FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA) for Electronic Discovery and Litigation Support (EDLS) Suite

December 22, 2021

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC public-facing website[1], which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government charged with maintaining stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, making large and complex financial institutions resolvable, and managing receiverships. In carrying out its mission, the FDIC may be involved in various legal activities, such as investigating and pursuing professional liability claims[2] arising from failures of insured financial institutions, bringing enforcement actions[3] against entities and individuals subject to its authority, and defending itself against litigation. In addition, the FDIC conducts internal/Corporate investigations, processes complaints, and responds to Freedom of Information Act (FOIA), Privacy Act (PA), Government Accountability Office (GAO), Congressional, subpoena, and other requests for information. These activities all have the potential to involve electronic discovery (e-discovery), which refers to the review, analysis, and use of electronically stored information (ESI), such as emails, computer files, and databases.

The FDIC obtains a significant amount of ESI as part of legal matters related to its Corporate and Receivership activities. Depending on the nature of a particular matter, the FDIC may derive this information from interviews, subpoenas, documents, research, public records, financial institutions and/or other parties involved in legal matters. The FDIC also collects information from agency staff and contractors who are custodians of potentially relevant ESI, as well as from its own computer network and systems. This ESI has the potential to contain any manner of personally identifiable information (PII) about current or former bank officers, employees, customers, or other institution affiliated parties. The ESI may also contain PII about FDIC employees and contractors stemming from Corporate legal matters, such as those related to employment applications or personnel actions.

Within FDIC, the Legal Division (Legal) is responsible for the collection, review, redaction, and production of agency records, including ESI and hardcopy documents, in support of processing and resolving FDIC legal matters. To effectively manage this responsibility, Legal utilizes a suite of tools, systems and processes herein referred to as Electronic Discovery and Litigation Support (EDLS). FDIC attorneys, investigators, and other staff use EDLS to collect, organize, process, review, and produce large volumes of agency records that are potentially responsive to discovery, subpoena, or other requests. EDLS replaces manual processes associated with gathering, sorting, reviewing and redacting such information, as well as assessing its relevance and/or responsiveness and applying appropriate privileges. The tools facilitate the forensically sound collection of such information and the production of records in the same format in which they were originally compiled or maintained (native format), along with any associated metadata. The tools also are used to import scanned paper records and extract electronic information from other FDIC systems and tools, such as FDIC Business Data Services (FBDS),[4] FDIC's network, and Enterprise Vault, which is FDIC's email repository and archiving solution used to support the litigation and discovery process.

The range of capabilities varies across the individual systems and toolsets, but collectively they streamline and automate the ESI review process by providing the following key features and functionality:

[1] www.fdic.gov/privacy
[2] www.fdic.gov/resources/resolutions/professional-liability/annual-reports.html
[3] www.fdic.gov/regulations/examinations/enforcement-actions/index.html
[4] FDIC System of Records Notice (SORN) 013, Insured Bank Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

- **Data extraction and loading** – Users import, extract and load electronic information in various data formats such as common office documents (pdfs, email, spreadsheets, etc.), allowing document analysis using a single integrated viewer that does not require use of the original application that created the file.

- **Data de-duping, organization and processing** – The tools provide the ability to upload ESI and process it in a more efficient manner. For example, the tools support data de-duplication, email threading (organization of email chains), text extraction, tiff conversion, image optimization, optical character recognition (OCR), metadata extraction, indexing/coding, and document numbering.

- **Data identification, tagging and redaction** – The tools aid in identifying and tagging information by allowing users to conduct keyword and Boolean (logic) searches across record sets. The tools automatically flag files that contain those keywords or Boolean statements, allowing users to review and ascertain whether the files or information contained therein are responsive. The tools also allow users to electronically redact protected portions of documents.

- **Case mapping and management** – The EDLS suite includes a case mapping tool that allows users to research, identify and organize key facts, documents, cast of characters, and issues of each case into a centralized repository for improved case management. Case organization, analysis, and reporting tasks can be delegated and distributed among users. While the primary users of the case mapping system are the Legal Division litigation attorneys, a small number of investigation staff from the FDIC Division of Risk Management and Supervision (RMS) and FDIC Division of Resolutions and Receiverships (DRR) also use the system.

- **Legal hold processing** – Among the features of the EDLS toolset is a Legal Hold Center that allows the Legal Division to initiate, manage and view legal holds. The Legal Hold solution also features a Custodian Portal that provides a listing of active notifications for employees/custodians, along with the current acknowledgement status (response) for each hold.

In addition to the aforementioned systems and toolsets, EDLS is comprised of contracted staffing and support services. The Legal Division executes legal services agreements (LSAs) with Outside Counsel law firms to provide support for litigation and other FDIC legal matters. Additionally, the FDIC contracts with vendors under Basic Ordering Agreements (BOAs) to obtain legal support services and products for electronically processing, hosting, and storing information related to FDIC investigations, inspections, and litigation activities. These Outsourced Litigation Support Services (OLSS) vendors perform a number of tasks on behalf of the FDIC in support of enforcement, bankruptcy, corporate, professional liability, and inherited litigation matters. The vendors process and host data collected from internal FDIC data sources, as well as open or closed banks pursuant to litigation or investigations. Potentially relevant information is placed on legal hold and preserved throughout the course of litigation. Specific services are addressed in the Statement of Objectives (SOO) included in each vendor's contractual agreement with FDIC, and may include the following activities, some of which may involve accessing or utilizing PII:

- **Document acquisition, preparation, and unitization**, including organizing documents; identifying document boundaries (e.g., inserting slip sheets); numbering documents; creating box or file level indices; capturing document images (e.g., single-page Tiff format or PDF format); copying documents; and preparing documents for production.

- **Database creation and data quality control**, including performing Optical Character Recognition (OCR); document coding/data entry; creating databases or database load files; documenting procedures; and performing quality control.

- **Electronic data acquisition and processing**, including extracting and converting data files, such as email files and other files in their native formats; automated and manual analysis of files to identify relevant or priority material; analyzing and reporting file type and other data metrics; assisting in the production of electronic data; documenting procedures; and performing quality control.

- **Pre-trial and trial support**, including courtroom services, such as providing, administering, operating, and maintaining equipment and other resources in support of litigation; exhibit preparation; courtroom presentation and audio/visual services; and performing quality control.

- **Forensic services**, including forensic data collection performed by certified forensics professionals as needed at sites throughout the United States; data analysis and reporting; documenting procedures; and performing quality control.

