



**Privacy Impact Assessment (PIA)
for
Examination Tools Suite (ETS)**



08/04/2025

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 PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government that protects the funds depositors place in banks and savings associations, also known as "insured banks" or "insured depository institutions." The FDIC's Division of Risk Management Supervision (RMS) has primary responsibility for examining and supervising State-chartered, non-Federal Reserve member banks to ensure they operate in a safe and sound manner. (As deposit insurer, the FDIC has back-up regulatory authority for other charter types.) During its examinations, RMS examiners devote significant attention to reviewing the quality of a bank's loan portfolio to determine risk to the FDIC insurance fund. Assessing loan portfolio quality puts examination staff into contact with personally identifiable information (PII) for both individual and commercial borrowers.

The Examination Tools Suite (ETS) is the primary examination tool used by RMS to produce the FDIC's Report of Examination (ROE). ETS enables examiners to more efficiently create, process, and share examination work papers and the final ROE, while providing the proper security controls to assure and protect sensitive examination data. Central Peer is a component of ETS that allows for collaboration and the transfer of examination information between examination team members. All exam data including bank information, loan information, report writing, and report review is shared through Central Peer.

ETS is used by FDIC, the Federal Reserve System (FRS), and State bank examiners to plan the examination, analyze the financial condition of the financial institution, review management's involvement in the financial institution operations, and develop the ROE. Specifically, ETS supports financial institution examiners in performing the following supervisory activities: (1) Safety and Soundness Examinations (also known as Risk

¹ www.fdic.gov/privacy

Management Examinations); (2) Bank Secrecy Act/Anti Money Laundering (BSA/AML) Examinations; (3) Specialty Examinations, such as: Information Technology Examinations, Trust Examinations, Government Security Dealer Examinations, Municipal Security Dealer Examinations, and Registered Transfer Agent Examinations; (4) Visitations; and (5) Investigations.

As part of producing ROEs in ETS, authorized RMS staff request electronic asset/loan data from the subject financial institution during the examination planning stage. The financial institution provides the data via Enterprise File Exchange (EFX), or secure email. At the examiner's discretion, the financial institution provides RMS staff with either a full download or subset of the financial institution's loan portfolio. In addition, the examiner collects electronic or hardcopy listings of securities owned by the bank, other real estate owned by the financial institution, or other asset types of records. This data is loaded into ETS by authorized RMS examination staff. The asset/loan records provided by financial institutions may include PII, such as the borrower's full name, bank account number/borrower identification number, loan/note number(s), outstanding balance(s), and other information detailed in Section 1.0 of this PIA. ETS contains limited information about bank officers, directors, and trustees, such as their names, home addresses (if applicable), biographies, year of birth, and salaries, as well as quantity of stock shares owned.

ETS was designed to advance data minimization and security of examination data. While examiners previously shared examination materials via email or removable media, ETS provides the capability for secure network-based file sharing and collaboration within FDIC and with other regulators. Additionally, by design, ETS is not intended to serve as a final repository for examination data. With limited exceptions, examination data in ETS is automatically deleted ninety-seven (97) days after the ROEs are mailed to financial institutions. This includes loan data within the examination record. When exams are deleted on local machines, ETS automatically deletes the data from its database to limit the collection and retention of PII. Loan archive data files needed for future exams are stored on a secure FDIC repository and purged after three (3) years. In limited cases, examination data may not be automatically deleted within 97 days, such as when a user creates an examination for analysis purposes only. These types of examinations may be deleted manually by users at any time. Otherwise, they will be deleted via an auto purge program after 365 days of inactivity. Refer to Section 6.0 of this PIA for additional information.

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;
- Access and Amendment;
- Minimization;
- Data Quality and Integrity;
- Individual Participation; and
- Use Limitation.

Transparency

Privacy Risk: ETS contains third-party data from financial institutions, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection, use, processing, storage, maintenance, dissemination, and disclosure of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC.

