



**Privacy Impact Assessment (PIA)
for
FDICLearn II**



March 31, 2022

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website¹, 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

FDIC's Corporate University (CU) is the agency's training and development division. It supports the FDIC mission by providing high-quality, cost-effective continuous learning and development. To meet its mission, CU is developing FDICLearn II as the central system to track training for both FDIC employees and external learners such as state banking employees and foreign bank representatives. The system is also used to track career development, certifications, continuing education, and learner skills and competencies. This system is the official record for training taken at FDIC. The system will also house training completion records from other third-party training portals to which FDIC employees have access.

Individuals log in to FDICLearn II using either single sign on (FDIC employees) or two factor authentication (external users). FDIC employees have their information pre-populated into FDICLearn II through a data feed from the FDIC's human resources system. External users must submit an account request providing their name, organization, and email to generate an account. External users accessing the system will be required to download an authenticator application on their mobile device to access the system. FDIC will not provide any information to the authenticator. FDIC will provide the user with a QR code unique to user's name and email address so they can begin generating codes.

Once logged into the system, users will be able to access a variety of training courses, including mandatory and other training content that may be of interest to the user. Users can view assigned training paths, completed courses, pending courses, courses in progress, as well as the completion history for external training portals to which FDIC employees have access.

PRIVACY RISK SUMMARY

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

- Transparency;
- Minimization;
- Data Quality and Integrity; and
- Individual Participation

¹ www.fdic.gov/privacy

Transparency Risks:

Privacy Risk: There is a risk that FDIC employees may be unaware that a subset of their human resources data is being transferred from FDIC's human resources system and repurposed for learning management.

Mitigation: This risk is partially mitigated through the publication of this PIA. FDIC employees and contractors are made aware of mandatory training requirements during the onboarding process and pre-populating with data from the authoritative source facilitates this process.

Privacy Risk: There is a risk that external users may be unaware that they are providing information to a third-party when using the required authentication mechanism.

Mitigation: This risk is mitigated by the requirement for external users to download an app that is clearly marked as belonging to a third party.

Minimization Risks:

Privacy Risk: There is a risk that FDICLearn II may maintain more information than necessary to maintain learner profiles, determine and assign training requirements, and maintain training histories.

Mitigation: FDIC mitigates this risk by regularly reviewing the data maintained in this system to ensure that only the minimum information necessary is kept. FDICLearn II requires basic information related to the learner to operate the system and maintain an official record for training.

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

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or use synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Data Quality and Integrity Risk:

Privacy Risk: There is a risk that the training records provided by the third-party providers is inaccurate.

Mitigation: FDIC extracts completion records from third-party providers and uploads those records in FDICLearn II. Depending on the third party training platform, FDIC updates FDICLearn between daily and monthly. If there are inaccuracies in the records provided by the third-party platform, users will need to contact the third party provider to update their training history. The updated record will then be accurately reflected in FDICLearn II at the next scheduled refresh.

Individual Participation Risk:

Privacy Risk: There is a risk that a non-FDIC user may be unaware that their information was passed to FDIC to create a FDICLearn II account, and therefore did not provide consent prior to account creation.

Mitigation: FDIC would not be aware of interactions between employers and employees. Employers should provide notice to employees prior to submitting their information to FDIC.

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?

FDICLearn II requires information about individuals who are taking FDIC training to determine training requirements and maintain training history. FDICLearn II maintains the following information:

- Full Name: First, Middle and Last name
- Employee Identification Number
- Email Address
- Job Title
- Office or Division
- Grade
- Department Name
- Federal Region: Location
- Paygroup
- Job Code
- Employment Status
- Hire Date
- Grade Entry Date
- Training History

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Place of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Social Security number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother's Maiden Name	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Home Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Phone Number(s)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Driver's License/State Identification Number	<input type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" 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 type="checkbox"/>	<input checked="" type="checkbox"/>
Other (Specify: _____)	<input type="checkbox"/>	<input checked="" 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
FDIC's human resources system	Employee Identification Number Full Name: First, Middle, and Last Name Job Title Office or Division Grade Department Name Federal Region: Location Paygroup Job Code Employment Status Hire Date Grade Entry Date
Active Directory	Network Identification Number Email Address
External Users	Full Name: First and Last name Organization Email address

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

The ATO was issued on March 29, 2022 and will be periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

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

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

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

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

FDIC-007 FDIC Learning and Development Records provides SORN coverage for this system. This SORN describes FDIC's collection and use of training information from current and former employees, as well as other individuals who have attended or completed training conducted or sponsored by FDIC.

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

No. This system does not require the collection of information or uses beyond what is covered by the FDIC-007 FDIC Learning and Development SORN.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to

individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

FDIC provides a Privacy Act Statement to users at the entry point to the system. However, FDIC pre-populates information about FDIC employees from FDIC's human resources system prior to the employee's first access to the system. FDIC uses the information from FDIC's human resources system to generate an account for each employee. As external users proactively provide an account request by email to FDIC, or have a request sent on their behalf, external users do not receive a Privacy Act Statement prior to FDIC's collection of their account creation information. The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1 'FDIC Forms Management Program.'

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

The FDIC Privacy Program page provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that FDIC employees may be unaware that their information is pre-populated into FDICLearn II.

