



**Privacy Impact Assessment
for
Enterprise File Exchange (EFX)**



PIA-FDIC-1238

July 9, 2019

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's public-facing website,¹ which describes FDIC's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The FDIC and its business partners are routinely required to transfer and exchange files and information with each other in support of FDIC's ongoing supervision and examination activities. The Enterprise File Exchange application (EFX) will help address the enterprise need for an improved file transfer and exchange capability between FDIC staff, such as examiners, and their business partners, which includes Financial Institutions (FI), Technology Service Providers (TSP), state regulators, and non-bank entities. EFX's long term goal is to provide all FDIC users with a mechanism to securely transfer files to and from business partners.

The initial pilot phases of EFX will provide authorized users from the FDIC Division of Risk Management Supervision (RMS) and the FDIC Division of Depositor and Consumer Protection (DCP) a secure method to exchange files with a select subset of business partners. The exchange of files and information are needed to support FDIC's mission of supervising and examining FIs for safety and soundness and consumer protection. EFX will be hosted on the Cloud.gov platform that is operated by the Office of 18F, a part of the General Services Administration (GSA). Access to EFX will be provided to pilot users via a secure URL and as a menu option from the FDICconnect (FCX) menu, which will provide a link to the secure URL. FCX currently provides a secure channel for FDIC business partners to conduct business with the FDIC via the Examiner File Exchange (EFE) transaction function and the Secure File Exchange (SFE) function. The initial pilot phases of EFX will replicate the EFE and SFE functionality currently available in FCX, and then replace those functions when fully implemented.

EFX is integrated with the FDIC's Enterprise Identity Management application (EIDM), which provides authentication, authorization and account management for external users accessing FDIC applications. EFX external users will be authenticated using EIDM.

PRIVACY RISK OVERVIEW

In conducting this PIA, we identified potential privacy risks, which are outlined below. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks are categorized within the following privacy functional areas:

- Access and Amendment
- Accountability
- Data Minimization
- Use Limitation

Access and Amendment Risk: EFX does not collect information directly from individuals. Instead, information is provided to FDIC by its business partners. The records and documents provided by business partners to FDIC are considered to be artifacts in support of FI examination, supervision and compliance activities. Permitting individuals to change that information could impact the integrity of the examination,

¹ www.fdic.gov/privacy

supervision and compliance activities. FDIC relies upon the entities that initially collected the PII to ensure that the PII is correct.

Recommended Mitigation: The FIs that initially collect PII that is exchanged using EFX 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. No additional mitigation actions are recommended.

Accountability Risk: Currently, EFX users must be approved users of the FCX application prior to being approved as users of EFX. While FDIC internal users and external FI users are provided training and/or are made aware of rules and responsibilities when handling sensitive information, including PII, when being authenticated as FCX users, state regulators are not currently provided this training and/or awareness, which could result in those users not being fully aware of their responsibilities when handling and safeguarding PII. Additionally, there is no annual requirement for external FI users and state regulator users to complete training and/or review the rules and responsibilities, which could result in users not being fully aware of their responsibilities when handling and safeguarding PII.

Recommended Mitigation: FDIC is working to provide EFX-specific training to all EFX users when they are authenticated as EFX users and on an annual basis thereafter or to present a banner when users access EFX that describes the user's information security and privacy responsibilities with respect to their access and use of EFX.

Data Minimization Risk: A formal records retention schedule or process has not yet been documented for EFX, 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.

Recommended Mitigation: FDIC business stakeholders are working with the Records and Information Management Unit (RIMU) to formally document requirements related to the maintenance, retention, and disposition of EFX records.

Use Limitation Risk: Manual business processes are used by FDIC to manage and monitor access by external FI users, however, their need for access may not be reviewed and validated on a periodic basis, which could result in users having access to data shared within EFX when they no longer have a business need.

Mitigation: FDIC should formally review and validate EFX external users on an annual or other periodic basis.

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?