Mitigation: ETS does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Therefore, notice, in the form of a Privacy Act Statement (PAS) or System of Records Notice (SORN), is not required. In instances where ETS contains bank data with PII, financial institutions are legally required to provide individuals with any applicable notices regarding the sharing of their information with financial regulators. Additionally, the FDIC does not use ETS to make decisions regarding individuals based on the PII received from the banks. However, this PIA serves as notice of the information collection. No additional mitigation actions are recommended.

Access and Amendment

Privacy Risk: The system does not have procedures or provide notification to individuals about how to access or amend their information.

Mitigation: The system does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their bank directly for access to their personal information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Minimization

Privacy Risk: There is a potential risk related to data minimization for ETS because users are able to upload supporting documentation into the system, which could potentially duplicate records stored in the source systems. This supporting documentation could also potentially be retained in ETS beyond the stated retention periods for those respective source systems.

Mitigation: FDIC relies on authorized ETS users to minimize unnecessary duplication of data. Whenever possible, users access information in the originating systems and only upload information that is necessary to support authorized business purposes. In addition, by design and policy, ETS is not intended to serve as a data repository for examination data. All examination data in ETS is deleted ninety-seven (97) days after the Reports of Examination are mailed to financial institutions. Loan archive data files needed for future exams are stored on a secure FDIC shared drive and removed after three (3) years. No additional mitigation actions are recommended.

Data Quality and Integrity

Privacy Risk: Since PII in ETS is not collected directly from individuals, there is a risk that the data may not be accurate or complete. In addition, manual entries of data into ETS may increase data quality and integrity risks.

Mitigation: All PII used by ETS is obtained from the financial institution under examination. Financial institutions are responsible for providing FDIC RMS examiners with data that is accurate and complete. The FDIC Examiner-in-Charge (EIC) has overall responsibility for ensuring the accuracy and completeness of the data acquired and processed by the ETS application through the examination team. The EIC assigns various parts of the examination to individual team members to ensure that the examination's scope is completed. The EIC checks the data for completion by reviewing the assignments made to each team member and the information prepared within the application. Additionally, paper records of reconciliation are obtained from financial institutions to compare and validate the completeness of electronic data that may have been provided directly by said institution. Therefore, no mitigation actions are recommended.

Individual Participation

Privacy Risk: Since data in the system is not collected directly from individual borrowers, there is a risk that these individuals will not know how their data is being used or shared, nor will they be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: The system does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and

requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, no mitigation actions are recommended.

Use Limitation

Privacy Risk: In limited cases, some examinations in ETS, such as those created for analysis purposes only, are removed using manual business processes. Therefore, there is some risk that examination data may be accessed or retained longer than necessary to meet the required business need.

Mitigation: By design and policy, ETS is not intended to serve as a data repository for examination data, and all examination data must be deleted within the timeframes prescribed in the applicable FDIC records retention periods. Accordingly, access to examinations data is automatically deleted within 97 days after the Report of Examination (ROE) is mailed to the institution. The automatic purge is tied to and triggered by the ROE "Mail Date" listed in the corresponding record in the Virtual Supervisory Information On the Net (VISION), FDIC's tracking system for examinations. In cases where an ETS examination is created without a corresponding VISION record (i.e., "Analysis Only" examinations), users may manually delete the examination at any time. Otherwise, the records will be deleted automatically via an auto purge program after 365 days of inactivity. The auto purge program is run nightly. No additional mitigation actions are recommended.

Section 1.0: Information System

1.1 What information about individuals, including PII (e.g., name, Social Security number, date of birth, address) and non-PII, will be collected, used or maintained in the information system or project?

The PII in the asset/loan records provided by financial institutions is required by RMS examiners and entered into ETS. It includes: the borrower's full name; bank account number/borrower identification number (i.e., a Customer Information File (CIF) number assigned by the financial institution); loan/note number(s); outstanding balance(s), interest rates, and payment information.

Some records may contain additional borrower/customer data, such as: Social Security number (SSN) (used by some financial institutions as the CIF); Tax

Identification Number (TIN) (occasionally used by some financial institutions as the CIF for commercial borrowers; in some instances, this may be an SSN); and home or business mailing address.