Mitigation: This risk is partially mitigated through the publication of this PIA. FDIC employees and contractors are made aware of mandatory training requirements during the onboarding process and pre-populating with data from the authoritative source facilitates this process.

Privacy Risk: There is a risk that external users may be unaware that they are providing information to a third-party when using the required authentication mechanism.

Mitigation: This risk is mitigated by the requirement for external users to download an app that is clearly marked as belonging to a third party.

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?

When logged into FDICLearn II, users may view their profile information. Additionally, the FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1360.20. Access procedures for this information system or projected are detailed in the SORN listed in Question 2.2 of this PIA. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

Users may not edit their information directly in FDICLearn. Individuals must contact the FDIC Helpdesk for assistance with correcting inaccurate information in the source system, which will subsequently update FDICLearn II. Additionally, the FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN listed in Question 2.2 of this PIA.

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

FDICLearn II will include Frequently Asked Questions and training aids, which will direct individuals to contact the FDIC Helpdesk for assistance in correcting their information. Additionally, The FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users, the procedures for which are published in the SORN listed in Section 2.2 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1360.20.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable risks associated with access and amendment for FDICLearn II.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

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

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

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

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

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

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

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

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

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, www.fdic.gov/privacy/.

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

FDIC will use contractor support to design, implement, and maintain FDICLearn II. Due to contractors' access to PII, contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

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

Yes, a Confidentiality Agreement has been completed and signed for contractors who work on the information system or project. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

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

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates,

and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

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

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

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

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

The system does not maintain an accounting of disclosures. FDIC does not share information from FDICLearn II with any external parties.

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

The system does not maintain an accounting of disclosures. FDIC does not share information from FDICLearn II with any external parties.

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

The system does not maintain an accounting of disclosures. FDIC does not share information from FDICLearn II with any external parties.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for FDICLearn II.

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).

12 U.S.C. 1819 is FDIC's authorizing statute. Employees must be properly trained to accomplish the FDIC's statutory mission. As part of its mission, FDIC also provides training to partners, such as state banking employees and foreign bank representatives.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with authority for FDICLearn II.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

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

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

FDICLearn II collects the minimum information necessary to maintain a learner profile, determine and assign training requirements, and maintain a training history. Additionally, through the conduct, evaluation and review of privacy artifacts,² 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?

As FDIC's central repository for training records, FDICLearn II only maintains information relevant to maintaining a learner profile, determining and assigning training requirements, and maintaining a training history. 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 semi-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.

FDIC is in the process of updating its learning management retention schedule. Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with NARA guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9.

² Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Record Notices (SORNs).

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

The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that FDICLearn II maintains more information than necessary to maintain learner profiles, determine and assign training requirements, and maintain training histories.

Mitigation: FDIC mitigates this risk by regularly reviewing the data maintained in this system to ensure that only the minimum information necessary is kept. FDICLearn II requires basic information related to the learner to operate the system and maintain an official record for training.

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

Mitigation: The FDIC is in the process of developing an enterprise test data strategy to mask or use synthetic data in the test and lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Section 7.0: Data Quality and Integrity

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

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

The FDIC reviews privacy artifacts for adequate measures to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

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

The information system or project collects PII directly from the individual and authoritative sources, such as FDIC's human resources system. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

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

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

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

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

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

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

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a risk that the training records provided by the third-party providers is inaccurate.

Mitigation: FDIC extracts completion records from third-party providers and uploads those records in FDICLearn II. Depending on the third party training platform, FDIC updates FDICLearn between daily and monthly. If there are inaccuracies in the records provided by the third-party platform, users will need to contact the third party provider to update their training history. The updated record will then be accurately reflected in FDICLearn II at the next scheduled refresh.

Section 8.0: Individual Participation

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

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

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

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

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

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

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant Privacy Act SORN(s) as well as the relevant PIA.

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

The project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

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

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

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There is a risk that a non-FDIC user may be unaware that their information was passed to FDIC to create a FDICLearn II account, and therefore did not provide consent prior to account creation.

Mitigation: FDIC would not be aware of interactions between employers and employees. Employers should provide notice to employees prior to submitting their information to FDIC.

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.**

FDIC uses FDICLearn II to track training for both FDIC employees (internal) and external learners such as state banking employees and foreign bank representatives. The system is also used to track career development, certifications, continuing education, and learner skills and competencies.

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

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

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

All FDIC employees and external users who have been granted an account will have access to their own profile and training data. All access is granted on a need-to-know basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

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.

FDIC's central user access request system receives users' annual security and privacy training completion record. The FDIC Enterprise Data Warehouse will receive training completion data for reporting.

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, FDICLearn II will not aggregate or consolidate data to make determinations or derive new data about individuals. FDICLearn II records are used to monitor compliance with FDIC training requirements.

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.

FDIC does not share information from FDICLearn II with any external parties. 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 1360.20 'Privacy Program', and FDIC Circular 1360.17 'Information Technology Security Guidance for FDIC Procurements/Third Party Products'. The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 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.

FDIC does not share information from FDICLearn II with external 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.

FDIC does not share information from FDICLearn II with external parties.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There are no identifiable risks associated with use limitation for FDICLearn II.

Mitigation: No mitigation actions are recommended.

Section 10.0: Security

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

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

The FDIC Privacy Section maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

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 risks associated with security for FDICLearn II.

Mitigation: No mitigation actions are recommended.