- **Managed legal review**, including acquisition and processing of electronic data for the purpose of batching/loading the data into a review application; domestic review of documents by licensed attorneys for relevance and identification of legal privileges; redaction; creation of privilege logs; production of electronic and imaged data; documenting procedures; and performing quality control.

- **Managed data hosting**, including secure hosting of data for access by FDIC (or others as designated by FDIC); administration and support of web-based database/legal review applications; documenting procedures; and performing quality control.

The OLSS vendor firms primarily support large matters under the supervision of FDIC Legal Division attorneys. FDIC staff gathers and provides the vendors with potentially relevant claims and enforcement case materials. Vendors do not download any ESI directly from FDIC Information Technology (IT) resources. FDIC attorneys also do not upload any documents to vendor websites. Rather, FDIC transfers data to the vendors using secure file transfer protocol (SFTP). FDIC also securely ships hardcopy documents or downloads ESI to encrypted media and securely ships them to the OLSS firms for uploading to a Federal Risk and Authorization Management Program (FedRAMP) certified cloud solution hosted by an external vendor. Authorized users (including FDIC employees, opposing counsel, outside counsel, and vendor staff) can access the secure, web-based review platform using dual-factor authentication. Data is placed in case-specific repositories, and users are granted access to data on a "need-to-know" basis in order to perform their respective work assignments. Users are able to review and tag documents, but are not able to edit or delete documents. Permission to perform any other activities outside of reviewing and tagging must be expressly approved by the Legal Division. Based on circumstances or agreements with opposing counsel or other participants, rights to print or download may be granted for subsets of data upon request.

EDLS collects, processes and maintains a significant amount of sensitive information and PII that is necessary for the purposes of performing tasks associated with FDIC investigations, inspections, examinations, litigation, responsive record requests, and other e-discovery activities. Depending on the nature and scope of a particular legal matter, the PII processed by EDLS may pertain to internal FDIC personnel, as well as members of the public, such as bank officers, employees, customers, and depositors, or individuals who file complaints with or against FDIC (complainants). EDLS may on occasion contain information imported or scanned into the system previously received from State Regulators or Federal agencies involved in certain legal matters. These entities include, for example, the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), U.S. Department of Justice (DOJ), U.S. Attorneys' Offices, and Federal or Local Law Enforcement. EDLS also may contain information received from parties involved in legal matters, such as assuming institutions, servicers, bank and law firm retained vendors, FDIC outside counsel, and other individuals or entities pertinent to the respective legal matter or resolution of the matter.

FDIC is conducting this PIA to evaluate and document the impact that EDLS has on personal privacy. In addition, FDIC has documented in multiple FDIC Systems of Records Notices (SORNs) the records about individuals processed within EDLS. Such SORNs generally include: FDIC-002, Financial Institution Investigative and Enforcement Records;[5] FDIC-005, Consumer Complaint and Inquiry Records;[6] FDIC-009, Safety and Security Incident Records;[7] FDIC-012, Financial Information Management Records;[8] FDIC-013,

[5] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[6] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[7] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[8] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

Insured Financial Institution Liquidation Records;[9] FDIC-015, Personnel Records;[10] FDIC-018, Grievance Records;[11] and FDIC-022, Freedom of Information Act and Privacy Act Request Records.[12] The context of the data being analyzed by the EDLS tools determines the applicable SORN. For example, any records relating to a FOIA/PA request would be covered by the Freedom of Information Act and Privacy Act Request Records SORN,[13] whereas any records relating to complaints would be covered by the Consumer Complaint and Inquiry Records SORN[14] and any records relating to an enforcement action would be covered by the Financial Institution Investigative and Enforcement Records SORN.[15] The FDIC Identity, Credential and Access Management Records SORN[16] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of the EDLS tools and resources by authorized individuals.

PRIVACY RISK SUMMARY

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

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

Individual Participation and Transparency

Privacy Risk: EDLS receives or derives information from other agency recordkeeping systems and third-party sources, such as financial institutions and government agencies. Therefore, there is a risk that individuals are not provided with direct notice or the opportunity to consent or opt out prior to the collection and use of their PII within EDLS.

Mitigation: This PIA serves as notice to the general public regarding the collection and use of information in EDLS to fulfill FDIC's corporate and receivership responsibilities. In addition, FDIC provides notice to individuals at the original point of data collection wherever possible. Specifically, in cases where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. In cases where PII is received from financial institutions, government agencies or other third parties, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. On occasions when notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

[9] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[10] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[11] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[12] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[13] Ibid.
[14] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[15] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[16] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

Access and Amendment

Privacy Risk: There is a risk that individuals are not able to access and amend information about themselves within EDLS.

Mitigation: Since EDLS serves as a repository for records gathered from other agency recordkeeping systems and third-party sources to satisfy e-discovery and litigation requirements, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), individuals seeking access to any record contained in those SORs may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or FOIA (for all individuals) request to FDIC in writing or electronically at www.fdic.gov/policies/privacy/request.html. However, depending on the nature of the records being processed, FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal an investigative or enforcement interest on the part of FDIC. In cases where EDLS receives PII from financial institutions or other government agencies, individuals should contact the source entities and agencies that originated their data to access and amend their information.

Data Minimization

Privacy Risk: There is a risk that EDLS could over-collect PII, as well as aggregate disparate PII from different sources.

Mitigation: EDLS collects and aggregates information as necessary to satisfy e-discovery and litigation requirements. EDLS only processes information for which FDIC already has the authority to collect and pursuant to litigation discovery or other responsive document requests. In cases where EDLS derives information from other FDIC recordkeeping systems, Legal works with the relevant FDIC system owners/program managers to scope and provide specifications for targeted datasets to be retrieved from the respective source systems. Additionally, FDIC restricts access to EDLS tools to those who have a need to use them in order to perform authorized business duties. EDLS tools also utilize role-based permissions to limit user access to data, including PII, on a need-to-know basis. Further, the EDLS tools have the ability to generate audit trails of all user activity, including the viewing of records in the system.

Privacy Risk: There is a risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: FDIC maintains the records in EDLS according to the records schedules and policies discussed in Section 6, and disposes of them accordingly. Legal certifies when records can be destroyed. However, due to business rules and storage limits within the EDLS tools, the records that are uploaded to and processed may be deleted from some of the tools after processing and production. Occasionally, there will be times when records are kept in EDLS due to ongoing litigation. To ensure that storage limits are not reached, users receive periodic housekeeping notices to review any maintained files and delete those no longer needed.

Data Quality and Integrity

Privacy Risk: There is a potential risk associated with data quality and integrity because information processed by the EDLS tools could be inaccurate.