In addition, loan records may contain the financial institution's risk rating of a particular loan (e.g., non-public confidential bank loan classifications, loan exposure risk level), as well as the appraised value of the collateral used to secure the loan. Loan records may also contain demographic information, such as the race, ethnicity, and gender of borrowers. Moreover, during the examination process, examiners may review hard copies of complete loan files, which may include credit reports and tax returns for individual borrowers. These hardcopy records may be scanned as supporting documentation for the examination but are purged at the conclusion of the examination.

ETS also may contain limited information about bank officers, directors, and trustees, such as their names, home addresses (if applicable), biographies, year of birth, and salaries, as well as quantity of stock shares owned.

The ETS Configuration service (ETSConfig) authenticates FDIC and Federal/State users with their names and work email addresses.

PII Element	Yes
Full Name	<input checked="" type="checkbox"/>
Date of Birth	<input checked="" type="checkbox"/>
Place of Birth	<input type="checkbox"/>
Social Security number (SSN)	<input checked="" type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>
Mother's Maiden Name	<input type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage)	<input type="checkbox"/>
Medical Information	<input type="checkbox"/>
Address	<input checked="" type="checkbox"/>
Phone Number(s)	<input checked="" type="checkbox"/>
Email Address	<input checked="" type="checkbox"/>
Employee Identification Number (EIN)	<input type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report)	<input checked="" type="checkbox"/>

PII Element	Yes
Driver's License/State Identification Number	<input type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input checked="" type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	<input checked="" type="checkbox"/>
Education Records	<input type="checkbox"/>
Criminal Information	<input type="checkbox"/>
Military Status and/or Records	<input type="checkbox"/>
Investigation Report or Database	<input type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>
Photographic Identifiers (e.g., image, video)	<input type="checkbox"/>
User Information (e.g., User ID, password)	<input checked="" type="checkbox"/>
Specify other:	<input type="checkbox"/>

1.2 What are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Financial Institutions	Authorized RMS examination staff request electronic asset/loan data from the targeted financial institutions during examination planning. The financial institution provides the data via authenticated access (FDICconnect) to Enterprise File Exchange (EFX), or secure email. At the examiner's discretion, the financial institution provides RMS examination staff with either a full download or subset of the financial institution's asset portfolio. Asset data includes electronic or hardcopy listings of loans, securities owned by the bank, other real estate owned by the financial institution or other asset types. This data is loaded into ETS by authorized RMS examination staff.
Authorized RMS Examination Staff	Examiners review asset data in ETS and may edit or add information using various analysis and data segmentation capabilities to determine the scope of asset reviews (primarily loans) for the upcoming examination.

Data Source	Description of Information Provided by Source
Virtual Supervisory Information On the Net (ViSION)	ViSION provides ETS with statistical data and offsite analysis and metrics of insured financial institutions, as well as examination-related information. Exam data may contain limited PII, such as the name of the examiner and Examiner in Charge (FDIC and state). ETS is working with the CIOO to reduce mainframe dependencies and data ingestion processes will be changing.
Federal Financial Institutions Examination Council's (FFIEC) Central Data Repository (CDR)	FFIEC's CDR is a central repository for the collection, storage, and distribution of Call Report data. Call Report data is prepared quarterly by each insured financial institution and uploaded to the CDR. CDR provides Call Reports and Uniform Bank Performance Reports (UBPRs) to ETS. Call data may contain limited PII such as names of Bank POCs, Patriot Act POC, primary and backup POC, the person signing report, and CFO. In addition to the names of the POCs, it may contain work-related contact information for the POCs (such as phone number, email, fax number).
Management Information Repository (MIR)	MIR (previously Interagency Examination Repository (IER)) provides bank management information to ETS via the ROE service. This information consists of bank management/shareholder data (i.e., names, addresses, dates of birth, titles, occupations, attendance, ownerships, committee memberships) that comes from IER.
Regional Automated Document Distribution and Imaging System (RADD)	RADD provides ETS historical ROE documents through a RESTful (REpresentational State Transfer) API. ROEs contain sensitive information and PII, particularly names of borrowers, current and historical bank CAMELS Ratings, Compliance/CRA, specialty exam ratings, and data about assets or loans identified as having potential weaknesses.
Structure Information Management System (SIMS)	SIMS provides publicly available financial institution data (name, certificate number, address, branches, CEO name, work contact information, web address, etc.) to ETS.
ETS Configuration (ETSConfig) Component	The ETSTConfig Component authenticates ETS user access with name and email address.

