPS are covered under the CAS ATO granted on December 20, 2013. DRR Internet Publications "Is My Account Fully Insured?" and DIV_FUNDS are covered under the Cloud.gov ATO granted December 22, 2020 and reauthorized each time a new subsystem is added. PHS is covered under Enterprise Data management GSS ATO granted on October 21, 2011. RRMP is covered under the Salesforce ATO granted on October 25, 2017.

The Authority to Operate for each 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.

FDIC Privacy Act SORN 30-64-0013, Insured Financial Institution Liquidation Records covers use of:

- CAS,
- DRR Internet Publications, "Is My Account Fully Insured?",
- NDC,
- DPS,
- PHS, and
- RRMP.

This SORN covers the individual's files held by the closed or assisted financial institution, including loan or contractual agreements, related documents, and correspondence.

FDIC Privacy Act SORN 30-64-0024, Unclaimed Deposit Account Records covers DIV_FUNDS. This SORN covers deposit account records, including signature cards, last known home address, social security number, name of insured depository institution, relating to unclaimed insured deposits or insured transferred deposits from closed insured depository institutions for which the FDIC was appointed receiver after January 1, 1989.

SORN coverage exists for financial institution closing activity only. Data used for resolution planning and validation of financial institution deposit hold, and sweep files for compliance purposes, do not operate as a Privacy Act system of 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 collect 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. However, financial institutions are required by law to provide applicable notices to their customers regarding the purpose for collection and intended uses of the information. Individuals may review the relevant third party's privacy notices to learn how to access their information. Moreover, financial institutions are legally obligated to provide notice to individuals regarding the FDIC role as regulator and insurer of deposits. For information that FDIC uses that originates from the Department of Treasury, OFAC, the Department of Treasury, OFAC would be responsible for providing notice. However, the FDIC does provide notice to the depositors in the event that access to their accounts is blocked as a result of the OFAC SDN List.

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, and the Privacy Program. See https://www.fdic.gov/policies/privacy/index.html.

Privacy Risk Analysis: Related to Transparency

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

Mitigation: When a financial institution is insured by the FDIC, it must display the FDIC logo at their physical locations and on their websites. This public association between the insured financial institution and the FDIC provides public transparency that there is an established relationship between the FDIC and the insured financial institution. Moreover, financial institutions are legally obligated to provide notice to individuals regarding the FDIC role as regulator and insurer of deposits. The access that the FDIC obtains to data from an insured financial institution is authorized and necessary under the Federal Deposit Insurance (FDI) Act to identify failing financial institutions and to resolve failed financial institutions.

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

Mitigation: When a financial institution fails, FDIC publishes a notice in the local newspaper(s) about the financial institution failure and information relating to the opportunity for creditors to file a claim. If there are

any "discovered" creditor claimants, they are directed to the main FDIC web site (www.fdic.gov) to obtain further information, such as the Proof of Claim form and then directed to the FDIC Claims Portal web site to register and set up a claimant record in NDC. Please see answer in 2.1 for more clarification.

Privacy Risk: Depositors and creditors may not know that their information will be searched against the U.S. Treasury Office of Foreign Assets Controls (OFAC) Special Designated Nationals (SDN) List in order for FDIC to ensure that it does not disburse insured deposits or debts owed to individuals, entities or countries targeted by OFAC-administered sanctions programs.

Mitigation: The FDIC has published this PIA to provide transparency to the public regarding how their information may be processed as part of the insurance determinations and payouts process. The FDIC must comply with the requirements of 31 CFR 501.603, 604, 606, which define the reports required regarding economic sanctions programs, to ensure that the FDIC does not disburse insured deposits or debts owed to individuals, entities or countries targeted by OFAC-administered sanctions programs. The U.S. Department of Treasury has also published a Privacy Impact Assessment associated with the OFAC SDN List to inform the public how the program is managed.[9] Moreover, the OFAC SDN List is available on the Treasury public website and a search tool is available to allow external parties and the general public the ability to search the list.[10]

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 from third parties: FDIC systems collect data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Given the limitations around how this data can be used for monitoring or resolving failed financial institutions, the FDIC may not be authorized to provide individuals access to the information that it obtains.