Mitigation: EDLS serves as a repository for reviewing and tagging records obtained from other agency recordkeeping systems and third-party sources in support of FDIC litigation and e-discovery requests. By design, therefore, EDLS contains only copies of records from these originating systems and sources. Additionally, the processing of information by the EDLS tools does not alter the original records in the source systems. Any inaccurate information, when identified, can be corrected in the source systems.

Purpose and Use

Privacy Risk: There is a potential risk that PII maintained in EDLS could be accessed or used inappropriately or for unauthorized purposes.

Mitigation: To help prevent unauthorized access and use of information, EDLS employs role-based permissions to restrict access to EDLS tools and the data contained therein. Access is granted only to authorized FDIC personnel who have a "need-to-know" in order to fulfill their job responsibilities. EDLS system/tool administrators grant access to users, and each individual user must be properly credentialed. In addition, all users are subject and must adhere to agency policies and procedures for using, sharing and safeguarding PII. All users receive annual Information Security and Privacy Awareness training, as well as specialized training, as applicable, which helps ensure PII is handled and safeguarded appropriately. The EDLS tools and platforms generate and maintain detailed audit logs that are capable of capturing any user's unauthorized use of information contained within the tool suite. EDLS IT security or administrators can review these logs when there is a confirmed or suspected compromise of information.

Additionally, EDLS limits the access and permission rights of users outside of the Legal Division, such as FDIC employees in other Divisions, opposing counsel, outside counsel, and contractor staff. By default, such users may only review and tag documents within certain EDLS platform(s) to which the Legal Division has granted them access, and they are prohibited via technical and administrative controls from editing or deleting documents. Permission to perform any other activities outside of reviewing and tagging must be expressly approved by the Legal Division. Based on circumstances or agreements with opposing counsel or other participants, rights to print or download ESI is only granted for subsets of data upon request and approval from the Legal Division.

Privacy Risk: There is a risk that disclosures of information in EDLS could be incompatible with the original purposes for which the information was collected.

Mitigation: Any disclosures of information processed by EDLS occur outside of the system itself. Therefore, EDLS is not designed to capture or record information sharing. However, because EDLS restricts access to data to users with a "need-to-know" who require the information to perform their job responsibilities, any disclosures outside of EDLS are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required by statute, federal court rules, or responsive document requests. Any information disclosures or withholdings are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover the source records.

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?

The EDLS suite collects, processes and maintains a wide range of sensitive information and PII as necessary to satisfy FDIC investigation, litigation and other e-discovery requirements or requests. This information could consist of emails, attachments, word processing documents, PDF files, spreadsheets, presentations, database entries, scanned hardcopy materials, or any other legal artifacts and ESI that FDIC collects in support of processing and resolving FDIC Corporate and Receivership legal matters and responding to requests for responsive materials. EDLS may on occasion contain information imported or scanned into the system previously received from Federal agencies or state regulators involved in certain legal matters. These entities include, for example, the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), U.S. Department of Justice (DOJ), U.S. Attorneys' Offices, and Federal or Local Law Enforcement. EDLS also may contain information imported or scanned into the system received from parties involved in legal matters, such as assuming institutions, servicers, bank and law firm retained vendors, FDIC outside counsel, and other individuals or entities pertinent to the respective legal matter or resolution of the matter.

Depending on the nature of a particular legal matter or responsive record request, the information in EDLS can be wide-ranging and may include employment records, banking records, contracts, personal and corporate financial information, legal documents, records or notes, and a variety of other types of records. This ESI has the potential to contain any manner of PII, including but not limited to names, dates of birth, Social Security numbers (SSNs), driver's license/state identification numbers, employee identification number, home addresses, phone numbers (e.g., phone, fax and cell), financial information (e.g., checking account #, PINs, access or security codes, etc.), email addresses and other types of PII noted in the table below. EDLS also captures and maintains metadata, which may contain PII (such as the name of the author of a particular electronic file), as well as system user information (Identity Credential/Access Management certificate and PIN code). While EDLS does not specifically collect SSNs from individuals, they may be contained within the text of records processed in investigation and litigation matters, as well as other responsive record requests.

Since EDLS has the potential to process ESI pertaining to any matter in the scope of FDIC's mission, the PII contained in the system could relate to various categories of individuals, including FDIC employees and contractors, employees of other government agencies, or members of the public, such as bank officers, employees, customers, vendors (e.g., law firms, appraisers and accountants hired by open or closed banks), and depositors, or individuals who file complaints with or against FDIC (complainants).

Note: The following list of PII elements is not intended to be exhaustive. As explained above, the specific PII contained in EDLS varies based on the nature of a particular legal matter or other e-discovery request.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☒	☐
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☒	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☒	☐
Criminal Information	☒	☐
Military Status and/or Records	☒	☐
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒	☐
Photographic Identifiers (e.g., image, x-ray, video)	☒	☐
Other (Specify: System User Information)	☒	☐

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

FDIC obtains the information stored in EDLS from a variety of internal and external sources as necessary to support litigation and other e-discovery requirements. Such sources may include, but are not limited to, any FDIC recordkeeping systems, such as FDIC Business Data Services (FBDS), Regional Automated Document Distribution and Imaging (RADD), Virtual Supervisory Information on the Net (ViSION); FDIC repositories for consumer complaint and call center data; FDIC employees and contractors who are custodians of potentially relevant information; FDIC outside counsel; other Federal or state banking or law enforcement agencies; and financial institutions. FDIC also may derive information in EDLS from interviews, subpoenas, documents, research, public records, opposing counsel and other parties involved in legal matters.

FDIC personnel gather the potentially relevant ESI and hardcopy documents pursuant to direction from the Legal Division to produce materials for purposes of litigation or other responsive record requests. FDIC technical support personnel may also search and extract electronic data from all locations where responsive ESI may be stored, such as FDIC desktops, laptops, server shares/file servers (e.g., shared drives), SharePoint, email repositories, and Enterprise Vault. Technical support personnel import/upload responsive documents into EDLS. In cases where EDLS derives information from other FDIC recordkeeping systems, the Legal Division works with the relevant FDIC system owners/program managers to scope and provide specifications for targeted datasets to be retrieved from the respective source systems. They then securely upload the identified data into EDLS.

Note: The following table provides a list of common, potential sources of PII, but is not intended to be exhaustive. As explained above, the specific PII contained in EDLS varies based on the nature of a particular legal matter or other e-discovery request.

