FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
New Financial Environment (NFE)

OCISO

PIA-FDIC-0170

11/23/2020

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

Owned by the FDIC's Division of Finance (DOF), the New Financial Environment (NFE) system is a unified set of financial systems that are managed together and operated in an integrated fashion. The system processes and records financial (i.e., income, expenses, liabilities, assets, etc.), budgetary, procurement, contractual, and investment data at both the Corporate (e.g., fund, account, program etc.) and Receivership levels. The data is summarized and reported on by a number of dimensions, such as time, fund, account, program, organization, and Receivership, down to the individual [Employee Identification Number (EIN) or Social Security Number (SSN)] and vendor level (Tax Identification Number). The system processes data daily, monthly, and at the end of the year.

NFE supports an array of accounting and financial data from the following areas: Budgetary, Invoicing, Purchase Orders, Vendors, Billing and Receivables, Contracts, Requisitions, Acquisitions, Receiverships, Cash and Investments, Capital Assets, Projects, Travel and Expense (T&E), Payroll Transmission Accounting and Reporting (PTAR), and General Ledger. The system is comprised of a suite of modules, of which the following contain personally identifiable information (PII) about FDIC employees, vendors that provide goods or services to FDIC, and Receivership claimants, which refers to customers or vendors of failed financial institutions that have claims against the FDIC in its Receivership capacity.

a. Supplemental Payment System (SPS) performs all corporate employee payment functions for NFE, including disbursing supplemental payments to current and former FDIC employees, as well as facilitating the reporting of tax data to federal and state agencies and employees by centralizing and integrating the calculation of taxes for various payments (buyout, travel, relocation, and other miscellaneous payments). As such, SPS contains PII such as the names, SSNs, banking information, and home addresses of current and former FDIC employees. SPS is owned by DOF, but it is housed in the Division of Administration's (DOA's) Corporate Human Resources Information System (CHRIS),[2] which is located on a different server from the other NFE modules.

While not stored in NFE or SPS, FDIC employees' Supplemental W-2s are available to employees for viewing and printing via the NFE Supplemental W-2 Self-Service application. FDIC employees can access the NFE Supplemental W-2 Self-Service application by logging into NFE and clicking on the link for W-2. The employee is then prompted to re-enter his/her FDIC Active Directory ID credentials, which are used to authenticate the employee and retrieve the employee's name, SSN, and EIN from SPS. In turn, these PII elements are used as the key fields to retrieve the employee's Supplemental W-2 from OneSource (eComply)[3] and return it on-screen to the requesting employee. OneSource is a financial database that is owned and operated by a third-party vendor that assists the FDIC with processing, mailing, and electronically filing tax reporting data.

[1] www.fdic.gov/privacy

[2] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[3] FDIC System of Records Notice (SORN) 30-64-0012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

b. **Payroll Transmission Accounting and Reporting (PTAR)** module is used by DOF to accurately record payroll and expense data, calculate monthly accruals, and create reports based on the biweekly payroll file exchanged with the United States Department of Agriculture (USDA) National Finance Center (NFC).[4] PTAR contains PII about FDIC employees such SSNs, names, dates of birth, and home addresses.

The process starts when FDIC employees input their time and attendance into the FDIC's time and attendance (TA) software application known as WebTA.[5] WebTA securely transmits this data, which includes employee names, SSNs, and timesheet charges for the most recent pay period, to NFC via an automated scheduled information transfer for the purpose of payroll processing. NFC processes the WebTA data, issues paychecks to employees, and securely transmits an electronic file of post-payroll data back to FDIC. The NFC file contains the output from the WebTA data, along with additional data provided by NFC, such as employee home address and wage/salary. The NFC data is automatically reformatted, edited, merged with accounting codes/data used to identify and track financial transactions and accounting distributions and the EIN, and creates the journal entries to be posted to the NFE General Ledger.

c. **Enterprise Performance Module (EPM)** is a data warehouse that provides financial reporting functionalities. EPM maintains vendor and employee financial transactions (payments), some of which may contain PII data (such as SSN and home address) from files received from NFC as described above. EPM stores the data in tables which are controlled via access control roles.

d. **Travel & Expense (T&E)** module enables FDIC travelers to request reimbursement for their official travel expenses. PII contained within this module includes names, home addresses, corporate-issued credit card numbers, and EINs of traveling employees.

FDIC employees have access to the T&E module to enter their travel vouchers and expense information. However, employees do not have the ability to enter their PII/personnel-related data (e.g., name, EIN, address, etc.) directly into NFE. This information is derived from the FDIC Corporate Human Resources Information System (CHRIS).

In addition, NFE receives a file containing FDIC travel and purchase card transactions from the General Services Administration (GSA) SmartPay Program contractor bank[6] for purposes of generating monthly payments and recording expenses. The GSA SmartPay Program contractor bank supplies purchase management and travel card services for the FDIC and other Federal agencies, handling all aspects of card approval, authorization, and processing.

e. **Supplier** module contains information about FDIC suppliers/vendors and Receivership claimants/payees. PII includes vendor name, vendor address, vendor ID, vendor phone number, vendor bank account, vendor taxpayer identification number (TIN), claimant name, and claimant address.

FDIC vendors and claimants/payees do not directly access or input information into NFE. With limited exceptions, NFE generally receives this information via the system interfaces detailed below. However, in limited cases, and upon request, FDIC Vendor Maintenance personnel manually enter vendor information and updates from the following forms into NFE: Internal Revenue Service (IRS)

---

[4] USDA Privacy Impact Assessment (PIA) for NFC (June 8, 2018), https://www.usaid.gov/privacy-policy/pia-summaries/usda-nfc-pps.