However, financial institutions are required by law to provide applicable notices to their customers regarding procedures for accessing their information. Individuals may review the relevant third party's privacy notices to learn how to access their information. For information that FDIC uses that originates from the Department of Treasury OFAC, the Department of Treasury, OFAC would be responsible for providing access. However, the FDIC does provide notice to the depositors in the event that access to their accounts is blocked as a result of the OFAC SDN List. In addition, individuals can access the OFAC SDN List on the Department of Treasury's public website and use the search tool to find their names.

Information collected and maintained by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, access procedures are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORN(s) 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 FDIC Circular 1360.1.

In addition, CAS, NDC, and DPS have additional procedures that allow individuals to access their information as described below:

- **CAS**—Shortly after a financial institution fails, DRR will send out "notice to depositors" explaining that a financial institution has closed and giving direction to depositors on the next steps of the process. Using this process, individuals provide additional data or documentation to support determination of ownership and insurance determinations. The resulting information is manually entered into CAS by an authorized Claims Agent.

[9] The Department of Treasury is responsible for ensuring compliance with privacy requirements associated with the OFAC SDN List. Office of Foreign Asset Control (OFAC) Consolidated Technology Systems (OCTS) Privacy Impact Assessment (PIA), March 15, 2013 available at https://home.treasury.gov/system/files/236/pia_ofac_octs.pdf.

[10] "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists," https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

- **NDC—** Shortly after the financial institution closing, FDIC publishes a notice in the local newspaper(s) about the financial institution failure and opportunity for creditors to file a claim. The Notice Letter that DRR mails to all non-deposit creditors found on the financial institution's book also provides a link to e-file via the FDIC Claims Portal. The non-depositor creditors are responsible for ensuring the completeness of the information when creating a claimant record and must confirm the information prior to submission. Claimant information can be updated by the Claims Agent within the FDIC Claims Portal. For non e-file claimants, the Proof of Claim form may be filed via U.S. mail or email. In those instances, authorized DRR Claims Agents will manually add the claim documents to the Claimant Record or create a new Claimant Record and upload the claim documents. During the review of the claim documents, DRR Claims Agents may determine that additional information is required to process the claim. The information is collected via U.S. mail, email, or via the FDIC Claims Portal.

- **Access and proposed edits to CAS, NDC, DPS via the FDIC Claims Portal—**Claimants can also use the FDIC Claims Portal to submit requested edits to their mailing address and payment method. Upon submission, the proposed edits are reviewed and approved by DRR prior to taking effect in CAS, NDC, or DPS.

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

Information collected from third parties: The FDIC systems that collect information from failed or failing financial institutions initially operate from a point-in-time snapshot[11] of data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Given the limitations around how this data can be used for monitoring or resolving failed financial institutions, the FDIC may not be authorized to correct inaccurate or erroneous information. However, financial institutions are required by law to provide applicable notices to their customers regarding procedures for correcting inaccurate or erroneous information. Individuals may review the relevant third party's privacy notices to learn the procedures to correct inaccurate or erroneous information. For information that FDIC uses that originates from the Department of Treasury, OFAC, individuals and entities listed on the SDN List have the ability to petition for removal via mail or email as instructed on the "Filing a petition for Removal from an OFAC List" on the Department of Treasury OFAC webpage.[12]

Information collected and maintained by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, amendment procedures are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORN(s) on the FDIC public-facing website, which includes rules and regulations governing how individuals may amend their records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1.

In addition, claimants who successfully accomplish the identity-proofing process via Login.gov through RRMP are able to review their records on the FDIC Claims Portal and submit updates to certain incorrect or erroneous information in their records in CAS, NDC, and DPS. Specifically, claimants can submit updates for their mailing address and financial account information where they wish to receive their insured deposits or dividends. Updates submitted by claimants are reviewed by DRR prior to the changes being made in CAS, NDC, or DPS.