Data Source	Description of Information Provided by Source
FDIC Email Communications and Enterprise Vault	FDIC technical support personnel search and retrieve email communications from central agency email repositories and Enterprise Vault, which is the Corporation's email repository and archiving solution used to support litigation discovery and other e-discovery processes. These email communications may include any of the PII elements specified in Section 1.1.
FDIC desktops, laptops, server shares, SharePoint sites	FDIC technical support personnel identify and extract ESI-Native files, text, images, and other relevant ESI from FDIC desktops, laptops, server shares, and SharePoint sites. This data may include any of the PII elements specified in Section 1.1. (Note: Information may be hardcopy in very limited circumstances, but the desired and default format is electronic.)
Hardcopy examination work papers	FDIC technical support personnel coordinate with relevant FDIC program offices to identify and collect relevant examination work papers, Reports of Examination, and other information related to examinations. The hardcopy examination papers may include any of the PII elements specified in Section 1.1, but generally do not include biometrics, education records or medical information.
FDIC Business Data Services (FBDS)	FDIC technical support personnel coordinate with relevant FDIC system owners/program managers to extract imaged and native ESI related to failed financial institutions from FBDS. This data may include any of the PII elements specified in Section 1.1.
Regional Automated Document Distribution and Imaging (RADD)	FDIC technical support personnel coordinate with relevant FDIC system owners/program managers to extract ESI pertaining to examinations from examiner emails, electronic work papers and digital Reports of Examination stored in RADD. This ESI may include any of the PII elements specified in Section 1.1, but generally does not include biometrics, education records or medical information.
Virtual Supervisory Information on the Net (ViSION)	FDIC technical support personnel coordinate with relevant FDIC system owners/program managers to extract examination data from ViSION. This ESI may include any of the PII elements specified in Section 1.1, but generally does not include biometrics, education records or medical information.
Consumer Complaint and Call Center Information	FDIC technical support personnel collect ESI data from FDIC repositories that store consumer complaint information and call center data. This ESI has the potential to include any of the PII elements specified in Section 1.1.
State Regulators	FDIC may collect or receive ESI from joint exams and correspondence with state regulators. Additionally, state law enforcement agencies or state bank regulatory agencies may contribute paper or electronic data to EDLS. They provide the information to Legal Division attorneys or other authorized FDIC staff via encrypted containers or encrypted files within such containers. Technical support personnel within the Legal Division import the information into EDLS. This ESI has the potential to include any of the PII elements specified in Section 1.1. Data sharing agreements are in place with each agency as applicable.
Other Government Agencies	EDLS may contain email correspondence sent to the FDIC from other government agencies. FDIC also may collect paper and electronic data from other government agencies, such as the U.S.

	Department of Justice, Federal Trade Commission, the Federal Bureau of Investigations, Security and Exchange Commission, U.S. Attorneys' Offices, law enforcement agencies and other bank regulatory agencies. These agencies provide this information to the Legal Division attorneys or other authorized staff via encrypted containers (e.g., encrypted hard drives) or encrypted files within such containers. This ESI has the potential to include any of the PII elements specified in Section 1.1. FDIC technical personnel upload this information to EDLS. Data sharing agreements are in place with each agency, as applicable.
Miscellaneous and Other Third-Party Sources	On occasion, external parties involved in a legal matter, such as the FDIC outside counsel, opposing counsel, or other stakeholders, will provide paper or electronic data to Legal Division attorneys or other authorized FDIC staff via encrypted containers or encrypted files within such containers. Technical support personnel within the Legal Division import the information into EDLS. FDIC also may derive information in EDLS from interviews, subpoenas, documents, research, public records, opposing counsel and other parties involved in legal matters. This information may include any of the PII elements specified in Section 1.1.

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

FDIC has authorized these e-discovery and litigation systems.

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.

EDLS receives and processes information, including PII, from other FDIC record systems that are covered by Privacy Act Systems of Records Notices (SORNs). FDIC-002, Financial Institution Investigative and Enforcement Records;[17] FDIC-005, Consumer Complaint and Inquiry Records;[18] FDIC-009, Safety and Security Incident Records;[19] FDIC-012, Financial Information Management Records;[20] FDIC-013, Insured Financial Institution Liquidation Records;[21] FDIC-015, Personnel

[17] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[18] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[19] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[20] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[21] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

Records;[22] FDIC-018, Grievance Records;[23] and FDIC-022, Freedom of Information Act and Privacy Act Request Records.[24]

The context of the data being analyzed by the EDLS tools determines the applicable SORN. For example, any records relating to a FOIA/PA request would be covered by the Freedom of Information Act and Privacy Act Request Records SORN,[25] whereas any records relating to consumer complaints would be covered by the Consumer Complaint and Inquiry Records SORN[26] and any records relating to an enforcement action would be covered by the Financial Institution Investigative and Enforcement Records SORN.[27] The FDIC Identity, Credential and Access Management Records SORN[28] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of the EDLS tools and resources by authorized individuals.

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

Not applicable. The system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

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."

Since EDLS serves as a repository for information collected from other agency record systems and third-party sources for purposes of litigation and e-discovery, it is not always possible or practical to provide notice to individuals prior to the collection and processing of their information within EDLS. Nonetheless, the FDIC provides notice to individuals at the original point of collection wherever possible. For example, in cases where EDLS imports or derives PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. In addition, this PIA serves as notice to the public about FDIC's collection and use of information in EDLS.

When EDLS receives data from a financial institution, government agency or other third-party entity, it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection.

When information is collected from internal FDIC systems for internal investigations or for the defense of suits brought against the agency, agency personnel are informed that FDIC's computing systems are monitored and that personal information may be collected. Notices are provided to FDIC

[22] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[23] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[24] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[25] Ibid.
[26] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[27] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[28] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

personnel at logon and are also conveyed in FDIC policy documents and during employee training as applicable.

When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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

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

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Since EDLS supports a secondary collection of information from other agency recordkeeping systems and third-party sources for litigation and e-discovery purposes, the FDIC does not always have the ability to provide individualized notice prior to the collection and use of PII within EDLS. Therefore, individuals may not be aware that their data has been provided to FDIC or processed by EDLS.

Mitigation: The FDIC provides notice to individuals at the original point of collection wherever possible. For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. This PIA serves as notice to the public about FDIC's collection and use of information in EDLS.

In instances where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals through the respective SORNs and Privacy Act Statements for the source systems. Such record systems typically include: FDIC-002, Financial Institution Investigative and Enforcement Records;[29] FDIC-005, Consumer Complaint and Inquiry Records;[30] FDIC-009, Safety and Security Incident Records;[31] FDIC-012, Financial Information Management Records;[32] FDIC-013, Insured Financial Institution Liquidation Records;[33] FDIC-015, Personnel Records;[34] FDIC-018, Grievance Records;[35] FDIC-022, Freedom of Information Act and Privacy Act Request Records;[36] and FDIC-035, Identity, Credential and Access Management Records SORN.[37] The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and 12 C.F.R. § 310.3 and 310.4. The FDIC publishes access

[29] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[30] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[31] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[32] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[33] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[34] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[35] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[36] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[37] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

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.

