FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment
for
Data Exchange and Portal Applications for Financial Institution Activities

April 11, 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

In conjunction with FDIC's mission of supervising and examining Financial Institutions (FI) for safety and soundness and consumer protection, the FDIC and its business partners are routinely required to transfer and exchange files and information with each other in support of various FDIC business functions. To facilitate this activity, the FDIC has implemented data exchange and portal applications. These applications include, but are not limited to, FDICconnect (FCX) and Enterprise File Exchange (EFX). Users of these applications include FDIC staff, such as examiners, and external users, which include FIs, Technology Service Providers (TSP), state and Federal regulators, and Systemically Important Financial Institutions (SIFI) or FI holding companies and foreign FI organizations (hereinafter referred to as *business partners*).

Data exchange applications provide a secure method to exchange the following types of forms, data, and files between FDIC and its business partners:

- Assessments: Provides electronic delivery of insurance assessment statements and payment information
- Institution information: Allows FIs to submit non-application information such as branch closings
- Post-exam survey: Accepts post-exam surveys for FIs
- Electronic Banking Application: Allows FIs to submit applications that include:
  - Applications pursuant to Prompt Corrective Action
  - Brokered deposit waiver
  - Consent to exercise trust powers
  - Establish or relocate domestic branch or office
  - Extension of time
  - Golden parachute and excess severance payments
  - Reduce or retire capital stock or capital debt
- Supervisory Business Center: Enables FIs to retrieve Reports of Examination and facilitates the submission of documents required by FDIC Rules and Regulations Part 363, Annual Independent Audits and Reporting Requirements
- File Exchange: Enables FDIC and business partners to exchange various files with each other in conjunction with supervision, examination, and compliance activities
- Securities Exchange Act Filings: Provides FIs with the ability to file forms and disclosures required by the Securities Exchange Act of 1934

Portal applications allow external users to securely access FDIC applications, including but not limited to:

- Enterprise Public Inquiry and Complaints (EPIC)[2]
- Financial Institution Diversity Assessment (FIDA)[3]
- Dividend Processing System (DPS)[4]
- FDIC Online Ordering System (OOS)[5]

[1] www.fdic.gov/privacy
[2] See EPIC PIA (November 25 2019) available at https://www.fdic.gov/policies/privacy/index.html
[3] See FDIC Contact and Demographic Information PIA (July 5, 2020) available at https://www.fdic.gov/policies/privacy/index.html
[4] See Determinations and Payouts PIA (December 9, 2020) available at https://www.fdic.gov/policies/privacy/index.html
[5] See FDIC Contact and Demographic Information PIA (July 5, 2020) available at https://www.fdic.gov/policies/privacy/index.html

PRIVACY RISK SUMMARY

In conducting this PIA of data exchange and portal applications, 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:

- Individual Participation
- Transparency
- Data Minimization
- Purpose and Use Limitation

Individual Participation and Transparency Risk:

Privacy Risk: There is a risk that individuals are not aware that their data is collected and provided to FDIC. Business partners collect and provide FDIC with records and documents that are considered to be artifacts in support of FI examination, supervision and compliance activities, and contain PII. As such, the FDIC does not have the ability to provide notice to these individuals prior to the collection and use of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC, and they are not provided with an opportunity to consent to or opt-out of FDIC's collection and use of their information.

Mitigation: The FDIC does not have the ability to provide privacy notices to individuals or provide the opportunity for individuals to consent or opt-out of FDIC's collection of their PII using data exchange and portal applications. In cases where PII is received from business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

Data Minimization Risk:

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

Mitigation: Procedures and controls have been established and implemented to ensure that data is not maintained within data exchange and portal applications in excess of prescribed time constraints. Data exchange and portal applications provide an expiration date/time feature for virtual data rooms used to facilitate data exchanges. The expiration date/time is required to be set to a finite future date when a user creates a virtual data room, with the default being nine months. The system does not retain exchanged information beyond the expiration date set by the FDIC users who create the virtual data rooms.

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond that which 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 to ensure all environments are secured appropriately based on the impact level of the information and the information system.

Purpose and Use Limitation Risk:

Privacy Risk: A potential exists for authorized users of data exchange and portal applications to be provided access to data to which they should not have access.

Mitigation: The FDIC has implemented training for users of data exchange and portal applications to reduce the risk that authorized users are provided access to information to which they should not have access. Additionally, FDIC maintains a breach response program that facilitates the prompt investigation and remediation of such instances.

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?

Data exchange and portal applications provide a secure method to exchange information and files with FDIC business partners that conduct business with the FDIC, and may include information relating to FI examinations, FI lookup/status data, FI assessment invoices, FI application status, FI post exam survey information, FI profile information, and SEC filings. The information and files exchanged could contain various types of PII related to FI customers and FI employees, as indicated in the following table.