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

Information collected from third parties: FDIC systems collect data provided by failed or failing financial institutions to the FDIC during the pre-closing activities. Accordingly, the FDIC is unable to

[11] When FDIC sends a file during the pre-close phase of the closing, it 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.
[12] Access and correction procedures are available at "Filing a Petition for Removal from an OFAC List", https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-sdn-list/filing-a-petition-for-removal-from-an-ofac-list.

notify individuals about the procedures for correcting their information that the FDIC collects from third parties. However, 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 to understand the procedures for correcting their information. For information that FDIC uses that originates from the Department of Treasury, OFAC, individuals may receive notice about the procedures for correcting their information through this PIA, the Department of Treasury's PIA,[13] and the Department of Treasury OFAC webpage.[14]

Information collected by FDIC: In cases where the FDIC has collected PII directly from the individual or maintains the information in a Privacy Act System of Record, notification is provided as described in Question 3.1 including "notice to depositors" and newspaper publications regarding closing/closed financial institutions. Additionally, notification procedures are detailed in the SORN(s) 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 amend their records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1.

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 SORN(s) listed in Section 10.4 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

The FDIC Claims Portal Homepage provides information about what claimants can do in RRMP, such as:

- Changing mailing address,
- Requesting deposits or dividends be sent electronically to an account at another bank,
- Requesting to speak to a Claims Agent, and
- Seek payment for goods and services supplied to an institution prior to that institution's failure.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: Individuals are not afforded access and amendment rights to all records that support the insurance determinations and payouts process.

Mitigation: Financial institutions provide DRR with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the FDI Act. Given the limitations around how this data can be used for monitoring or resolving failed financial institutions, the FDIC is not authorized to provide individuals access and amendment to all the information that it obtains. However, financial institutions are required by law to provide applicable notices to their customers regarding opportunities for access and amendment of their information. For individuals impacted by the Department of Treasury OFAC program and SDN List, Department of Treasury publishes a website detailing their program, including the formal process for seeking removal of an individual's name from the SDN List.

To the extent that the FDIC collects data directly from individuals, access to that information is provided via procedures outlined in the applicable SORN. Moreover, the FDIC has developed two systems, DRR Internet Publications "Is My Account Fully Insured?" and DIV_FUNDS to provide individuals with greater access to information related to failed financial institutions.

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

[13] https://home.treasury.gov/system/files/236/pia_ofac_octs.pdf.
[14] https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-list-sdn-list/filing-a-petition-for-removal-from-an-ofac-list.

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 insurance determinations and payouts process are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/policies/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 DRR based on evolving business requirements and the 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.

Contractors may also provide services to the FDIC, such as staff and operations augmentation to support noticing and claims administration in the event that DRR must scale its operations to support resolution of a large and complex financial institution that has failed.

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 support the insurance determinations and payouts process. Access to individual's PII is role-based and minimized. All contractors must also pass a background check. 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.

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 (SAOP) Report 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?

Where the insurance determinations and payouts process is covered by the Privacy Act, 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 1031.1 Disclosures are tracked and managed using FOIAXpress.

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 1031.1.

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

Where the insurance determinations and payouts process is covered by the Privacy Act, 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 1031.1.

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 System of Records Notices (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:

- 12 U.S.C. 1819: states that FDIC can make examinations of and to require information and reports from depository institutions
- 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 performing required functions
- 12 CFR 366: deals with FDIC contractors

- 31 CFR 501.603, 604, 606: defines requirements of economic sanctions programs

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority, as 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 System of Records 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?

FDIC minimizes the PII elements to what is relevant and necessary to accomplish the legally authorized purpose of making the insurance determinations and payouts in the following ways:

- DRR extracts the minimum data elements needed to make insurance determinations and issue payouts as part of an overall transfer of the depositor information files from the failed or failing institution to FDIC during the financial institution closing process.
- The systems that support DRR insurance determinations and payouts process use system-to-system connections wherever possible to ensure that the data exchanged maintains a high level of accuracy and only import required data elements wherever possible. For example:
    - CAS shares PII with DPS, DRR Internet Publications: "Is My Account Fully Insured?" and NDC;
    - NDC shares PII with DPS;
    - DPS shares with CAS, NDC, and DIV_FUNDS;
    - PHS shares with CAS and DPS; and
    - RRMP shares with CAS, NDC, and DPS.
- DRR only uses supporting collections (e.g. Proof of Claim form) to gather data elements needed to verify and process the claim, as necessary.
- DRR minimizes the publication of insurance determinations and unclaimed funds via DRR Internet Publications, "Is My Account Fully Insured?" and DIV_FUNDS, respectively, to what is necessary to help individuals locate, understand the status of, and make appropriate changes, as necessary, to their accounts previously held by a failed institution.
- The systems supporting the insurance determinations and payouts process are analyzed by FDIC Records and Information Management Unit (RIMU) to establish retention and disposition schedules to reduce privacy risk.
- DRR uses only those data attributes collected by Login.gov for the purposes of identity-proofing a claimant necessary to link the claimant to the appropriate record in CAS, NDC, or DPS via RRMP. The data is encrypted and used for mere moments to confirm a link between the user and the record before being deleted in RRMP. DRR has worked with the Privacy Program to determine that the current dataset is the minimum necessary to ensure a correct link.

Additionally, through the conduct, evaluation and review of privacy artifacts,[15] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

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

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?

The FDIC insurance determinations and payouts process only collects and retains PII from financial institution depositor and non-depositors when a financial institution is being monitored for resolution planning or has failed, as represented in the notice financial institutions are legally obligated to provide to individuals regarding the FDIC role as regulator and insurer of deposits.

Notice regarding specific sub-processes—e.g., the FDIC publication of unclaimed deposits and insurance determination of accounts via DIV_FUNDS and DRR Internet Publications "Is My Account Fully Insured?" respectively, and the use of OFAC SDN List—is implicitly provided via FDIC authorities to resolve failed financial institutions.

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.

For CAS, deposit records for financial institutions that do fail are destroyed 15 years after the termination of the receivership while deposit records for financial institutions that do not fail are destroyed 2 years after discontinuance of case. For NDC, records are destroyed ten years after the termination of the receivership. For DPS, records are destroyed ten years after the termination of the receivership.

For DIV_FUNDS, FDIC has determined that a retention schedule is not required since DPS is the source.

For DRR Internet Publications: "Is My Account Fully Insured?", RIMU has determined that they are not agency records and do not require a retention schedule. The information that supports the "Is My Account Fully Insured?" function is maintained on the website for 30 days following a financial institution failure.

For PHS, data from open financial institutions being monitored are maintained for no longer than 6 months after receipt of the data from the financial institution, and data from failed financial institutions are maintained for 6 months from date of receivership.

For RRMP, deposit claim records are destroyed 15 years after the termination of the receivership and non-deposit claims are destroyed 10 years after the termination of the receivership.

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 1210.1 and 1360.9.

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: To the extent that the FDIC is not explicitly required to publish insurance determinations via DRR Internet Publications: "Is My Account Fully Insured?" or unclaimed funds via DIV_FUNDS, and thus explicit notice regarding such use is not provided, there is a risk that greater PII is disclosed than is required or addressed via notices.

Mitigation: The FDIC publishes information via DRR Internet Publications: "Is My Account Fully Insured?" and DIV_FUNDS to provide better customer service to individuals impacted by the failure of an insured financial institution. It is in the individual's interest to learn about the status of their deposits and unclaimed funds.

Privacy Risk: There is a risk that RRMP collects more data from Login.gov than is necessary to correctly link the identity-proofed claimant to the appropriate records in CAS, NDC, and/or DPS.

Mitigation: Data fields in CAS, NDC, and DPS have been established via specific file structures set forth in FDIC Resolution and Receivership Rules.[16] Having reviewed the list of attributes that could be passed from Login.gov to FDIC via RRMP, DRR determined that the attributes collected are the minimum necessary to properly link an identity-proofed claimant to the appropriate records in CAS, NDC, and/or DPS with an appropriate level of certainty. The fact that the attributes are only maintained by RRMP for mere moments prior to being purged also partially mitigates this risk. As the RRMP claim function matures, DRR and the Privacy Program will continue to review the data necessary to create this link and will update the attributes passed from Login.gov as appropriate.

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.

Most systems involved in the FDIC insurance determinations and payouts process operate from a point-in-time snapshot of data provided by failed or failing financial institutions during the pre-closing activities, or from non-depositor or creditor entities. The responsibility for quality, utility, and objectivity of that point-in-time snapshot of data belongs to the failed or failing financial institutions. Similarly, the Department of Treasury maintains the OFAC SDN List and is responsible for ensuring the data quality and integrity of the SDN List.