When EDLS receives data from a financial institution, government agency or other third-party entity, it is incumbent upon the bank or agency to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection.

When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. On occasions when notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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?

Because EDLS serves as a repository for records gathered from other agency recordkeeping systems and third-party sources pursuant to litigation and e-discovery requirements, it is not designed and does not have procedures to allow individuals to access their information. However, in cases where EDLS processes information about individuals imported from other FDIC Privacy Act systems of records (SORs), the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and 12 C.F.R. § 310. 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 12 C.F.R. § 310.3 and 310.4. 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. FDIC uses EDLS to (among other things) conduct searches for responsive records for these types of Privacy Act requests. Depending on the nature of the records being processed (and any applicable Privacy Act exemptions), FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal a prospective enforcement or investigative interest on the part of FDIC.

In addition, in some cases, EDLS processes data from financial institutions, government agencies or other third-party entities. The system or project does not have procedures for individual access in these cases. Individuals should contact these source entities directly for access to their personal information.

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

Since EDLS serves as a repository for records gathered from other agency recordkeeping systems and third-party sources pursuant to litigation and e-discovery requirements, EDLS is not designed to allow individuals to correct inaccurate or erroneous information about themselves. Therefore, the system does not have Privacy Act redress procedures. However, in cases where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), the FDIC allows these individuals to correct or amend PII maintained by the FDIC in the respective source systems of records as specified by the Privacy Act and 12 C.F.R. § 310. The procedures for correcting inaccurate data are

provided in related SORNS: FDIC-002, Financial Institution Investigative and Enforcement Records;[38] FDIC-005, Consumer Complaint and Inquiry Records;[39] FDIC-009, Safety and Security Incident Records;[40] FDIC-012, Financial Information Management Records;[41] FDIC-013, Insured Financial Institution Liquidation Records;[42] FDIC-015, Personnel Records;[43] FDIC-018, Grievance Records;[44] FDIC-022, Freedom of Information Act and Privacy Act Request Records;[45] and FDIC-035, Identity, Credential and Access Management Records SORN.[46] Individuals seeking to correct inaccurate data in the source systems can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. These requests are subject to any applicable Privacy Act exemptions intended to prevent harm to FDIC's investigation and enforcement interests. In addition, the EDLS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In cases where EDLS receives third-party data from banks or government agencies, the FDIC does not have the ability to implement procedures to allow individuals to correct inaccurate or erroneous information within EDLS. Individuals should contact their bank or the government agency directly to correct any erroneous or inaccurate information.

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

Because EDLS processes information about individuals derived from other FDIC Privacy Act systems of records, the FDIC allows these individuals to be notified about procedures to correct or amend PII maintained in the respective source systems as specified by the Privacy Act and 12 C.F.R. § 310. The notification procedures are provided in related SORNS: FDIC-002, Financial Institution Investigative and Enforcement Records;[47] FDIC-005, Consumer Complaint and Inquiry Records;[48] FDIC-009, Safety and Security Incident Records;[49] FDIC-012, Financial Information Management Records;[50] FDIC-013, Insured Financial Institution Liquidation Records;[51] FDIC-015, Personnel Records;[52] FDIC-018, Grievance Records;[53] FDIC-022, Freedom of Information Act and Privacy Act Request Records;[54] and FDIC-035, Identity, Credential and Access Management Records SORN.[55] Individuals seeking to correct inaccurate data can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. In addition, the EDLS PIA is published on

---

[38] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[39] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[40] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[41] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[42] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[43] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[44] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[45] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[46] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[47] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[48] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[49] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[50] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[51] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[52] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[53] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[54] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[55] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In some cases, EDLS processes data from banks, government agencies or other third-party entities. The system or project does not have procedures for individual access in such cases. Individuals should contact these entities directly for access to their personal information.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There is a risk that individuals are not able to access and amend information about themselves within EDLS.

Mitigation: Since EDLS serves as a repository for records gathered from other agency recordkeeping systems and third-party sources to satisfy e-discovery and litigation requirements, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), individuals seeking to access or amend any record contained in those SORs may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or FOIA (for all individuals) request to FDIC in writing or electronically at www.fdic.gov/policies/privacy/request.html. However, depending on the nature of the records being processed and any applicable Privacy Act exemptions, FDIC may be unable to provide individual access to records as they could inform the subject of an ongoing investigation or reveal an investigative or enforcement interest on the part of FDIC. In cases where EDLS receives PII from financial institutions or other government agencies, individuals should contact the source entities and agencies that originated their data to access and amend their information.

Section 4.0: Accountability

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

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

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

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

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

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

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

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

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy. 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 a contractor have with the design and maintenance of the information system or project?

Contractors may be employed to provide support and maintenance of systems and tools within the EDLS suite. Additionally, the FDIC contracts with vendors under a Basic Ordering Agreement (BOA) to obtain legal support services and products for electronically processing, hosting, and storing information related to FDIC investigations, inspections, and litigation activities. These Outsourced Litigation Support Services (OLSS) vendors perform a number of tasks in support of FDIC enforcement, bankruptcy, corporate, professional liability, and inherited litigation matters. The vendors process and host data collected from internal FDIC data sources, as well as open or closed banks pursuant to litigation or investigations. Specific services are addressed in the Statement of Objectives (SOO) included in each vendor's contractual agreement with FDIC, and may include the following activities, some of which may involve accessing or utilizing PII: document acquisition, preparation, and unitization; database creation and data quality control; electronic data acquisition and processing; pre-trial and trial support; forensic services; managed legal review; managed data hosting, including secure hosting of data for access by FDIC (or others as designated by FDIC); administration and support of web-based database/legal review applications; documenting procedures; and performing quality control.

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

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

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

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

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy

Program is currently in the process of implementing a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

All EDLS tools are required to undergo, at minimum, a privacy threshold analysis to ensure compliance with this PIA and other applicable FDIC policies. The EDLS tools and platforms have the ability to audit successful and unsuccessful logon attempts and user activity in the system. These audit logs capture account management events, policy change, privilege use, data access, data deletions, data changes, data printing/tagging and exports, permission changes, and all administrator activity. System administrators and other designated users can access and review these audit logs to identify unauthorized use of EDLS and take any necessary corrective actions. For litigation matters, the federal courts provide an additional control regarding the unauthorized disclosure, dissemination, or re-dissemination of PII or privileged information.