[5] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[6] GSA Privacy Impact Assessment (PIA) for SmartPay Purchase Charge Card Program (September 14, 2020), https://www.gsa.gov/cdnstatic/GSA%20SmartPay%20-US%20Bank_PIA_September2020docx.pdf.

Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10).

The United States General Services Administration (GSA) System for Award Management (SAM),[7] which is the U.S. Federal Government's authoritative source and central registrant database for government contractors/vendors, sends vendor registrant data to FDIC via a batch job to a server, which uploads the file to NFE. NFE also receives contract award and contract modification data from the FDIC's Automated Procurement System (APS), which is the FDIC's contract drafting, tracking, and monitoring system. APS does not operate as a Privacy Act System of Record and, therefore, is not covered by a Privacy Act System of Records Notice (SORN).

Additionally, NFE receives legal-related contract invoices that include vendor profile information, such as the vendor name, address, and phone number, from the FDIC's Advanced Legal Information System (ALIS). ALIS is the FDIC's principal system for legal matter management/tracking, budgeting, and invoice processing. ALIS does not operate as a Privacy Act System of Record; however, it processes information imported from other FDIC record systems for which there currently are Privacy Act Systems of Records in existence.[8]

FDIC's Warranties Representations Account Processing System (WRAPS)[9] provides claimant/payee and disbursement records to NFE via nightly batch jobs. WRAPS supports DRR with processing and tracking claims made by purchasers of Receivership loans and other related assets under the terms of their loan sales agreements.

FDIC's Dividend Processing System (DPS)[10] provides dividend checks/wire orders and vendor transactions via secure transmission to NFE for reconciliation and recording. DPS assists FDIC's Division of Resolutions and Receiverships (DRR) with calculating and issuing the appropriate payments to claimants, as well as reconciling those payments with the FDIC's General Ledger. DPS also sends a list of claimant names and addresses to NFE's Accounts Payable module. This occurs when uninsured deposit claimants and unpaid vendors/payees are set up to receive dividends from the sale of the failed bank's assets.

f. **Accounts Payable (AP)** module supports all FDIC accounts payable functions. The module contains the following types of PII: vendor name, vendor address, vendor ID, vendor phone number, vendor bank account number, claimant name, and claimant address. Refer to the above section for details on how NFE derives this information.

FDIC Accounts Payable produces payment files that are transmitted to a third-party financial institution[11] with which FDIC has contracted to issue payments for vendor products and services, for employee travel reimbursements, or to individuals with claims against FDIC-insured institutions. In turn, the contracted financial institution provides NFE with a disbursement file containing the status of payments.

---

[7] GSA Privacy Impact Assessment (PIA) for System for Award Management (SAM) (July 16, 2020), https://www.gsa.gov/cdnstatic/System_for_Award_Management_(SAM)_PIA_July2020docx.pdf .

[8] FDIC System of Records Notices (SORNs) Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015), 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[9] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[10] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[11] FDIC System of Records Notice (SORN) 30-64-0012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

g. **Accounts Receivable (AR)** module contains name, address, and phone number of individuals or third parties (e.g., other government agencies, employees, or claimants) that owe funds to the FDIC. Individuals and third parties who are owed funds by FDIC do not have direct access to enter their information into NFE. Information pertaining to claimants is derived via the system interfaces described above. Information pertaining to employees or other government agencies that owe funds to FDIC is typically manually entered into NFE by DOF staff.

h. **eProcurement and Purchasing** modules work together to help manage organizational spending by decentralizing basic purchasing activities and empowering employees to make procurement decisions. The Purchasing module manages all purchasing activities (such as requisitions, change orders, purchase orders, contracts, and shipment receipts) related to procurement of goods and services. The eProcurement module integrates with the Supplier module to provide search tools that help users find the right items to purchase and supports the approval of procurement requests. To support the aforementioned functionality, the eProcurement and Purchasing modules contain information about FDIC suppliers/vendors, such as vendor name, vendor address, vendor ID, vendor phone number, and contract number. Refer to the above sections for details on how NFE derives this vendor information.

PRIVACY RISK SUMMARY

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

- Transparency
- Access and Amendment
- Minimization
- Individual Participation

Transparency:
Privacy Risk: NFE generally does not collect PII directly from individual FDIC employees, vendors and claimants/payees who are owed funds by the FDIC. Rather, NFE typically receives this PII via the system interfaces described in the previous section of this PIA. Therefore, these individuals may not be aware that their data has been utilized or processed by NFE.

Mitigation: In instances where NFE imports PII from other FDIC Privacy Act systems of records (SORs), including those referenced in the previous section of this PIA, the FDIC provides notice to individuals through the respective Privacy Act Statements (PASs) and System of Records Notices (SORNs) for these source systems. Such record systems include the Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), Personnel Benefits and Enrollment Records (FDIC-30-64-0014), and Personnel Records (SORN 30-64-0015). The FDIC publishes its SORNs on the FDIC public-facing website, which includes instructions on how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

In instances where NFE ingests PII from non-FDIC systems or entities, including those detailed in the System Overview section, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice of FDIC's uses of the PII. No additional mitigation actions are recommended.