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

The ATO was re-issued on May 15, 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.

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the system or project does not retrieve information by personal identifier. Therefore, a SORN is not required.

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

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the system or project does not retrieve information by personal identifier. Therefore, a SORN is not required.

2.4 If a Privacy Act Statement² is required, how is the Privacy Act Statement provided to individuals before collecting their PII? Explain.

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the system or project does not retrieve information by personal identifier. Therefore, a SORN is not required.

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: ETS contains third-party data from financial institutions, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection, use, processing, storage, maintenance, dissemination, and disclosure of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC.

Mitigation: ETS does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Therefore, notice, in the form of a Privacy Act Statement (PAS) or System of Records Notice (SORN), is not required. In instances where ETS contains bank data with PII, financial institutions are legally required to provide individuals with any applicable, required notices regarding the sharing of their information with financial regulators. Additionally, the FDIC does not use ETS to make decisions regarding individuals based on the PII received from the banks. Further, this PIA serves as notice of the information collection. No additional mitigation actions are recommended.

² See 5 U.S.C. §552a(e)(3). 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.

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?

The system or project receives third-party data from financial institutions. The FDIC does not have the ability to implement procedures for individual access. Individuals should contact their financial institution directly for access to their personal information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the financial institutions.

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

The system or project receives third-party data from financial institutions. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their financial institution directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the financial institutions.

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

The system or project receives third-party data from financial institutions. The FDIC is unable to notify individuals about the procedures for correcting their information. Individuals should contact their financial institution directly to correct any inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the financial institutions.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: The system does not have procedures or provide notification to individuals about how to access or amend their information.

Mitigation: The system does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices and may contact their bank directly for access to their personal information. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, 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 supports the SAOP in the management and execution of the FDIC's Privacy Program.

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). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

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?

Yes, this PIA captures privacy risks posed by ETS through the privacy risk analysis sections throughout the document. PIAs are posted on FDIC's public-facing website, <https://www.fdic.gov/policies/privacy/index.html>.

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

Contractors are employed by the FDIC's Division of Information Technology (DIT) to provide development and maintenance support for the ETS application, as needed. In this role, contractors do not have access to any borrower or other data that is processed by the application.

Contractors also are employed by DIT to support the DIT Examiner Help Desk. In this capacity, contractor staff have limited access to borrower data for the purpose of assisting examiners with formatting the data for use by the ETS application on the examiner's laptop. The sending of borrower data is performed through secure email.

Due to contractors' access to PII, contractors 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, appropriate Confidentiality Agreements have been completed and signed for contractors who work on ETS. 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 implements a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130. ETS does not operate as a Privacy Act System of Records.

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

Corporate Information Security and Privacy Training, which includes Rules of Behavior, are mandatory for all users of the ETS system. System-specific training covers information regarding the compromise of data and the prevention of its misuse. Rules of Behavior, in addition to FDIC Corporate policies, establish user responsibility and accountability. Annual role-based training is taken by users, including external users.

In addition, 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 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 Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA, and regular reporting to the SAOP, the Chief Information Security Officer (CISO), and the Information Technology Risk Advisory Council.

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

The system includes automated checks to ensure that data entered by ETS staff is complete (e.g., mandatory fields are not left blank). In addition, ETS uses an access control system and maintains audit logs to ensure user activities, access to data, and login attempts are legitimate and authorized.

In addition, 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 when possible. Additionally, FDIC has implemented technologies to track, respond, remediate, and report on breaches, as well as to track and manage PII inventory.