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) (non-work)	☒	☐
Email Address (non-work)	☒	☐
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: _____)	☐	☐

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

Data Source	Description of Information Provided by Source
Financial Institutions	Financial Institution and customer information and requests. This includes SIFIs or FI holding companies and foreign FI organizations.
State and Federal Banking Regulators	Information relating to FI examinations, which may include PII of FI employees and/or FI customers.

Data Source	Description of Information Provided by Source
Structure Information Management System (SIMS)[6]	FI lookup and status data, which includes the PII of FI officers.
Assessment Information Management System (AIMS)[7]	Insurance assessment invoices and other correspondence, including the names and email addresses of FI points of contact, in support of the invoicing and collection of deposit insurance assessments.
Virtual Supervisory Information on the Net (ViSION)[8]	Select application forms from FIs are received and processed through to ViSION, which may include the PII of FI employees.
Securities Exchange Act Filings System[9]	Securities disclosure filings, which include the PII of FI directors, officers, and principal shareholders.
FDIC Active Directory	User account information to facilitate access to data exchange and portal applications.

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

Data exchange and portal applications operate within the boundaries of Cloud.gov (ATO date of 8/7/20) and FDICconnect (ATO date of 3/17/2013), and are periodically reviewed as part of the FDIC's 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 does this information system or project operate? Provide number and name.

Data exchange and portal applications do not operate as Privacy Act systems of records, nor do they require an alteration to an existing system of records. Data exchange and portal applications process information imported from other FDIC record systems that is collected and maintained for purposes related to other business processes for which there are currently Privacy Act systems of records in existence. Such record systems include Financial Institution Investigative and Enforcement Records (30-64-0002) and Beneficial Ownership Filings (30-64-0025).

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

Not applicable. Data exchange and portal applications do not operate as Privacy Act systems of records.

[6] See FDIC Contact and Demographic Information PIA (July 5, 2020) available at https://www.fdic.gov/policies/privacy/index.html

[7] See FDIC Contact and Demographic Information PIA (July 5, 2020) available at https://www.fdic.gov/policies/privacy/index.html

[8] See ViSION PIA (March 28, 2021) available at https://www.fdic.gov/policies/privacy/index.html

[9] FDIC System of Records Notice (SORN) 30-64-0025, Beneficial Ownership Filings (Securities Exchange Act), 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/index.html

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.

Not applicable. Data exchange and portal applications do not operate as Privacy Act systems of records.

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: There is a risk that individuals are not aware that their data is collected and provided to FDIC. Business partners collect and provide FDIC with records and documents that are considered to be artifacts in support of FI examination, supervision and compliance activities, and contain PII. As such, the FDIC does not have the ability to provide notice to these individuals prior to the collection and use of their PII.

Mitigation: Data exchange and portal applications do not operate as Privacy Act systems of records. Therefore, notice, in the form of a Privacy Act Statement or SORN, is not required. In instances where business partners provide FDIC with records containing PII, it is incumbent upon the business partners to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection.

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?

Data exchange and portal applications do not have procedures for individual access since they do not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act individual access requirement. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC, which may include information about FI customers or FI employees collected in conjunction with FDIC's examination, supervision and compliance authorities. Individuals should contact the appropriate FI directly for access to their personal information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

In cases where data exchange and portal applications facilitate the transport or exchange of information related to FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 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 Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

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

Data exchange and portal applications do not have procedures to correct inaccurate or erroneous information. They do not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act redress requirement. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC. Individuals should contact the appropriate FI directly to correct any inaccurate or erroneous information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

In cases where data exchange and portal applications facilitate the transport or exchange of information related to FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 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?

Data exchange and portal applications do not notify individuals about the procedures for correcting their information. They do not operate as Privacy Act systems of records and, therefore, are not subject to the Privacy Act redress requirement. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC. Individuals should contact the appropriate FI directly to correct any inaccurate information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: Data exchange and portal applications do not have procedures or provide notification to individuals about how to access or amend their information.

Mitigation: Data exchange and portal applications do not operate as Privacy Act systems of records, and are not subject to the Privacy Act redress requirement. Instead, information is collected and provided to FDIC by its business partners. Records and documents provided to FDIC are considered to be artifacts in support of FI examination, supervision and compliance activities. The FIs that initially collect PII that is provided to the FDIC using data exchange and portal applications have a vested interest in ensuring that the PII they collect is correct to preclude compliance issues with Federal mandates, such as the Fair Credit Reporting Act.

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, 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 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 data exchange and portal applications are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). The PIA for data exchange and portal applications is publicly available at: 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 for/to data exchange and portal applications 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 versions of data exchange and portal applications; however, if there is need for contractor administrator-level support, some contractors may be granted access to the production version and data of the applications.

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?