EFX provides a secure method to exchange files with FDIC business partners that conduct business with the FDIC. The files 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Place of Birth	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Social Security Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother's Maiden Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Home Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number(s) (non-work)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address (non-work)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

PII Element	Yes	No
Employee Identification Number (EIN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Driver's License/State Identification Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Education Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Criminal Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Military Status and/or Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Investigation Report or Database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other (Specify: _____)	<input type="checkbox"/>	<input type="checkbox"/>

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

Data Source	Description of Information Provided by Source
FIs	FI information and requests and FI customer information.
State Banking Regulators	Information relating to FI examinations, which may include PII of FI employees and/or FI customers.
Technology Service Providers	FI information and requests; and FI customer information, on behalf of FIs.
Non-bank entities	Information from companies or other non-bank entities, which may include PII of employees and/or customers. Non-bank entities could include Systemically Important Financial Institutions (SIFI) or FI holding companies and foreign FI organizations.
FCX-EFE	FI profile information is imported from FCX-EFE. This information includes FI users who have registered for FCX and includes email address and phone number.

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

EFX will operate within the boundary of Cloud.gov. The ATO for Cloud.gov was updated on 3/29/2019 to include EFX.

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.

EFX does not operate as a Privacy Act System of Records.

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

EFX does not operate as a Privacy Act Systems of Records and its use does not require alteration to any existing system of records notice.

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.

A Privacy Act Statement is not required. Data is not collected directly from individuals. Rather, data is provided by FDIC business partners that conduct business with the FDIC. FDIC requires this data to fulfill its mission and mandated obligations as regulator, receiver and insurer of FIs; therefore, no opt-out is provided.

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 webpage located at www.fdic.gov/privacy contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Section Chief, and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There are no identifiable risks associated with openness and transparency for EFX.

Mitigation: No 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?

EFX receives 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 and supervision authorities. Individuals should contact the appropriate FI directly for access to their personal information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

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

EFX receives 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, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

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

EFX receives 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, 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: EFX does not collect information directly from individuals. Instead, information is provided to FDIC by its business partners. Records and documents provided to FDIC by its business partners are considered to be artifacts in support of FI examination, supervision and compliance activities. Permitting individuals to change that information could impact the integrity of the examination, supervision and compliance activities. FDIC relies upon the entities that initially collected the PII to ensure that the PII is correct.

Mitigation: The FIs that initially collect PII that is exchanged using EFX 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. 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 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 EFX 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?

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

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

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

Yes, Contractor Confidentiality Agreements have been completed by contractors who work on EFX. However, contractors will not have access to individuals' PII. Additionally, privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

Currently, EFX users are required to be authenticated users of the FCX application. With respect to internal FDIC users, user rules and responsibilities are defined for FCX and require new users to accept them as part of the user provisioning process. The rules describe FCX user responsibilities and expected behavior with regard to information and information system usage; and Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations. Signed acknowledgments are obtained from users.

With respect to FI users, FI Coordinator rules and responsibilities are defined 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. Electronic acknowledgments are obtained 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.

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; monthly reports to the CISO, monthly meetings with the SAOP and CISO; monthly 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?

This question is non-applicable since EFX does not operate as a system 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?

This question is non-applicable since EFX does not operate as a system 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?

This question is non-applicable since EFX does not operate as a system of records.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: While FDIC internal users and external FI users are provided training and/or are made aware of rules and responsibilities when handling sensitive information, including PII, when being authenticated as FCX users, state regulators are not currently provided this training and/or awareness, which could result in those users not being fully aware of their responsibilities when handling and safeguarding PII. Additionally, there is no annual requirement for external users to complete training and/or review the rules and responsibilities, which could result in users not being fully aware of their responsibilities when handling and safeguarding PII.

Mitigation: FDIC is working to provide EFX-specific training to all EFX users when they are authenticated as EFX users and on an annual basis thereafter or to present a banner when users access EFX that describes the user's information security and privacy responsibilities with respect to their access and use of EFX.

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.

EFX may be used to exchange Privacy Act Records from existing FDIC Privacy Act Systems of Records between FDIC staff and FDIC business partners in connection with their various Corporate and examination job responsibilities. FDIC EFX users are responsible for ensuring there is coverage under the appropriate System of Records Notice for the data exchanged/maintained and ensuring that appropriate procedures are followed.

EFX maintains PII pursuant to the following legal authority:

Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Data Minimization

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

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

The PII elements contained within EFX are relevant and necessary to support the examination of FIs and are dictated based on the requirements associated with the examination of those institutions. Additionally, through the conduct, evaluation and review of privacy artifacts, 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?

Data is not collected directly from individuals. Rather, data is provided by FDIC business partners that conduct business with the FDIC. The PII elements contained within EFX support the examination of FIs and are dictated based on the requirements associated with the examination of those institutions. Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that 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 a periodic 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.