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and 12 C.F.R. part 310, however, ETS does not operate as a System of Record.

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

The FDIC retains an accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and 12 C.F.R. part 310, however, ETS does not operate as a System of Record.

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

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and 12 C.F.R. part 310, however, ETS does not operate as a System of Record.

Privacy Risk Analysis: Related to Accountability

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

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Directive 1360.20, "Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. ETS collects PII pursuant to the following laws and regulations: Sections 5, 6, 7, 8, 9, 18, and 19 of the Federal Deposit Insurance Act (12 U.S.C. 1815, 1816, 1817, 1818, 1819, 1828, 1829):

- 12 U.S.C. §1815: deals with application for deposit insurance.
- 12 U.S.C. §1816: are factors that need to be considered when evaluating an application for deposit insurance or merger.
- 12 U.S.C. §1817: concerns assessments levied by the FDIC on insured depository institutions to primarily fund the Deposit Insurance Fund (DIF),
- 12 U.S.C. §1818: Allows the FDIC to terminate an insured depository institution's (IDI) status for various reasons including unsafe or unsound practices.
- 12 U.S.C. §1819: exercises FDIC's corporate powers to conduct examinations of and to require information and reports from depository institutions.
- 12 U.S.C. §1828: governs regulations for insured depository institutions, including those related to deposit insurance. It covers various aspects,

including displaying official signs, preventing false advertising, and addressing misrepresentations about insured status.

- 12 U.S.C. §1829: penalizes individuals convicted of certain crimes from participating in the affairs of insured depository institutions (IDIs) without the written consent of the Federal Deposit Insurance Corporation (FDIC).

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

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

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

ETS, by design, helps to advance data minimization and enhance protection of examination data. ETS provides the capability for secure network-based file sharing and collaboration within FDIC and with other regulators, thereby strengthening security controls and minimizing redundant and duplicate repositories of data. ETS only collects the minimum PII elements needed to accomplish authorized tasks and only collects PII that is directly relevant and necessary to accomplish specified purpose(s). ETS does not duplicate files containing PII and uses the minimum elements necessary for legally authorized purposes. Data related to examinations is collected by RMS staff as a result of their supervisory examination authority under the FDI Act. ETS uses an access control system to restrict user view and edit rights to the minimum necessary to perform daily work tasks, based on predefined roles and restrictions on FDIC division and regulatory authority.

Additionally, through the conduct, evaluation, and review of privacy artifacts,³ the

³ Privacy artifacts include Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Record Notices (SORN).

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 related to examinations is collected by RMS staff as a result of their supervisory examination authority under the FDI Act. RMS staff collect and review records and information obtained directly from insured banks. For example, data related to examinations is not provided directly by individuals. In addition, ETS only collects PII that is directly relevant and necessary to accomplish specified purpose(s).

Generally, ETS examination data is automatically deleted ninety-seven (97) days after the ROEs are sent to financial institutions. This includes loan data within the examination record. When exams are deleted on local machines, ETS Central Peer automatically deletes the data from its database to limit the collection and retention of PII. Loan archive data files needed for future exams are stored on a secure FDIC repository. After three (3) years, Regional Archive Managers remove the loan archive data.

In limited cases, examination data may not be automatically deleted within 97 days, such as when a user creates an examination for analysis purposes only and, therefore, a corresponding record and “Mail Date” for a Report of Examination are not created in ViSION. Examinations without corresponding ViSION records (i.e., “Analysis Only” examinations) may be deleted manually by users at any time within the ETS application. Otherwise, they will be deleted via an auto purge program after 365 days of inactivity. The auto purge program is run nightly.

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.

6.3 How often does the information system or project evaluate the PII 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?

The FDIC maintains an inventory of systems that contain PII. The Privacy Program reviews information in the systems at the frequency defined in the FDIC Information Security Continuous Monitoring Strategy. New collections are evaluated to determine

if they should be added to the inventory.