Additionally, FDIC personnel access EDLS tools from their FDIC-issued devices, which are encrypted. In cases where data is hosted in the cloud, each cloud instance must undergo and adhere to FDIC privacy/security requirements outlined in FDIC policy and contractual agreements, as applicable. EDLS system owners/program managers within the Legal Division control who may access EDLS tools and data. Access is determined on a "need to know" basis and managed through the FDIC's identity access management system and in accord with FDIC's information security and privacy policies and procedures.

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

The Legal Division provides users with e-discovery and litigation procedures, resources and training materials as applicable. Legal also provides users with system-specific training for certain EDLS systems and tools to which they have access. All FDIC users who have EDLS access must complete required annual security and privacy awareness training that covers the rules of behavior. These rules, in addition to FDIC Corporate policies, establish user responsibility and accountability.

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

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

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

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

Privacy has been integrated within the FDIC 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. FDIC also has implemented technologies to track, respond, remediate and report on breaches, as well as to track and manage PII inventory.

Only authorized FDIC personnel and partners are granted access to EDLS. These users access the EDLS platforms using dual factor authentication. FDIC personnel log in with user names and are validated using a dual factor authentication method which is selected by FDIC and integrated with the OLSS vendors' environments, as applicable. EDLS also terminates sessions after a certain period of inactivity. Users are given system access to the least amount of information needed to perform their work duties. The EDLS tools and platforms have the ability to audit successful and unsuccessful logon attempts and user activity in the system. These audit logs include account management events, policy change, privilege use, data access, data deletions, data changes, permission changes, and all administrator activity.

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and 12 C.F.R. § 310. Disclosures are tracked and managed using the FDIC's FOIA solution.

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

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and 12 C.F.R. § 310.

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. § 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for the system.

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 Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws and regulations: 12 U.S.C. §§ 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1828, 1829, 1831, and 1832; Executive Order 9397, as amended; and 12 CFR parts 330 and 366. The context of the records being analyzed determines the specific legal authority that permitted their original collection. Additionally, the nature and context of the data dictates whether/which FDIC system of records notice (SORN) applies. For example, any records relating to a FOIA/PA request would be covered by

the Freedom of Information Act and Privacy Act Request Records SORN,[56] whereas any records relating to complaints would be covered by the Consumer Complaint and Inquiry Records SORN[57] and any records relating to an enforcement action would be covered by the Financial Institution Investigative and Enforcement Records SORN.[58] The FDIC Identity, Credential and Access Management Records SORN[59] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of the EDLS tools and resources by authorized individuals.

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

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

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

EDLS only collects information for which the FDIC has the authority to collect and pursuant to litigation discovery or other e-discovery or responsive document requests. EDLS leverages 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. This includes limiting access to the EDLS tools and data contained therein to only those authorized users with a need-to-know. Additionally, the EDLS tools have the capability to generate a robust audit trail of all user activity, as detailed above in Section 4.

Further, through the conduct, evaluation and review of privacy artifacts,[60] 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?

All FDIC personnel are required to complete annual information security and privacy awareness training. This is required for EDLS end users prior to gaining access to the system. This online training addresses how to determine what constitutes PII and how to handle it. In addition, breach prevention is addressed in the training. The EDLS tools and platforms have built-in user security features to help manage and restrict what information users have access to on a "need-to-know"

[56] Ibid.
[57] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[58] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[59] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[60] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).

basis and according to their work responsibilities. These user security permissions are controlled by EDLS system administrators.

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. Whenever possible, users access information in the originating systems. Information is not uploaded into EDLS except as needed to support authorized business purposes as described above.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of data in this information system? or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

FDIC maintains data in EDLS for the duration of the legal matter. The law or ruling also establishes the retention guidelines. FDIC also retains the records in EDLS in accord with FDIC Records Retention Schedules and follows guidance on permanent and temporary records disposition issued by the National Archives and Records Administration (NARA). Legal certifies when records can be destroyed. However, due to business rules and storage limits within the EDLS tools, the records that are uploaded to and processed may be deleted from some of the tools after processing and production. Occasionally, there will be times when records are kept in EDLS due to ongoing litigation. To ensure that storage limits are not reached, users receive periodic housekeeping notices to review any maintained files and delete those no longer needed.

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.

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 utilize 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 EDLS could over-collect PII, as well as aggregate disparate PII from different sources.

Mitigation: EDLS collects and aggregates information as necessary to satisfy e-discovery and litigation requirements. EDLS only processes information for which FDIC already has the authority to collect and

pursuant to litigation discovery or other responsive document requests. In cases where EDLS derives information from other FDIC recordkeeping systems, Legal works with the relevant FDIC system owners/program managers as appropriate to scope and provide specifications for targeted datasets to be retrieved from the respective source systems. Additionally, FDIC restricts access to EDLS tools to those who have a need to use them in order to perform authorized business duties. EDLS tools also utilize role-based permissions to limit user access to data, including PII, on a need-to-know basis. Further, the EDLS tools have the ability to generate audit trails of all user activity, including the viewing of records in the system.

Privacy Risk: There is a risk that information will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: FDIC maintains the records in EDLS according to the records schedules and policies discussed in Section 6, and disposes of them accordingly. Legal certifies when records can be destroyed. However, due to business rules and storage limits within the EDLS tools, the records that are uploaded to and processed may be deleted from some of the tools after processing and production. Occasionally, there will be times when records are kept in EDLS due to ongoing litigation. To ensure that storage limits are not reached, users receive periodic housekeeping notices to review any maintained files and delete those no longer needed.

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 utilize 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.

FDIC reviews information collected as part of its investigation, enforcement and other mission activities to ensure it is accurate, complete and timely as required by the particular activity. As applicable, FDIC staff may perform research to verify the accuracy and completeness of the information they obtain and/or require the individual submitting the information to certify the accuracy of the information (e.g., witness or financial statements in court cases). However, in most cases, EDLS does not collect personal information directly from individuals, but instead receives copies of records obtained from other FDIC recordkeeping systems and third-party sources. Therefore, FDIC relies on the FDIC program or entity that originally collected the information to ensure the accuracy and completeness of PII. Additionally, FDIC does not use the EDLS tools as an authoritative source for PII about individuals or use the tools to alter PII in the original records. Any inaccurate or incomplete information, when identified, can be corrected in the source systems as described earlier in Section 3.