Access and Amendment:
Privacy Risk: In some cases, NFE derives PII about vendors from third-party sources, including the United States General Services Administration (GSA) System for Award Management (SAM). The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: In instances where NFE derives PII from GSA SAM, GSA has a responsibility and vested interest in ensuring that the PII it collected is correct to preclude compliance issues with Federal mandates. Namely, GSA SAM, as the U.S. Federal Government's authoritative source and central registrant database for government contractors/vendors, is responsible for ensuring accurate, complete and up-to-date information for entities that register to do business with the U.S. government, in accordance with the Federal Acquisition Regulation (FAR) Subpart 4.11 and Title 2 of the Code of Federal Regulations (2 CFR) Subtitle A, Chapter I, and Part 25. Since GSA SAM originates and maintains the Federal government's authoritative source for vendor registrant data, FDIC refers vendors directly to GSA SAM to correct any erroneous or inaccurate vendor registrant/PII data. Vendors wishing to make amendments to transactional or invoicing information contained in NFE may contact the applicable FDIC Technical Monitor who is responsible for approving their invoices. Additionally, in limited cases and upon request, FDIC Vendor Maintenance personnel may manually enter/update vendor information in NFE, using the tax forms described in the previous section. No additional mitigation actions are recommended.

Minimization:
Privacy Risk: NFE collects and maintains Social Security Numbers (SSNs) for identification and payment/tax-related purposes. As a Privacy best practice, organizations should minimize the collection and use of SSN wherever possible.

Mitigation: Since SSN is the primary identifier for individuals for purposes of taxes and financial interactions, the data quality benefits of using SSN within the system have justified its continued use. Nevertheless, wherever possible, NFE uses Employee Identification Number (EIN) in place of SSN.

Privacy Risk: A formal records retention process has not yet been documented for NFE, which could result in records being maintained for a period longer than necessary and increases the potential amount of PII compromised in the event of a privacy breach.

Mitigation: There is currently an effort underway with FDIC Records and Information Management Unit (RIMU) to determine appropriate retention schedules for data contained within NFE. No formal retention schedule(s) have been determined yet.

Individual Participation:
Privacy Risk: There is risk related to individual participation for NFE because data is not always collected directly from individuals. Rather, NFE typically receives PII via the system interfaces described in the first section of this PIA. Therefore, individuals may not be aware of and/or have provided explicit consent for the collection and use of their information within NFE.

Mitigation: In instances where NFE derives PII from third-party sources, including those described in the first section of this PIA, the FDIC does not have the ability to provide privacy notices or obtain explicit consent prior to its processing of these individuals' PII. Individuals should review the relevant third party's privacy notices. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

In instances where NFE receives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals via the respective source systems of records' Privacy Act Statements (PASs) and other applicable privacy notices, which describe the choices available to the individual, and obtain implicit or explicit consent with respect to the collection, use, and disclosure of PII. Such record systems include the Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), Personnel Benefits and Enrollment Records (FDIC-30-64-0014), and Personnel Records (SORN 30-64-0015), and are available on the FDIC public-facing website. No additional mitigation actions are recommended.

Section 1.0: Information System/Project Description

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?

NFE contains personal information about the following categories of individuals:

a. **FDIC Employees** (both current and terminated/retired) including full name, EIN, SSN, home address, and other pertinent information related to supporting human resources information processing and payroll (such as salary and wage data, hours worked, and other timesheet information). NFE also maintains financial information related to employee travel and expenses (e.g., voucher totals, expense amounts, accounting string data) in the Travel & Expense (T&E) module.

While not stored in NFE, FDIC Employee Supplemental W-2s are available to employees for viewing and printing through the NFE Supplemental W-2 Self-Service application. The NFE Supplemental W-2 Self-Service application is a custom web application that FDIC employees can access by logging into NFE using their Active Directory ID (AD ID) credentials and clicking on the link for W-2. The employee is then prompted to re-enter their AD ID credentials, which are used to authenticate the employee and to retrieve the employee's name, SSN, and EIN from SPS, which is housed in CHRIS. In turn, these PII elements are used as the key fields to retrieve the employee's Supplemental W-2 from OneSource (eComply) and return it on-screen to the requesting employee. As noted in the first section of the PIA, OneSource is a financial database that is owned and operated by a third-party vendor that assists the FDIC with processing, mailing, and electronically filing tax reporting data.

b. **FDIC Vendors** including name, address, Taxpayer Identification Number (TIN), and bank account number.

c. **FDIC Receivership Claimants/Payees** including claimant name, address, and payment type.

d. **FDIC Payors** (i.e., those who owe funds to FDIC, such as FDIC employees) including name, address, and phone number.

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	☐	☒

PII Element	Yes	No
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: Vendor TIN)	☒	☐