6.4 What are the retention periods of the 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.

In accord with the FDIC records retention schedule, all examination data in ETS is deleted ninety-seven (97) days after the Reports of Examination are mailed to financial institutions, with the exception of "Analysis Only" examinations which may be deleted manually or auto purged after 365 days of inactivity. When exams are deleted on local machines, ETS Central Peer automatically deletes the data from its database to limit the collection and retention of PII. Loan archive data files needed for future exams are stored on a secure FDIC shared drive and removed after three (3) years.

Additionally, records are retained in accordance with the FDIC Directive 1210.01 "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and 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 Directives 1210.01 and 1360.09, "Protecting Information."

By design, ETS is not a data repository and is not subject to the Privacy Act of 1974 System of Record requirements. By policy directive, FDIC bank examination staff are required to back-up asset/loan data to the ETS Archive Library site and delete all electronic data files from their laptops related to an examination at the conclusion of that examination through final review and approval of the ROE and destroy the bank provided electronic files by FDIC-approved method(s). According to FDIC's Records Retention schedule, zipped and encrypted archived RMS examination files and printed work papers are securely retained for one examination cycle, in the event of litigation.

6.5 What are the policies and procedures that minimize the use of 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 developed 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 potential risk related to data minimization for ETS because users are able to upload supporting documentation into the system, which could potentially duplicate records stored in the source systems. This supporting documentation could also potentially be retained in ETS beyond the stated retention periods for those respective source systems.

Mitigation: FDIC relies on authorized ETS users to minimize unnecessary duplication of data. Whenever possible, users access information in the originating systems and only upload information that is necessary to support authorized business purposes. In addition, by design and policy, ETS is not intended to serve as a data repository for examination data. All examination data in ETS is deleted ninety-seven (97) days after the Reports of Examination are mailed to financial institutions, with the exception of “Analysis Only” examinations which are removed manually or are auto purged after 365 days of inactivity. Loan archive data files needed for future exams are stored on a secure FDIC shared drive and removed after three (3) years, in accordance with the FDIC records retention schedule. When exams are deleted on local machines, ETS Central Peer automatically deletes the data from its database to limit the collection and retention of PII. Refer to Section 9 for additional details. During the course of conducting this PIA, FDIC formally reviewed and validated the record retention and disposition procedures for ETS, as well as established an official FDIC records retention schedule to govern ETS data. No additional mitigation actions are recommended.

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.

All PII used in ETS is obtained from the financial institution under examination. Financial institutions are responsible for providing FDIC RMS examiners with data that is accurate and complete. The loan data provided by financial institutions is securely transferred to FDIC electronically, which reduces the risk of errors arising from manual entry. Additionally, records of reconciliation are obtained from financial institutions to compare and validate the completeness of electronic data that may have been provided directly by institutions. Further, FDIC employs a rigorous review and clearance process when drafting ROEs. The FDIC Examiner-in-Charge (EIC) has overall

responsibility for ensuring the accuracy and completeness of the ROE along with the supporting data acquired and processed by the examination team in ETS. The EIC assigns various parts of the examination to individual team members to ensure that the examination's scope is completed. The EIC checks the data for completion by reviewing the assignments made to each team member and the information prepared within the application. ETS also checks data automatically to ensure that the information entered by ETS staff is complete (e.g., mandatory fields are not left blank).

Additionally, the FDIC reviews privacy artifacts for adequate controls 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?

PII that is contained in the asset/loan customer records is provided by banks and required by RMS examiners. Financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act.

Data is not collected directly from individuals. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their financial institution directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the financial institutions.

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

As noted in Section 7.1, all PII data used in ETS is obtained from the financial institution under examination. Financial institutions are responsible for providing FDIC RMS examiners with data that is accurate and complete. The loan data provided by financial institutions is securely transferred to FDIC electronically, which reduces the risk of errors arising from manual entry. Additionally, records of reconciliation are obtained from financial institutions to compare and validate the completeness of data. Further, FDIC employs a rigorous review and clearance process when drafting ROEs. The FDIC EIC has overall responsibility for ensuring the accuracy and completeness of the ROE and the supporting data acquired and processed by the examination team in ETS. The EIC assigns various parts of the examination to individual team members to ensure that the examination's scope is completed. The EIC checks the data for completion by reviewing the assignments made to each team member and the information prepared within the application. ETS also checks data

automatically to ensure that the information entered by ETS staff is complete (e.g., mandatory fields are not left blank).