[16] 12 C.F.R. Part 360.

Systems involved in the insurance determinations and payouts process maintained by the FDIC have processes in place to ensure that data fields have appropriate formatting, and that the data matches any existing records or PII, especially in cases of identification for claims and payments purposes. Where manual data entry is used, as in the case of Claims Agents entering claim information received from non-depositors via email or U.S. mail into NDC, there is a second-level review process for each claim and a subsequent process for the non-depositor to correct any error after they receive FDIC's determination. 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.

For the information that FDIC publishes via DRR Internet Publications: "Is My Account Fully Insured?" and DIV_FUNDS, the FDIC has the following Website Policies, General Disclaimer:

> The FDIC has taken reasonable measures to ensure that the information and data presented on this website is accurate and current. However, the FDIC makes no express or implied warranty regarding such information or data, and hereby expressly disclaims all legal liability and responsibility to persons or entities who use or access this site and its content, based on their reliance on any information or data that is available through this website.

Finally, 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.

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

The FDIC collects PII directly from the individual to the greatest extent practicable, which primarily involves collecting directly from the individual to provide customer service and verify the identity of individuals providing the information necessary for the processing of claims and payments. The majority of the insurance determinations and payouts process, however, relies on the collection of information from failing and failed financial institutions and the Department of Treasury, OFAC.

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 configures 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: Currently, the NDC non-depositor claimants have the ability to electronically file (e-file) information directly into the FDIC Claims Portal or to submit their information to the DRR Claims department via email or U.S. mail in which case the Claims Agent will enter the information into the NDC system. There is a risk that information may be manually entered incorrectly into the FDIC Claims Portal by the claimant or provided incorrectly via email or U.S. mail by the claimant, which could cause the claimant's information to be incorrect and/or cause for non-payment or misdirected payment.

Mitigation:
If there are errors in a non-depositor claim submitted via the FDIC Claims Portal or via email or mail, and a data entry occurs, such errors are typically discovered during a second-level review process for each claim. If an error passes the second level approval process and exists in the determination letter, it is up to the claimant to notify DRR Claims department and have a Claims Agent correct the error. Claim determinations are based on the claim amount submitted by the claimant as the most reliable source of information.

Privacy Risk: The FDIC collects information from failed or failing financial institutions and cannot attest directly to data quality that it receives. 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. The FDIC also follows procedures that allow individuals to subsequently access and correct their information, as appropriate. Please see answer in 3.0 for more clarification.

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.

Individuals authorize the use of the PII for insurance determinations and payouts process when they choose to establish a business relationship with the financial institution insured by the FDIC, and when they choose to submit their information directly to the FDIC, as appropriate. To the extent that the FDIC publishes insurance determinations via DRR Internet Publications: "Is My Account Fully Insured?" or unclaimed funds via DIV_FUNDS, individual authorization is implied and the lack of explicit authorization is offset by need to inform individuals about the insurance status and location of their accounts previously held by a failed institution.

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. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 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.

The insurance determinations and payouts process primarily receives data from third parties, i.e., failed or failing financial institutions, and from Department of Treasury, OFAC. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant third party's privacy notices. FDIC-insured financial institutions are required by law to provide notice to individuals regarding FDIC insurance, to display the official FDIC logo, and to meet requirements for how depository institutions may advertise their FDIC membership. The FDIC also provides the general public with notice regarding how deposit insurance works. These notices help the individual understand the consequences of establishing a business relationship with an FDIC-insured institution. For information that FDIC collects originating from the Department of Treasury, OFAC, the FDIC provides notice to the depositors about the consequences of how their PII is being used in the event that they are blocked from accessing their accounts in accordance with the FDI Act.

Where the insurance determinations and payouts process collects information 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. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 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.

8.3 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.

The insurance determinations and payouts process only uses PII for the purposes listed in Section 9.1. This PIA and the relevant SORNs listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

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/policies/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 are 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 DRR with the depositor information files pursuant to the supervisory and regulatory authority granted to the FDIC by the FDI 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.