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

Data Source	Description of Information Provided by Source
FDIC Personnel	**FDIC employees** manually enter certain information directly into the system, such as their travel vouchers and expense information. However, employees do not have access to enter their PII/personnel-related data (e.g., name, EIN, address, etc.) directly into NFE. This information is derived from the FDIC Corporate Human Resources Information System (CHRIS) as detailed below. In addition, while not housed on the NFE servers, the SPS web application allows employees to enter reimbursement claims for supplemental payments. Some information within NFE is derived from hardcopy forms completed by FDIC employees (e.g., travel expense reports, notification of relocation, service agreements, etc.) **FDIC supervisors** have access to review and approve/disapprove the travel and expense reports of the employees they supervise. **FDIC DOF personnel** have access to the system to review and update records, as applicable. For example, DOF Travel Specialists may update any records within the T&E module of NFE as appropriate and necessary within the scope of their duties. The Frequent Traveler Lodging Stipend Program (FTLSP) uses information from the T&E modules to determine if an employee qualifies for the stipend. Authorized DOF personnel enter the query results into NFE if the employee qualifies. In addition, DOF Accounts Receivable personnel manually enter payor information and updates into NFE. Note: Vendors and claimants/payees do not directly access or input information into NFE. With limited exceptions, NFE generally receives this information via the system interfaces detailed below. However, in limited cases, and upon request, FDIC Vendor Maintenance personnel manually enter vendor information and updates from the following forms into NFE: Internal Revenue Service (IRS) Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10).
Corporate Human Resources Information System (CHRIS)[12] [Secure File Transfer Protocol (SFTP)]	CHRIS supports FDIC Human Resource (HR)/personnel activities and is FDIC's system of record to request, approve, and track personnel actions that are sent to the USDA National Finance Center (NFC) payroll system for processing. To reduce data redundancy, NFE retrieves FDIC personnel information from CHRIS, such as EIN, name, address, and other pertinent information, but NFE does not retain/store this PII.

[12] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

WebTA[13] (SFTP)	WebTA is a web-based FDIC system that supports the collection, and reporting of time and attendance (TA) data for all FDIC employees. WebTA provides accounting information, as well as employee time and attendance and leave data, to NFE to ensure wages paid to employees are properly recorded on the General Ledger. This data includes employee name, SSN, and timesheet charges for the most recent pay period.
MyEnroll[14] (Manual Download/Upload)	MyEnroll is an external website operated by a third party that allows FDIC employees to self-enroll and update their elections associated with certain Federal and FDIC benefits. FDIC Disbursement staff download from MyEnroll files containing Domestic Partner Program (DPP) data. The DPP data includes: employee ID, full name, tax year, address, annual imputed income, balance year, DPP state, DPP wage, Medicare tax, and Old Age, Survivors, and Disability Insurance (OASDI) tax, as applicable. Disbursement staff request a series of jobs that load the file to SPS where it is combined with the OneSource/eComply file to update DPP fields and imputed income. This process allows employees to receive a single W-2 from SPS.
Dividend Processing System (DPS)[15] (SFTP)	DPS assists FDIC's Division of Resolutions and Receiverships (DRR) with calculating and issuing the appropriate payments to claimants, as well as reconciling those payments with the FDIC's General Ledger. DPS provides dividend checks/wire orders and vendor transactions via secure transmission to NFE for reconciliation and recording in the General Ledger. DPS also sends a list of claimant names and addresses to NFE's Accounts Payable system. This occurs when uninsured deposit claimants and unpaid vendors/payees are set up to receive dividends from the sale of the failed bank's assets.
Structure Information Management System (SIMS)[16] (SFTP)	SIMS maintains all structure data for financial institutions insured, supervised, and monitored by FDIC. Structure data is public in nature and encompasses attribute, classification, and ownership information. SIMS exports institutional demographic data (such as bank name and address) to NFE.
Automated Procurement System (APS) (SFTP)	APS is the FDIC's contract drafting, tracking, and monitoring system. APS provides contract award and contract modification data to NFE, which includes the NFE requisition number, vendor name, contract number, vendor number, vendor address, and vendor phone number. APS sends this data to NFE via a nightly batch job.
Advanced Legal Information System (ALIS)[17] (SFTP)	ALIS is the FDIC's principal system for legal matter management/tracking, budgeting, and invoice processing. ALIS provides NFE with legal-related contract invoices that include vendor profile information, such as the vendor name, address, and phone number.

[13] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[14] FDIC System of Records Notice (SORN) 30–64–0014, Personnel Benefits and Enrollment Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[15] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[16] FDIC System of Records Notice (SORN) 30-64-0013, Insured Financial Institutions Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[17] FDIC System of Records Notices (SORNs) Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015), 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

Warranties Representations Account Processing System (WRAPS)[18] (SFTP)	WRAPS supports FDIC's Division of Resolutions and Receiverships (DRR) with processing and tracking claims made by purchasers of Receivership loans and other related assets under the terms of their loan sales agreements. WRAPS provides NFE with claimant/payee and disbursement records via nightly batch jobs for processing.
Third-Party Financial Institution for Disbursements[19] (Globalscape)	FDIC Accounts Payable produces payment files that are transmitted daily to a third-party financial institution with which FDIC has contracted for purposes of disbursing payments for vendor products and services, for employee travel reimbursements, or to individuals with claims against an FDIC insured institution. The payment files contain PII, including name, address, and bank account, in order to issue payment to vendors, employees and claimants. In turn, the contracted financial institution provides the status of payments to NFE.
General Services Administration (GSA) SmartPay Program Contractor Bank[20] (FTP)	The GSA SmartPay Program contractor bank supplies purchase management and travel card services for the FDIC Corporate Purchase Card (PCard) and Travel Card Programs, handling all aspects of card approval, authorization, and processing. In this capacity, the GSA SmartPay Program contractor bank maintains data related to purchases and travel expenses made by FDIC officials using PCards and/or Travel Cards issued by the bank. The contractor bank provides NFE with a file containing FDIC purchase and travel card transactions for purposes of generating monthly payments and recording expenses.
United States Department of Agriculture (USDA) National Finance Center (NFC)[21] (VPN Tunnel)	NFC provides automated payroll and accounting services to federal agencies. NFC currently serves as the official payroll provider for the FDIC, as well as for other government agencies. NFC transmits post-payroll data to NFE. The post-payroll data includes the output from the WebTA data, along with additional data provided by NFC, such as employee name, home address, and wage/salary. PTAR reformats the NFC data, retrieves EIN and accounting codes/data used to identify and track financial transactions and accounting distributions, and creates the journal entries for posting to the NFE General Ledger. Please note that, in an effort to reduce SSN usage, NFE processes the PTAR reconciliation reports using EIN, rather than SSN. However, NFC does not carry FDIC EINs on its records. Therefore, it is necessary for NFE to retrieve EINs from CHRIS upon receipt of the NFC post-payroll file.
United States General Services Administration (GSA) System for Award Management (SAM)[22]	GSA SAM is the U.S. Federal government's central registrant database for government contractors/vendors. SAM sends vendor information via a batch job to a server, which uploads the file to NFE. PII in the file includes vendor name, banking information, TIN, address, phone number, and email address.