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

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.

As noted in Section 7.1, all PII data used in ETS is obtained from the financial institution under examination. The loan data provided by financial institutions is securely transferred to FDIC electronically, which reduces the potential for data integrity issues. Refer to Section 7.1 for details. Through the 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 Information Security Officer validates the configuration of 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. Consequently, the FDIC does not need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: Since PII in ETS is not collected directly from individuals, there is a risk that the data may not be accurate or complete. In addition, manual entries of data into ETS may increase data quality and integrity risks.

Mitigation: All PII data used by ETS is obtained from the financial institution under examination. Financial institutions are responsible for providing FDIC RMS examiners with data that is accurate and complete. The loan data provided by financial institutions is securely transferred to FDIC electronically, which reduces the risk of errors arising from manual entry. Additionally, paper records of reconciliation are obtained from financial institutions to compare and validate the completeness of the data. Further, FDIC employs a rigorous review and clearance process when drafting ROEs. The FDIC EIC has overall responsibility for ensuring the accuracy and completeness of the ROE and the supporting data acquired and processed by the examination team in ETS. The EIC assigns various parts of the examination to individual team members to ensure that the examination's scope is completed. The EIC checks the data for completion by reviewing the assignments made to each team member and the information prepared within the application. ETS also checks data automatically to ensure that the information entered by ETS staff is complete (e.g., mandatory fields are not left blank). No additional mitigation actions are recommended.

Section 8.0: Individual Participation

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

8.1 Explain how the information system or project provides means, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

ETS does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice 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.

Not applicable. ETS does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, 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, when 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. In the event of significant changes to new uses or disclosures of previously collected PII, the FDIC Privacy Program will update the relevant SORN(s) as well as this PIA, thereby providing public notice of those changes. SORN modifications are subject to a public comment period and FDIC will review and consider any comments related to new or changed uses or disclosures of PII.

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

ETS receives data from third parties. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. 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, <http://www.fdic.gov/privacy/>, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Since data in the system is not collected directly from individual borrowers, there is a risk that these individuals will not know how their data is being used or shared, nor will they be provided with an opportunity to authorize or opt out of any new uses of data pertaining to them.

Mitigation: The system does not operate as a Privacy Act system of records and does not collect PII directly from individual borrowers. Rather, financial institutions provide examiners with commercial and consumer loan data pursuant to the supervisory and regulatory authority granted to the FDIC by the Federal Deposit Insurance Act. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII and requires this information in order to perform its statutory duties. Financial institutions are required by law to provide applicable notices to their customers regarding the sharing of their information with financial regulators. Individuals may review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from third parties. Therefore, 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.

ETS supports financial institution examiners in performing the following supervisory activities:

1. Safety and Soundness Examinations (also known as Risk Management Examinations)

2. Bank Secrecy Act/Anti Money Laundering (BSA/AML) Examinations
3. Specialty Examinations, such as:
 - a. Information Technology Examinations
 - b. Trust Examinations
 - c. Government Security Dealer Examinations
 - d. Municipal Security Dealer Examinations
 - e. Registered Transfer Agent Examinations
4. Visitations
5. Report of Investigations

PII that is contained in customer records provided by banks and required by RMS examiners using ETS includes:

- Borrower's full name
- Bank account number/Borrower Identification number (i.e., a Customer Information File (CIF) number assigned by the bank)
- Loan/note number(s)
- Outstanding balance(s), interest rates, and payment information

9.2 Describe how the information system or project uses 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, and in conjunction with the implementation of applicable privacy controls, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Directive 1360.09 "Protecting Information." Additionally, annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

The RMS ETS Program Manager is responsible for the ETS application. The examination team's EIC is directly responsible for all actions of the examination team and all data that comes into the possession of the examination team in the process of examining a particular financial institution. The EIC is directly accountable, by virtue of the commissioning and position assignment, for the integrity of all data generated during the examination process. Additionally, requirements for ensuring the security and confidentiality of bank and customer related data are covered by several directives in the RMS Regional Director Memoranda system. Mandatory security awareness training conducted online annually by the RMS Information Security

Manager covers general data security issues.