EFX provides an expiration date/time feature for the virtual room that is required to be set to a finite future date when a user creates a virtual data room. The system does not retain exchanged information beyond the expiration date set by the FDIC users who create the virtual data rooms.

FDIC business stakeholders are working with the FDIC Records and Information Management Unit (RIMU) to formally document requirements related to the maintenance, retention, and disposition of EFX records.

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

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 or process has not yet been documented for EFX, 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: FDIC business stakeholders are working with RIMU to formally document requirements related to the maintenance, retention, and disposition of EFX records.

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.

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 EFX. Data is not collected directly from individuals. Rather, 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.

Since EFX receives PII provided by FDIC business partners that conduct business with the FDIC, the FDIC relies upon the entities that initially collected the PII to ensure that the PII is correct. The FIs that initially collect PII that is exchanged using EFX 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.

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 configures administrative and technical controls for the system or project based on the FIPS 199 determination.

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: Data is not collected directly from individuals. Rather, data is provided by the FDIC business partners that conduct business with the FDIC.

Mitigation: Since the FDIC does not use any information provided by FDIC business partners to deprive an individual of a right or benefit, the privacy-related data quality and integrity risks associated with data exchanges between those entities and the FDIC are minimal. 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.

The system or project receives data from FDIC business partners and from the existing FCX system via the same stakeholders. 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 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.

EFX receives data from FDIC business partners, and from the existing FCX system via the same stakeholders. 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 get 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.

EFX receives data from FDIC business partners and from the existing FCX system via the same stakeholders. 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.

8.5 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 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: There are no identifiable risks associated with individual participation for EFX.

Mitigation: No mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

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

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

The intended use of the data above is to support ongoing RMS/DCP examination, supervision, and compliance activities. FDIC business partners will use EFX to upload requested documentation to the system for FDIC assessment and review.

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 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.

Within FDIC, RMS and DCP Program Managers/Data Owners, Technical Monitors, Oversight Managers, and Information Security Managers (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by the FDIC data protection rules that are outlined in the FDIC's Information Security and Privacy Awareness training course, which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

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 EFX. The EFX platform provides controls for auditing who accesses information via EFX. Access to the data is restricted on a "need to know" basis, in conjunction with Active Directory group membership and EIDM integration. An EFX 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 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 EFX.

With respect to Insured Institution users, access is currently facilitated through the FCX application. Insured Institutions 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 strictly from the FCX Helpdesk; and complete their online registration through the registration system at FDICconnect.gov. Coordinators authorize users; all authorized users must complete the online registration. Manual business processes are in place to manage and monitor access by FDIC external users of EFX.

With respect to state regulators and non-bank entities, FDIC business divisions are responsible for establishing and promulgating the procedures for controlling access to the data transmitted via EFX. The EFX platform provides controls for auditing who accesses information via EFX. Access to the data is restricted on a "need to know" basis, in conjunction with Active Directory group membership and EIDM integration. An EFX 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 through the provisioning of Extranet access using the 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. FI Profile information and user information is imported from FCX-EFE. The FI Profile information includes the FI user's account information, name, email, phone number, and association with one or more institutions via certificate number. All of this information originates in FCX-EFE, and is imported to EFX to leverage the existing account information and associate users with their correct institutions in EFX.

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, the information system or project will not aggregate or consolidate data in order to make 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.

EFX does not operate as a system of records and does not provide information to external systems via system interconnections. However, authorized EFX users include FDIC business partners that authenticate to the system which may provide access to PII maintained within EFX. A Memorandum of Agreement exists between FDIC and those entities that defines the purpose, use and restrictions on data shared.

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 and the consequences of unauthorized use or sharing of PII.

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: Manual business processes are used by FDIC to manage and monitor access by external FI users, however, their need for access may not be reviewed and validated on a periodic basis, which could result in users having access to data shared within EFX when they no longer have a business need.

Mitigation: FDIC should formally review and validate EFX external users on an annual or other periodic basis.

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 a semi-annual basis, FDIC conducts 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 for EFX.

Mitigation: No mitigation actions are recommended.

Approval Signature

7/22/2019

X Howard Whyte

Howard Whyte
Chief Privacy Officer
Signed by: HOWARD WHYTE