Contractor Confidentiality Agreements have been completed by contractors who work on data exchange and portal applications. 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, 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 program in accordance with OMB Circular A-130. Data exchange and portal applications do not operate as systems of records.

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

With respect to internal FDIC users, user rules and responsibilities are defined for data exchange and portal applications and require new users to accept them as part of the user provisioning process. The rules describe user responsibilities and expected behavior with regard to information and information system usage associated with data exchange and portal applications and NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

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.

With respect to FI users, FDIC defines FI Coordinator rules and responsibilities and new coordinators are required to accept them as part of the user provisioning process. The rules describe Coordinator responsibilities and expected behavior with regard to information and information system usage, including the handling of sensitive information and PII. FDIC obtains electronic acknowledgments from coordinator applicants indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the information and the information system.

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 SAOP Report, as required by FISMA; reports to the CISO, meetings with the SAOP and CISO; Information Security Manager's 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 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?

Not applicable. Data exchange and portal applications do not operate as Privacy Act systems of records.

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?

Not applicable. Data exchange and portal applications do not operate as Privacy Act systems of records.

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

Not applicable. Data exchange and portal applications do not operate as Privacy Act systems of records.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for data exchange and portal applications.

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 PII are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of SORNs. FDIC Circular 1360.20 "FDIC Privacy Program" mandates that the collection of PII be in accordance with Federal laws and guidance. Data exchange and portal applications maintain PII pursuant to the following legal authority: 12 U.S.C. 1819 and 12 U.S.C. 1820.

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Data Minimization

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

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

The PII elements contained within data exchange and portal applications are relevant and necessary to support various FDIC business functions, including ongoing examination, supervision and compliance activities, and are dictated on FDIC business requirements.

Additionally, through the conduct, evaluation and review of privacy artifacts,[10] 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?

FDIC does not collect data directly from individuals. Rather, data is provided by FDIC business partners that conduct business with the FDIC. The PII elements contained within data exchange and portal applications are relevant and necessary to support various FDIC business functions, including ongoing examination, supervision and compliance activities, and are dictated by FDIC business requirements.

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.

By design, data exchange and portal applications are not data repositories and are not subject to Privacy Act system of records requirements. Data exchange and portal applications provide an expiration date/time feature for the virtual data rooms used to facilitate data exchanges. The expiration date/time is required to be set to a finite future date when a user creates a virtual data

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

room. The system does not retain exchanged information beyond the expiration date set by the FDIC users who create the virtual data rooms.

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.

Privacy Risk Analysis: Related to Data Minimization

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

Mitigation: Procedures and controls have been established and implemented to ensure that data is not maintained within data exchange and portal applications in excess of prescribed time constraints. Data exchange and portal applications provide an expiration date/time feature for virtual data rooms used to facilitate data exchanges. The expiration date/time is required to be set to a finite future date when a user creates a virtual data room, with the default being nine months. The system does not retain exchanged information beyond the expiration date set by the FDIC users who create the virtual data rooms.

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond that which 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 to ensure all environments are secured appropriately based on the impact level of the information and the information system.

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.

Data is collected from FDIC business partners that conduct business with FDIC. As such, the FDIC relies on them to provide accurate data. 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?

Individuals do not directly provide data and may not opt out of providing their personal information to data exchange and portal applications. The data is not collected directly from individuals. Rather, the data is provided by the FDIC business partners that conduct business with the FDIC.

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

Data is collected from FDIC business partners that conduct business with FDIC. As such, the FDIC relies on them to provide accurate and current data. See the response to Question 6.4 regarding the disposition of outdated information.

The FDIC reviews privacy artifacts to ensure adequate measures are taken 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 the PII. The Office of the Chief Information 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: There are no identifiable risks associated with data quality and integrity for data exchange and portal applications.

Mitigation: No 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.

Data exchange and portal applications do not operate as Privacy Act systems of records and do not collect PII directly from individuals. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC.

The FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice of

the information collection. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

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.

Data exchange and portal applications do not collect PII directly from individuals. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.3 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 obtain direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update this PIA as necessary.

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.

Data exchange and portal applications do not collect PII directly from individuals. Rather, data exchange and portal applications receive data provided by FDIC business partners that conduct business with the FDIC. The FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII using data exchange and portal applications. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

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

The FDIC Privacy Program website, https://www.fdic.gov/policies/privacy/index.html, instructs individuals 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 the PII received and maintained by data exchange and portal applications is not collected directly from individuals, there is a risk that these individuals will not know how their data is being used or shared. Additionally, individuals are not provided with an opportunity to consent to or opt out of the FDIC's collection and use of their PII.