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

For each bank examination, a RMS Field Supervisor is responsible for assigning RMS examination team members. This assignment conveys approval for access, by management, to a financial institution's asset data provided at the time of an examination. ETS has built-in measures such as multi-factor authentication, firewalls, and encryption. Access is reviewed annually and limited to authorized members of the examination team using multi-factor authentication and encrypted hard-drive laptops. Access to examination data is removed automatically as soon as "Mail Date" information is entered into the VISION. For exams that are conducted by the State and FRS examiners, which do not have a corresponding VISION record, each examiner is responsible for removing the examination from his/her machine. Once the exam is deleted on local machines, ETS Central Peer will automatically delete the data from its database. An exam can be created offline and connected to VISION later in order to take advantage of the automatic purge of data. Since some exams could potentially never have a corresponding VISION record (i.e., Analysis Only exams), users must therefore remove them manually. Otherwise, the auto purge program will delete these records from ETS after 365 days of inactivity.

Only authorized examination staff are given access and rights into the ETS application. The primary distribution method for all banker correspondence, including ROEs and other documents containing PII, are distributed electronically via secure email, as outlined in FIL-9-2025.

All access is granted on a need-to-know basis. FDIC follows 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. Federal and State regulatory agency users follow a similar structure for controlling ETS access.

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.

Data Destination	Description of Shared Information
IER Database	PII may include bank officer name, title and phone number.

Content Management Web Service (CMWS)	Reports of Examination which contain limited PII. Examiner name, Examiner in Charge name; regional manager name; and possibly information about bank officials (name, salary)
Management Information Repository (MIR)	During examinations, examiners generally input information about bank directors and senior officers, including names, home addresses, salaries, biographies, and stock ownership. This data is transmitted to the MIR for retention and is pulled from MIR into ETS while gathering historical examination artifacts, and it is then updated for the current exam cycle.

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No, FDIC does not aggregate data to make program-level decisions.

9.6 Does the information system or project share 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.

Financial institutions provide loan data files and management information electronically, but there is no direct connection to ETS. The Federal Financial Institutions Examination Council (FFIEC) Central Data Repository (CDR) provides Call Report and UBPR data to ETS. External sharing is pursuant to an existing information sharing access agreement.

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, and FDIC Directive 1360.20 "Privacy Program." 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 Directive 1360.09.

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 employees and contractors, which includes information on rules and regulations

regarding the sharing of PII with third parties.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: In limited cases, some examinations in ETS, such as those created for analysis purposes only, are removed using manual business processes. Therefore, there is some risk that examination data may be accessed or retained longer than necessary to meet required business needs.

Mitigation: By design and policy, ETS is not intended to serve as a data repository for examination data, and all examination data must be deleted within the timeframes outlined in Section 6 of this PIA. Generally, access to examination data in ETS is removed ninety-seven (97) days after the Report of Examination is mailed to the financial institution, with the exception of “Analysis Only” examinations. Such examinations may either be removed manually at any time by users or be deleted via an auto purge program after 365 days of inactivity, whichever comes sooner. The auto purge program is run nightly.

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 PII.

The FDIC Privacy Program 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 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. Oversight of FDIC's breach response activities occurs through quarterly reporting to both the FDIC's Senior Agency Official for Privacy and the FDIC Information Technology Risk Advisory Council. ITRAC seeks to properly align the management of IT risks with the FDIC's Enterprise Risk Management Program. Additionally, FDIC holds a breach response tabletop exercise every year to test the effectiveness of the Plan and identify improvements or changes needed to the Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to security for ETS.

Mitigation: No mitigation actions are recommended.