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 DRR Standard Operating Procedures (SOP) detail how all PII is collected, used, and maintained as part of the DRR insurance determinations and payouts process, to perform the following functions:

1. Determine financial institution depositor's account(s) insurance status;
2. Make determinations and payments in accordance with insurance;
3. Evaluate and process depositor and non-depositor/creditor claims;
4. Complete payouts and dividend distributions;
5. Manage account balances, reporting, and reconciliation with the General Ledger;
6. Manage and process income statements and other tax-related items;
7. Allow depositors to query status and coverage of failed institutions;
8. Search for unclaimed funds; and
9. Verify and investigate claims against U.S. Treasury Office of Foreign Assets Controls (OFAC), Credit Bureaus, State Officials, and other investigatory databases.

In general, names, Social Security numbers, financial information, and contact information are necessary to support each of these functions.

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.

Moreover, DRR 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 the FDIC 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. Below is a listing of the primary users and uses of the data supporting the insurance determinations and payouts process:

- DRR Claims Agents use information to analyze claims, make determinations for disbursements, and respond to depositor inquiries;
- DRR Business Information Systems staff use information to prepare for CAS and NDC claims processing;
- DRR customer service personnel use information to respond to inquiries for both deposit and non-deposit (creditor) claims;
- DRR Accounting personnel use information to process disbursements and other accounting matters;
- DRR Cashier staff use information for reviewing payout liabilities and to print payout checks; and
- Contractor personnel support DRR in a general capacity and use the information for authorized purposes.

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 the systems involved in the insurance determinations and payouts 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.

The table below describes the sharing of data with internal systems and the purpose for the sharing.

Source	Destination	Purpose
Failing/Failed Financial Institutions (Depositor Information Files)	- Claims Administration System (CAS) - Non-Deposit Claims (NDC) - Dividend Processing System (DPS) - Provisional Hold System (PHS)	Support insurance determinations and payouts
CAS/NDC	DPS	Support payouts
	DRR Internet Publications : Is My Account Fully Insured?	Permit website publication so individuals can locate and understand the status of their accounts previously held by a failed institution
	RRMP	Support the "self-service" functionality that permits claimants to view and submit appropriate edits to their data to support the efficient resolution of a failed financial institution
DPS	NFE General Ledger	Manage account balances, reporting, and reconciliation with the General Ledger
	DIV_FUNDS	Permit website publication so individuals can locate unclaimed funds
	PASS	Support the settlement process with the Acquiring Institution
	RRMP	Support the "self-service" functionality that permits claimants to view and submit appropriate edits to their data to support the

Source	Destination	Purpose
		efficient resolution of a failed financial institution
OFAC SDN List	Closed Bank SharePoint Site	Facilitate financial institution closing activities by storing, organizing, and sharing documents used during the resolution process
RRMP	CAS. NDC, DPS	Support the "self-service" functionality that permits claimants to view and submit appropriate edits to their data to support the efficient resolution of a failed financial institution
PASS	DPS	Support the settlement process with the Acquiring Institution

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.

The sharing with external entities, the purpose and agreements related to the sharing are for the systems supporting the insurance determinations and payout process is discussed in the table below.

Source	Destination	Purpose	Sharing Pursuant to…
CAS	Department of Treasury, OFAC	Compliance with economic sanctions	MOU
NDC	Department of Treasury, OFAC	Compliance with economic sanctions	MOU
DPS	Department of Treasury, OFAC	Compliance with economic sanctions	MOU
	Federal and State Tax Offices	Tax reporting purposes	Law
	Check Distribution Vendors	Payouts	Contract
	Electronic Payment Provider	Payouts	Contract
DRR Internet Publications: "Is My Account Fully Insured?"	Members of the Public via website	Transparency	N/A
DIV_FUNDS	Members of the Public via website	Transparency	N/A
Login.gov	RRMP	Identity Verification	IAA

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 1031.1 "Administration of the Privacy Act," 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 and FDIC Circular 1360.9.

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 for the insurance determinations and payouts process. 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 related to security for the insurance determinations and payouts process.

Mitigation: No mitigation actions are recommended.