Mitigation: Data exchange and portal applications do not collect PII directly from individuals. Rather, data is collected and provided by business partners that conduct business with the FDIC. The FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII using data exchange and portal applications. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice 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 FDIC developed data exchange and portal applications to facilitate secure electronic communication with FDIC business partners that conduct business with FDIC. FDIC business partners use data exchange and portal applications to transfer data, forms and files, and to securely access other FDIC applications.

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.

The Program Managers and Data Owners of data exchange and portal applications and the systems sharing data with data exchange and portal applications are responsible for the management and decision authority over their specific area of corporate data. The 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.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized purposes internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information." 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.

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

With respect to internal FDIC users, FDIC business divisions are responsible for establishing and promulgating the procedures for controlling access to the data transmitted via data exchange and portal applications. Data exchange and portal applications provide controls for auditing who accesses information via data exchange and portal applications. Access to the data is restricted on a "need to know" basis, in conjunction with Active Directory group membership. The user profiles associated with data exchange and portal applications are based on the user's job requirements, managerial decisions, and dependent on the purpose for which access to the data is needed. Access requires management approval, and is facilitated using the FDIC's Access Request and Certification System (ARCS), which is used to grant, manage and monitor access by FDIC internal users to data exchange and portal applications.

With respect to FI users, FIs must apply to FDIC to participate and designate someone as a Coordinator for their institution. The Coordinator must register and become "associated" with their institution. Coordinators approved by the Insured Institution's Authorizing Official can then approve others to be authorized to perform transactions. Coordinators must complete a coordinator registration form, available from the FCX Helpdesk; and complete their online registration through the FDICconnect.gov FI registration module. Coordinators authorize users within their FIs, and the users subsequently complete their online registration through the FDICconnect.gov user registration module. All FI users are reviewed and verified by the FDIC Division of Risk Management Supervision (RMS) prior to completion of the registration process. Once registered, processes are in place to manage and monitor access. Access to the data is restricted on a "need to know" basis, in

conjunction with Active Directory group membership and Extranet Identity Management (EIDM) authentication. EIDM facilitates two-factor authentication for external users accessing FDIC applications.

With respect to state and Federal regulator users, FDIC business divisions are responsible for establishing and promulgating the procedures for controlling access to the data transmitted via data exchange and portal applications. Access to the data is restricted on a "need to know" basis, in conjunction with Active Directory group membership and EIDM two-factor authentication. A user's profile is based on the user's job requirements, managerial decisions, and dependent on the purpose for which access to the data is needed. Access requires approval by authorized FDIC staff, and is facilitated and monitored though the provisioning of access using FDIC's ARCS.

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. User account information is exchanged between FCX and other applications in conjunction with the role of FCX as a portal for the following FDIC applications: Enterprise File Exchange, Enterprise Public Inquiry and Complaints, Financial Institution Diversity Assessment, and the FDIC Online Ordering Solution. Additionally, the following internal applications receive data through data exchange and portal applications.

Internal FDIC Information System	Description of Data
Assessment Information Management System (AIMS)	Insurance assessment invoices and other correspondence, including the names and email addresses of FI points of contact, is obtained from AIMS in support of the invoicing and collection of deposit insurance assessments.
Virtual Supervisory Information on the Net (ViSION)	Select application forms from FIs are received and processed through to ViSION, which may include the PII of FI employees.
Structure Information Management System (SIMS)	FI lookup and status data is obtained from SIMS. SIMS maintains structure information for financial institutions insured, supervised and monitored by FDIC, and includes the PII of FI officers.
System of Uniform Reporting of Compliance and CRA Exams (SOURCE)	Compliance Post Examination Surveys completed for FIs.
Securities Exchange Act Filings System	Securities disclosure filings required by the Securities and Exchange Act of 1934.
Extranet Identity Management (EIDM)	Facilitates two-factor authentication for external users accessing FDIC applications through data exchange and portal applications.

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.

Data exchange and portal applications do not operate as systems of records and do not provide information to external systems via system interconnections. However, authorized users of data exchange and portal applications include FDIC business partners that authenticate to the systems which may provide access to PII maintained within data exchange and portal applications. Memorandums of Agreement exist between FDIC and those entities that define the purpose, use and restrictions on data shared.

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 of 1974, 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 Purpose and Use Limitation

Privacy Risk: A potential exists for authorized users of data exchange and portal applications to be provided access to data to which they should not have access.

Mitigation: The FDIC has implemented training for users of data exchange and portal applications to reduce the risk that authorized users are provided access to information to which they should not have access. Additionally, FDIC maintains a breach response program that facilitates the prompt investigation and remediation of such instances.

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 conducts an evaluation of information in the systems to ensure it is the same as in the PIAs 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?

The FDIC has implemented training for users of data exchange and portal applications to reduce the risk of that authorized users are provided access to information to which they should not have access. In the event that a privacy incident occurred, it would be reported, investigated and remediated in accordance with 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.