[18] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[19] FDIC System of Records Notice (SORN) 30-64-0012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[20] GSA Privacy Impact Assessment (PIA) for SmartPay Purchase Charge Card Program (September 14, 2020), https://www.gsa.gov/cdnstatic/GSA%20SmartPay%20-US%20Bank_PIA_September2020docx.pdf.

[21] USDA Privacy Impact Assessment (PIA) for NFC (June 8, 2018), https://www.usaid.gov/privacy-policy/pia-summaries/usda-nfc-pps.

[22] GSA Privacy Impact Assessment (PIA) for System for Award Management (SAM) (July 16, 2020), https://www.gsa.gov/cdnstatic/System_for_Award_Management_(SAM)_PIA_July2020docx.pdf.

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

The ATO for NFE was issued on May 29, 2012 and will be 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.

NFE operates under the FDIC Privacy Act SORN 30-64-0012, Financial Information Management Records, which covers financial records including, but not limited to, employee payroll, benefit, and disbursement-related records; contractor and vendor invoices and other accounts payable records; customer records related to accounts receivables; payment records for individuals who were depositors or claimants of failed financial institutions for which the FDIC was appointed receiver; and accounting and financial management records.

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

No, the SORN does not require amendment or revision at this time. Generally, the FDIC conducts reviews 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.

FDIC employees have limited access to NFE to enter certain information, such as their travel vouchers and expense information. The NFE system, as well as forms used to collect information from individual FDIC employees, provide a Privacy Act Statement that describes the authority to collect PII, the purpose for the collection, the intended uses of the information, and the consequences of not providing the information. Additionally, the Privacy Act Statement includes contact information for the FDIC Chief Privacy Officer and applicable SORN details. 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'.

Members of the public whose PII is contained in NFE, such as vendors, claimants and other payees who are owed funds by the FDIC, do not directly access or input information into NFE. With limited exceptions described below, NFE receives their PII, as well as FDIC employee PII, via the system interfaces detailed in Section 1.0 of this PIA.

In instances where NFE imports PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals through the respective Privacy Act Statements (PASs) and System of Records Notices (SORNs) for these source systems. Such record systems include the Financial

Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), Personnel Benefits and Enrollment Records (FDIC-30-64-0014), and Personnel Records (SORN 30-64-0015). The FDIC publishes its SORNs on the FDIC public-facing website, which includes instructions on how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

In instances where NFE ingests PII from non-FDIC systems or entities, including those detailed in Section 1.0, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice of FDIC's uses of this PII.

In addition, upon request, DOF Vendor Maintenance personnel manually enter limited vendor information from the following forms: Internal Revenue Service (IRS) Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10). These forms include Privacy Act Statements that describe the authority to collect PII, the purpose for the collection, the intended uses of the information, and the consequences of not providing the information.

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

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

Privacy Risk Analysis: Related to Transparency

Privacy Risk: NFE generally does not collect PII directly from individual FDIC employees, vendors and claimants/payees who are owed funds by the FDIC. Rather, NFE receives this PII via the system interfaces described in Section 1.0 of this PIA. Therefore, these individuals may not be aware that their data has been utilized or processed by NFE.

Mitigation: In instances where NFE imports PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals through the respective Privacy Act Statements (PASs) and System of Records Notices (SORNs) for these source systems. Such record systems include the Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), Personnel Benefits and Enrollment Records (FDIC-30-64-0014), and Personnel Records (SORN 30-64-0015). The FDIC publishes its SORNs on the FDIC public-facing website, which includes instructions on how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

In instances where NFE ingests PII from non-FDIC systems or entities, including those detailed in Section 1.0, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice of FDIC's uses of this PII. No additional mitigation actions are recommended.

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?

For employees: Individuals are able to access their information by registering for a user account and logging into the system. After logging into the system, individuals have the ability to view information and submissions, but are not able to alter records or data within NFE. After submission of a claim, amending information must be done via contacting a system administrator or via requesting an alteration to the record in the applicable source system.

The FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1031.1. Access procedures for this information system or project are detailed in the SORN(s) listed in Section 2.2 of this PIA. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

For vendors/claimants/payees: Vendors and claimants/payees do not have direct access to NFE. Instead, NFE receives their PII via system interfaces or, in limited cases, via manual entry by DOF personnel as described in Section 1.0. Therefore, in most instances, these individuals should submit requests to access and amend their PII to the originating source/entity that initially collected their information. For example, access and amendment requests from claimants are referred to DRR for processing. Vendor requests to access and amend their vendor registration information/PII are typically referred to GSA SAM. Upon request, FDIC Vendor Maintenance personnel may manually enter/update vendor information in NFE, using the tax forms described in Section 1.0. Additionally, vendors wishing to make amendments to transactional or invoicing information should contact the applicable FDIC Technical Monitor who is responsible for approving their invoices.