Further, information incorporated into EDLS system is subject to appropriate security and chain-of-custody control as appropriate to protect sensitive information, including PII, from undue compromise, loss or alteration and to assure the integrity of evidentiary materials from the point at which they are included in EDLS. EDLS tools are able to log data modifications and provide usable audit trails.

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

Since EDLS serves as a repository for information collected from other agency record systems and third-party sources for purposes of litigation and e-discovery, EDLS does not typically collect information directly from individuals. In cases where EDLS processes information about individuals imported from other FDIC Privacy Act systems of records, the FDIC allows these individuals to correct or amend PII maintained by the FDIC in these respective systems of records as specified by the Privacy Act and 12 C.F.R. § 310. The procedures for correcting inaccurate data are provided in related SORNS: FDIC-002, Financial Institution Investigative and Enforcement Records;[61] FDIC-005, Consumer Complaint and Inquiry Records;[62] FDIC-009, Safety and Security Incident Records;[63] FDIC-012, Financial Information Management Records;[64] FDIC-013, Insured Financial Institution Liquidation Records;[65] FDIC-015, Personnel Records;[66] FDIC-018, Grievance Records;[67] FDIC-022, Freedom of Information Act and Privacy Act Request Records;[68] and FDIC-035, Identity, Credential and Access Management Records SORN.[69] Individuals seeking to correct inaccurate data can submit their request to the Legal Division, FOIA & Privacy Act Group, in accordance with FDIC regulations in 12 CFR Part 310. In addition, the EDLS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office. When EDLS receives third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact these entities directly to correct any erroneous or inaccurate information.

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 PIAs and SORNs 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 utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer 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?

---

[61] FDIC SORN-002, Financial Institution Investigative and Enforcement Records, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/policies/privacy/sorns.html.
[62] FDIC SORN-005, Consumer Complaint and Inquiry Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[63] FDIC SORN-009, Safety and Security Incident Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[64] FDIC SORN-012, Financial Information Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[65] FDIC SORN-013, Insured Financial Institution Liquidation Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[66] FDIC SORN-015, Personnel Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[67] FDIC SORN-018, Grievance Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[68] FDIC SORN-022, Freedom of Information Act and Privacy Act Request Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.
[69] FDIC SORN-035, FDIC Identity, Credential and Access Management Records, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/policies/privacy/sorns.html.

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 potential risk associated with data quality and integrity because information processed by the EDLS tools could be inaccurate or incomplete.

Mitigation: EDLS serves as a repository for reviewing and tagging records obtained from other agency recordkeeping systems and third-party sources in support of FDIC litigation and e-discovery requests. By design, therefore, EDLS contains only copies of records from these originating systems and sources and typically does not collect information directly from individuals. The processing of information by the EDLS tools does not alter the original records in the source systems. Any inaccurate information, when identified, can be corrected in the source systems. Additionally, FDIC reviews information collected as part of its investigation, enforcement and other mission activities to ensure it is accurate, complete and timely as required by the particular activity. Information incorporated into EDLS system is subject to appropriate security and chain-of-custody control as appropriate to protect sensitive information, including PII, from undue compromise, loss or alteration and to assure the integrity of evidentiary materials from the point at which they are included in EDLS. EDLS tools are able to log data modifications and provide usable audit trails.

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.

Since EDLS serves as a repository for information collected from other agency record systems and third-party sources for purposes of litigation and e-discovery, it is not always possible or practical to provide notice and choice opportunities to individuals prior to the collection and processing of their information within EDLS. Wherever feasible, FDIC provides notice and relevant consent options to individuals at the original point of collection. For example, in cases where EDLS imports or derives PII from other FDIC record systems, the FDIC provides notice to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When EDLS receives third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. 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.

For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. In addition, this PIA serves as notice to the general public about FDIC's collection and use of information in EDLS.

When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice (or consent opportunities) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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.

As detailed above in Section 8.1, the system serves as a repository for information collected from other agency record systems and third-party sources for litigation and e-discovery purposes. Therefore, opportunities for providing individualized notice and consent options may be limited or non-existent. In cases where EDLS imports or derives PII from other FDIC record systems, the FDIC provides notice and consent opportunities to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When EDLS receives third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. 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.

When EDLS receives third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. 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.

For information that is collected pursuant to a request from the FDIC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). Litigants in civil cases are made aware that courts may compel FDIC to search for and produce agency records pertaining to them and their claims during the litigation process. In addition, this PIA serves as notice to the general public about FDIC's collection and use of information in EDLS.

When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice (or the opportunity to consent) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice cannot be provided or is not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

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.

As discussed above, EDLS serves as a repository for information collected from other agency record systems and third-party sources for litigation and e-discovery purposes. Therefore, opportunities for providing individualized notice and consent options may be limited or non-existent. In cases where EDLS imports or derives PII from other FDIC record systems, the FDIC provides notice and consent opportunities to individuals at the original point of collection through the respective Privacy Act Statements, SORNs, and PIAs, as applicable, for those source systems. This notice explains the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

When EDLS receives third-party data from a financial institution, government agency or other entity, the FDIC does not have the ability to provide privacy notices prior to the agency's processing of individuals' PII. In such cases it is incumbent upon the source entity to provide any applicable, required notices to the individuals from whom they collected the information. 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.

Refer to Section 8.1 for additional details on how the system 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.

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

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

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There is risk related to individual participation for EDLS because data is not always collected directly from individuals. Individuals may not be aware and/or have provided explicit consent for the collection and use of their information within EDLS.

Mitigation: This PIA serves as notice to the general public regarding the collection and use of information in EDLS to fulfill FDIC's corporate and receivership responsibilities. In addition, FDIC provides notice and consent options to individuals at the original point of data collection wherever possible. Specifically, in cases where EDLS imports or derives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals at the original point of collection through the respective SORNs and Privacy Act Statements (PAS) for those source systems. In cases where PII is received from third-parties, such as financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. When FDIC collects information pursuant to discovery or a related court order or as part of an ongoing investigation, individuals may not receive notice (or the opportunity to consent) as to how their information will be used or disclosed. The use and disclosure of this information is governed by applicable federal law, discovery rules, and court orders. When notice and/or consent opportunities cannot be provided or are not required, the FDIC provides constructive notice through its general Privacy Policy and PIAs, including this one.

Section 9.0: Purpose and Use Limitation

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

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

The EDLS suite collects, processes and maintains PII as necessary to satisfy a wide-variety of litigation and other e-discovery requirements and requests, such as resolving FDIC Corporate and Receivership legal matters, conducting internal investigations, and responding to litigation discovery, subpoenas and other requests for responsive materials, such as Freedom of Information Act (FOIA)/Privacy Act (PA), Government Accountability Office (GAO), and Congressional requests.

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.

Supervisory attorneys in the Legal Division assign attorneys and paralegals to individual cases and matters. The assigned attorneys and paralegals are responsible for ensuring a complete and diligent discovery search, preservation, collection, and production of relevant records, as applicable. They have access to records gathered and imported into EDLS in preparation for trials/litigation and to resolve legal matters, and to respond to other e-discovery or responsive record requests. The attorneys and paralegals sort and search the data, as well as review the records for relevance and for the potential need to redact PII and/or confidential information. FDIC attorneys and paralegals also take case data to trials or hearings using secure, FDIC-issued laptops. FDIC Legal Information Technology Unit (LITU) personnel have access in order to assist with importing and uploading information to EDLS and to conduct other system administration functions such as adding users to the system, system upgrades, and troubleshooting user reported problems.

Authorized staff from the FDIC Legal Division, Division of Resolutions and Receiverships (DRR), Division of Risk Management Supervision (RMS), and other FDIC Divisions/Offices who serve as case reviewers have access to EDLS. In addition, a limited number of uses in the FDIC Division of Information Technology (DIT) may have access to certain systems/tools within the EDLS suite for system administration and troubleshooting purposes. They generally are unable to view/access the EDLS database containing PII.

Additionally, the FDIC contracts with vendors under a Basic Ordering Agreement (BOA) to obtain legal support services and products for electronically processing, hosting, and storing information in EDLS related to FDIC investigations, inspections, and litigation activities. These Outsourced Litigation Support Services (OLSS) vendors perform a number of tasks in support of FDIC enforcement, bankruptcy, corporate, professional liability, and inherited litigation matters. The vendors process and host data collected from internal FDIC data sources, as well as open or closed banks pursuant to litigation or investigations. Specific services are addressed in the Statement of Objectives (SOO) included in each vendor's contractual agreement with FDIC, and may include the following activities, some of which may involve accessing or utilizing PII within EDLS: document acquisition, preparation, and unitization; database creation and data quality control; electronic data acquisition and processing; pre-trial and trial support; forensic services; managed legal review; managed data hosting, including secure hosting of data for access by FDIC (or others as designated by FDIC); administration and support of web-based database/legal review applications; documenting procedures; and performing quality control.

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

The EDLS system owners/program managers serve as the primary source of information for data definition and data protection requirements and are responsible for supporting FDIC's corporate-wide view of data sharing. Additionally, all FDIC employees and Outside Counsel firms who have authorized access to information in EDLS bear responsibility for assuring proper use of the data and abiding by the FDIC data protection rules. These rules are outlined in any system-specific training provided for the tools and platforms within the EDLS suite. Additionally, all users with access to the system must complete annual Information Security and Privacy Awareness Training. This training has specific information regarding the compromise of data and the prevention of misuse of data.

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

EDLS users are granted access to specific roles set within the EDLS tool suite. All internal and external users who have access to EDLS must have the approval of their Manager/Supervisor, as applicable, and the FDIC Program Manager/System Owner for the EDLS tool to which they require access. Additionally, the functional security of the EDLS tool suite limits a user's access to specific functions and regulates a user's ability to update data for a specific function based on job responsibilities and limited to information needed to perform position duties.

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. The EDLS suite does not have any automated interconnections with other FDIC recordkeeping systems.

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?

EDLS aggregates data from multiple sources in support of investigatory, litigation and enforcement actions. This aggregation may result in the creation of new evidentiary information about an individual, which may be used in legal matters. Refer to Sections 3 and 4 for additional information about the controls in place to protect data from unauthorized access or use.

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 may need to produce and share EDLS data with courts, opposing counsel, defendants, law enforcement partners, bank regulatory agencies, vendors, or other entities or individuals as authorized or required by law. When the FDIC shares information with external entities, it typically does so pursuant to non-disclosure agreements, memorandums of understanding, court-approved protective orders, and/or contractual agreements with privacy and security provisions or similar data protection controls.

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 Information Security and Privacy Awareness Training is mandated for all FDIC users of EDLS. In addition, training specific to certain EDLS tools is provided to users of those tools. Users are not granted access until the training is completed. Contractors also must complete the Information Security and Privacy Awareness Training, which includes Rules of Behavior.

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

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

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a risk that PII maintained in EDLS could be accessed or used inappropriately or for unauthorized purposes.

Mitigation: To help prevent unauthorized access and use of information, EDLS employs role-based permissions to restrict access to EDLS and the data contained therein to only authorized FDIC personnel who have a "need-to-know" in order to fulfill their job responsibilities. EDLS system/tool administrators grant access to users, and each individual user must be properly credentialed. In addition, all users are subject and must adhere to agency policies and procedures for using, sharing and safeguarding PII. All users receive annual Information Security and Privacy Awareness training, as well as specialized training, as applicable, which helps ensure PII is handled and safeguarded appropriately. The EDLS tools and platforms generate and maintain detailed audit logs that are capable of capturing any user's unauthorized use of information contained within the tool suite. EDLS system administrators periodically review these logs and when there is a confirmed or suspected compromise of information.

Additionally, EDLS limits the access and permission rights of users outside of the Legal Division, such as FDIC employees in other Divisions, opposing counsel, outside counsel, and contractor staff. By default, such users may only review and tag documents within certain EDLS platform(s) to which the Legal Division has granted them access, and they are prohibited via technical and administrative controls from editing or deleting documents. Permission to perform any other activities outside of reviewing and tagging must be expressly approved by the Legal Division. Based on circumstances or agreements with opposing counsel or other participants, rights to print or download ESI is only granted for subsets of data upon request and approval from the Legal Division.

Privacy Risk: There is a risk that uses or disclosures of information in EDLS could be incompatible with the original purposes for which the information was collected.

Mitigation: Any disclosures of information processed by EDLS occur outside of the system itself. Therefore, EDLS is not designed to capture or record information sharing. However, because EDLS restricts access to data to users with a "need-to-know" who require the information to perform their job responsibilities, any disclosures outside of EDLS are initiated by authorized FDIC personnel who have a responsibility to share the information for purposes that are compatible with the purpose for which the PII was originally collected and/or that are otherwise legally authorized or required by statute, federal court rules, or responsive document requests. Any information disclosures or withholdings are made based on the nature of the records and, as applicable, pursuant to the routine uses and exemptions in the SORNs that cover those records.

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

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

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

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

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

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks associated with security for the system.

Mitigation: No mitigation actions are recommended.