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

For employees: Individuals are able to access their information by registering for a user account and logging into the system. After logging into the system, individuals have the ability to make changes to their information with the exception of their PII. To correct their PII/personnel data, employees should contact DOA. In certain cases, after employees have submitted information (e.g., reimbursement claims for supplemental payments), they do not have ability to make further changes to their information. They may contact DOF via telephone or email to make necessary corrections or adjustments to their information.

For vendors/claimants/payees: Vendors and claimants/payees do not provide their PII directly to NFE. Instead, NFE receives this PII via system interfaces or, in limited cases, via manual entry by DOF personnel as described in Section 1.0. Amendments to PII and transactional information can be made by following the procedures outlined in Section 3.1.

Additionally, the FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1031.1. Access procedures for this information system or project are detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-

facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

For employees: The "Notification Procedure" section in the applicable SORN for this system, listed in Section 2.2, provides contact information as well as instructions for individuals to request corrections to their information within the system.

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 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

For vendors/claimants/payees: Vendors and claimants/payees do not provide PII directly to NFE. Instead, NFE generally receives this PII via system interfaces as described in Section 1.0. In such cases, the responsibility to notify individuals falls to the systems/entities at the initial point of collection.

In addition, some vendor information and updates are collected and manually entered by DOF Vendor Maintenance personnel from the following forms: Internal Revenue Service (IRS) Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10). These forms include Privacy Act Statements that describe the authority to collect PII, the purpose for the collection, the intended uses of the information, and the consequences of not providing the information.

In instances where NFE processes vendor PII from non-FDIC systems or entities, including the United States General Services Administration (GSA) System for Award Management (SAM), it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Individual vendors should contact SAM directly to correct any erroneous or inaccurate information. In addition, upon request, FDIC Vendor Maintenance personnel may manually enter/update vendor information in NFE. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice of FDIC's uses of the PII.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: In some cases, NFE derives vendor information, including PII, from third-party sources. Specifically, NFE receives vendor information from the United States General Services Administration (GSA) System for Award Management (SAM), the U.S. Federal Government's authoritative source and central registrant database for government contractors/vendors. The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: In instances where NFE derives PII from GSA SAM, GSA has a responsibility and vested interest in ensuring that the PII it collected is correct to preclude compliance issues with Federal mandates. Namely, GSA SAM, as the U.S. Federal Government's authoritative source and central registrant database for government contractors/vendors, is responsible for ensuring accurate, complete and up-to-date information for entities that register to do business with the U.S. government, in accordance with the Federal Acquisition Regulation (FAR) Subpart 4.11 and Title 2 of the Code of Federal Regulations (2 CFR) Subtitle A, Chapter I, and Part 25. Since GSA SAM originates and maintains the Federal government's authoritative source for vendor registrant data, FDIC refers vendors directly to GSA SAM to correct any erroneous or inaccurate vendor registrant/PII data. Vendors wishing to make amendments to transactional or invoicing information contained in NFE may contact the applicable FDIC Technical Monitor who is responsible for approving their invoices. Additionally, in limited cases and upon request, FDIC Vendor Maintenance personnel may manually enter/update vendor information in NFE, using the tax forms described in the previous section. No additional mitigation actions are recommended.

Section 4.0: Accountability

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

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

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

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

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

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

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and 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 NFE are captured in this PIA, which was 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/about/privacy/index.html.

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

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, Confidentiality Agreements have been completed and signed for contractors who work on the information system or project. 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.

NFE provides system specific training to individuals who will access the system, including quick start guides, job aides, and simulation training materials for various modules in NFE. Additionally, the FDIC Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

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

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

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

Privacy has been integrated within the FDIC Rational Unified Process (RUP) 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 inventory.

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using FOIAExpress.

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?

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 SORNs. FDIC Circular 1360.20 'FDIC Privacy Program' mandates that the collection of PII be in accordance with Federal laws and guidance.

NFE collects and maintains PII pursuant to the following legal authorities: 12 U.S.C. 1819, 12 U.S.C. 1820, and Executive Order 9397.

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: 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 personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

NFE collects only PII that is relevant and necessary to accomplish authorized tasks. NFE does not duplicate files containing PII and uses the minimum elements necessary for legally authorized purposes. Within the application, there are a vast number of inherent controls that prevent any unnecessary data elements from being incorporated. DOF also maintains a workflow review and approval process for any proposed interface or module going into the system in order to be able to identify all data exchange capabilities and requirements.

Additionally, through the conduct, evaluation and review of privacy artifacts,[23] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

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

NFE only collects PII that is directly relevant and necessary to accomplish specified purpose(s). NFE does not duplicate files containing PII and uses the minimum elements necessary for legally authorized purposes. 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 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.

There is currently an effort underway with FDIC Records and Information Management Unit (RIMU) to determine appropriate retention schedules for data contained within NFE. No formal retention schedule(s) have been determined yet.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9. Additionally, detailed guidance is provided to users in the Privacy Section-issued guide titled 'Protecting Sensitive Information in Your Work Area.'

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

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?

Use of sensitive data outside the production environment requires management approval via a waiver. Any production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management, and appropriate controls have been put in place.

As part of NFE's testing efforts within the production environment, NFE has an active, approved waiver for use. PII elements, including SSN, are scrambled within the environment for additional risk mitigation.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: NFE collects and maintains Social Security Numbers (SSNs) for identification and payment/tax related purposes. Privacy best practice is to remove SSN wherever possible.

Mitigation: As SSN is the primary identifier for individuals pertaining to taxes and financial interactions, the data quality benefits of using SSN within the system to ensure accuracy have justified its continued use. Wherever possible, however, NFE utilizes employee identification number in place of SSN.

Privacy Risk: A formal records retention process has not yet been documented for NFE, which could result in records being maintained for a period longer than necessary and enhance the potential for breach of PII in the event of privacy breach and/or security incident.

Mitigation: There is currently an effort underway with FDIC Records and Information Management Unit (RIMU) to determine appropriate retention schedules for data contained within NFE. No formal retention schedule(s) have been determined yet.

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.

NFE employs a number of technical controls to prevent any unnecessary data elements and records from being incorporated into the system. For example, Transfer Control File (TCF) markers are utilized in interfaces between NFE and source systems to prevent duplicate records and ensure data integrity. DOF also maintains a workflow review and approval process for any proposed NFE interfaces or modules in order to identify all data exchange capabilities and requirements. Access in the NFE application is restricted to pages and query access tables via permission lists through a user role assigned based on approvals in ARCS. Further, DOF has taken measures to reduce the use of SSN within the system wherever possible, including removing SSN from 17 PTAR reconciliation reports. Instead, NFE now processes the reports using EIN.

Additionally, 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?

For employees: The information system or project collects PII from manual input and system interfaces as specified in Section 1.2. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

For vendors/claimants/payees: NFE does not collect PII directly from vendors or claimants/payees, but instead receives this PII via system interfaces or, in limited cases, via manual entry as described in Section 1.0.

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. Certain modules within NFE that require the use of PII for processing transactions have automated controls to validate the PII, such as the vendor pre-notification process and the PTAR/CHRIS SSN cross-reference process.

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 the PII. The Office of the Chief Security Officer prescribes 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: NFE does not always collect PII directly from individuals. In some instances, NFE ingests existing unstructured native data from FDIC record systems and other sources for claims and disbursement purposes. As a result, the FDIC does not have the ability to verify and validate, in all cases, the quality and integrity of the PII prior to NFE's ingestion and processing of it.

Mitigation: In instances where NFE processes PII data derived from other sources, it is incumbent upon the source system or entity to verify and validate that the information being shared is accurate, up-to-date and complete. Additionally, NFE employs a number of technical and administrative controls to enhance data quality and integrity. For example, Transfer Control File (TCF) markers are utilized in interfaces between NFE and source systems to prevent duplicate records and ensure data integrity. DOF also maintains a workflow review and approval process for any proposed NFE interfaces or modules in order to identify all data exchange capabilities and requirements. Further, access in the NFE application is restricted to pages and query access tables via permission lists through a user role assigned based on approvals in ARCS. No additional mitigation actions are recommended

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.

For employees: 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.

For vendors/claimants/payees: NFE receives data from third parties as listed in Sections 1 and 9. In addition, some vendor information and updates are collected and manually entered by DOF Vendor Maintenance personnel from the following forms: Internal Revenue Service (IRS) Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10). These forms include Privacy Act Statements that describe the authority to collect PII, the purpose for the collection, the intended uses of the information, and the opportunity to, and consequences of, not providing the information.

In instances where NFE processes PII from non-FDIC systems or entities, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection.

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.

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

For vendors/claimants/payees: NFE receives data from third parties as listed in Sections 1 and 9. In addition, some vendor information and updates are collected and manually entered by DOF Vendor Maintenance personnel from the following forms: Internal Revenue Service (IRS) Form W-9, Request for Taxpayer Identification Number and Certification, and/or Substitute Form W-9 (FDIC 4531/10). These forms include Privacy Act Statements that describe the authority to collect PII, the purpose for the collection, the intended uses of the information, and the opportunity to, and consequences of, not providing the information.

In instances where NFE processes PII from non-FDIC systems or entities, it is incumbent upon the source system or entity to provide any applicable, required notices to the individuals from whom they collected the information.

Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

8.3 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. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORN(s) 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 system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) 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/about/privacy/index.html, instructs viewers to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There is risk related to individual participation for NFE because data is not always collected directly from individuals. Rather, NFE typically receives PII via the system interfaces described in Section 1.0 of this PIA. Therefore, individuals may not be aware and/or have provided explicit consent for the collection and use of their information within NFE.

Mitigation: In instances where NFE derives PII from third-party sources, such as vendor PII from GSA SAM, the FDIC does not have the ability to provide privacy notices or obtain explicit consent prior to its processing of these individuals' PII. Individual vendors should review the relevant third party's privacy notices. Additionally, this PIA and the SORN listed in Section 2.2 serve as notice and implicit consent with respect to the collection, use, and disclosure of PII.

In instances where NFE receives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals via the respective source systems of records' Privacy Act Statements (PASs) and other applicable privacy notices, which describe the choices available to the individual, and obtain implicit or explicit consent with respect to the collection, use, and disclosure of PII. Such record systems include the Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), Personnel Benefits and Enrollment Records (FDIC-30-64-0014), and Personnel Records (SORN 30-64-0015), and are available on the FDIC public-facing website. No additional mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

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

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

NFE collects and uses the employee information described in Section 1 for purposes of performing all employee payment/payroll functions, as well as processing of supplemental payroll and Travel & Expense transactions. Within NFE, PTAR processes and reconciles payroll and timesheet transactions to record General Ledger entries.

NFE maintains the vendor and claimant/payee information described in Section 1 in order to facilitate the automated payment of vendors and claimants/payees on behalf of the FDIC. NFE requires the data for purposes of processing AP payments and reconciling those payments for recording in the General Ledger. Additionally, NFE maintains the vendor's tax information for tax reporting purposes including 1099 reporting.

In addition, the NFE EPM module maintains vendor and employee financial transactions for financial reporting purposes. Note: While not stored in NFE, employees' Supplemental W-2s are accessible to FDIC employees for viewing and printing through the NFE Supplemental W-2 Self-Service application, as detailed in Section 1.0.

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. In addition to Corporate-wide Information Security and Privacy Awareness Training, there is also system-specific training that (among other things) addresses the requirements for protecting sensitive information, including PII. This system-specific training is required for all employees and contractors with more than NFE default access.

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

The system contains security controls that protect NFE application data from unauthorized access. Access to NFE is only granted to those persons within the FDIC specifically authorized by the Corporation. Access levels and permission levels have been established and access is provided only to those persons who have a "need to know" the information contained in the system in order to carry out their official business duties. In accordance with Federal law and policy, NFE has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permission and software controls.

Access to NFE requires manager approval and follows the FDIC's Access Request and Certification System (ARCS) access control procedures. Upon approvals in ARCS, access to the NFE application is granted to pages and query access tables via permission lists through an assigned user role based on the user's job responsibilities.

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. Multiple systems receive data or have access to the data as detailed below in section 9.6.

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?

NFE will not aggregate or consolidate data in order to make privacy determinations or derive new data about individuals.

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.

NFE shares data with the following external systems:

System Name (Acronym)	Transmission Method	Description of Data Provided by NFE
Contractor Financial Institution for Disbursements[24]	SFTP	NFE sends out payments requests (EFTs and checks) through a third-party financial institution with which FDIC has contracted for disbursement purposes. The data elements exported are name, address, banking account, and routing number. The purpose of the export is to provide the contracted financial institution with banking information for vendor payments, expense reimbursements, claimant payments, and employee-related expenses for travel and petty cash.
General Services Administration (GSA) SmartPay Program Contractor Bank[25]	Globalscape	NFE sends a digitally signed (PGP) file to the GSA SmartPay Program contractor bank that includes employee name, EIN, address and last four digits of SSN. The purpose of this file is to send application information to the contractor bank for the establishment of an employee's travel credit card account.
OneSource (eComply)[26]	SFTP	A file from the AP module containing payment information for 1099 tax reporting purposes is sent to FDIC DOF's Receivables, Receipts, and Vendor Maintenance Section as an encrypted email attachment. The staff decrypts the file and uploads the data to OneSource via secure transmission. OneSource is a financial database that is owned and operated by out-sourced service provider Thomson Reuters [Tax & Accounting], a third party vendor that assists FDIC with processing, mailing, and electronically filing tax reporting data. Additionally, a file of FDIC Employee Supplemental Payment information for W-2s and 1099s is created in NFE's SPS module and then securely transmitted via

[24] FDIC System of Records Notice (SORN) 30-64-0012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[25] GSA Privacy Impact Assessment (PIA) for SmartPay Purchase Charge Card Program (September 14, 2020), https://www.gsa.gov/cdnstatic/GSA%20SmartPay%20-US%20Bank_PIA_September2020docx.pdf.

[26] FDIC System of Records Notice (SORN) 30-64-0012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

		HTTPS/SFTP to a Server. The file is manually uploaded to the vendor's website. Additionally, a file of FDIC Employee Supplemental Payment information for W-2s and 1099s is created in NFE's SPS module and then securely transmitted via HTTPS/SFTP to a Server.
Warranties Representations Account Processing System (WRAPS)[27]	SFTP	NFE provides updated accounting data and payment data to WRAPS when invoices are paid via Enterprise Operational Data Store (ENTODS). The transmission method is SFTP. The purpose of the interface is to provide an automated method for publishing the accounting data that facilitates the creation of invoice data from an internal FDIC system and send the data to the AP for payment.
Advanced Legal Information System (ALIS)[28]	SFTP	NFE provides updated accounting data and payment data to ALIS when invoices are paid via Enterprise Operational Data Store (ENTODS). The transmission method is SFTP. The purpose of the interface is to provide an automated method for publishing accounting data elements that facilitate the creation of invoice data and send the data to the AP for payment.
Supplemental Payment System (SPS)[29]	SFTP	NFE provides information to SPS, which is a part of CHRIS, via a nightly batch processing to perform all corporate employee payment functions. *(Note: While SPS is a part of CHRIS, it is also considered a module of NFE and is owned by DOF.)*
Automated Procurement System (APS)	SFTP	NFE provides requisition data that does not include personal information to APS via ENTODS.
Dividend Processing System (DPS)[30]	SFTP	NFE provides updated accounting data and claimant payment data when invoices are paid. NFE publishes the DPS posted journal entry data and TCF via ENTODS.
WebTA[31]	SFTP	NFE provides accounting data to WebTA via ENTODS.

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.

[27] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[28] FDIC Systems of Records Notices (SORNs) Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015), https://www.fdic.gov/about/privacy/records.html.

[29] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[30] FDIC System of Records Notice (SORN) 30-64-0013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

[31] FDIC System of Records Notice (SORN) 30-64-0015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

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 privacy risks associated with use limitation.

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

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

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

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

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

Privacy Risk Analysis: Related to Security

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

Mitigation: No mitigation actions are recommended.