FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
LEGAL RESEARCH AND MATTERS MANAGEMENT SOLUTIONS (LRMMS)

OCISO

May 18, 2023

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

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

SYSTEM OVERVIEW

Describe what this information system[2] does in terms of purpose, functionality, and PII collection/use. What is the goal of the system? What gap does it serve to close?

Synopsis

The FDIC Legal Division (Legal) leverages several information technology (IT) systems and platforms, herein referred to as the Legal Research and Matters Management Solutions (LRMMS), to manage, research and report on FDIC legal matters. LRMMS allows Legal staff to track and share information regarding the conduct and progress of FDIC legal matters. LRMMS also provides legal research and drafting functionality, as well as shared document management repositories, allowing users to upload and attach copies of files, documents or other content compiled or generated in a matter. FDIC has conducted this Privacy Impact Assessment (PIA) because LRMMS uses and maintains personally identifiable information (PII).

Background

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.

[1] www.fdic.gov/privacy

[2] OMB Circular No. A-130, "Managing Information as a Strategic Resource," (July 27, 2016). The Circular defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

The FDIC's Legal Division handles nationwide litigation involving the FDIC in both its Corporate and Receivership capacities, and is responsible for litigating, overseeing, and monitoring all appeals in which the FDIC in any capacity is a party or has an interest. The Legal Division also provides legal advice and counsel to all business lines on a myriad of regulatory and policy initiatives and various other legal matters related to Corporate and Receivership activities. The Federal Deposit Insurance (FDI) Act, including but not limited to 12 U.SC. 1819, 12 U.S.C. 1820, 12 U.S.C. 1821, and 12 U.S.C. 1822, provides broad authority for FDIC to conduct these matters.

The types of matters tracked by the Legal Division and subject to this PIA generally fall into the following categories:

- **Supervision, legislation and enforcement matters**, which includes matters relating to FDIC's supervision[3] of insured depository institutions and the pursuit of enforcement actions[4] to promote compliance with risk-management, safety and soundness, consumer protection, and related laws and regulations. Legal also provides legal counsel on deposit insurance and assessment matters, legislation, regulations, supervisory appeals, and related issues, as well as provides legal counsel regarding the FDIC's risk-management and consumer compliance supervision of State nonmember banks and other insured depository institutions.

- **Litigation matters**, which refers to matters that are prepared for and managed through a court procedure or formal complaint process. Legal provides litigation support for all FDIC business lines in all trial and appellate courts. Legal also handles "open bank" related litigation matters, as well as coordinates with the Division of Resolutions and Receiverships (DRR) to pursue civil professional liability claims[5] against professionals and directors and officers of failed financial institutions.

- **Resolution and receivership matters**, which relate to the FDIC's resolution and receivership activities,[6] ranging from accepting appointment to termination of receivership, as well as sales and other dispositions of assets from the receiverships, resolution planning, and responsibilities related to complex financial institutions.

- **Corporate operation and miscellaneous matters**, which includes Corporate and governance matters related to, for example, agency authority, ethics, IT security/privacy and legal information management, labor and employment, procurement and outside counsel management, and risk management and internal controls.

---

[3] www.fdic.gov/resources/supervision-and-examinations/
[4] www.fdic.gov/regulations/examinations/enforcement-actions/
[5] www.fdic.gov/resources/resolutions/professional-liability/annual-reports.html
[6] www.fdic.gov/resources/resolutions/

The Legal Division manages and tracks FDIC legal matters, which includes administrative activities such as logging the matter into LRMMS, assigning the matter to an appropriate FDIC attorney, tracking key deadlines and updates, and closing out the matter within LRMMS. As part of managing legal matters, the FDIC may collect and maintain a significant amount of data, including PII. Such PII could relate to FDIC employees and contractors, employees of other government agencies, or members of the public, such as bank officers, employees, customers, depositors, vendors (e.g., law firms, appraisers and accountants hired by open or closed banks), and any other external parties who are involved or associated with FDIC legal matters. The PII in LRMMS varies depending on the nature of the particular matter being tracked and reported on by the Legal Division. The section below provides additional information about the specific systems and platforms that comprise LRMMS and the type of data maintained within each.

Overview of LRMMS

The Legal Division utilizes a collection of systems and platforms, referred to herein as 'LRMMS,' to manage, research and report on FDIC legal matters. LRMMS allows Legal staff to track and share information regarding the conduct and progress of FDIC legal matters, as well as to identify and assign the personnel and resources necessary to conduct each matter. Additionally, LRMMS supports legal research and drafting activities, and provides shared document management repositories, allowing users to upload and attach copies of files, documents or other content compiled or generated in a matter.

The following systems and platforms comprise LRMMS and serve the purposes outlined below:

Advanced Legal Information System (ALIS)

The Advanced Legal Information System (ALIS) is the Legal Division's principal information system, containing all types of information related to the Legal Division's business functions, such as records of matters, people, organizations, events, narratives, invoices, and budgets. It is a highly configurable, externally hosted, web-based application that integrates the Division's matter management, budgeting, and invoice processing into a single application. While it is used to process invoice data, it does not produce or process payments. The application has strong search and reporting capabilities.

The primary types of information collected and maintained within ALIS include open and closed bank data, subsidiary data, invoice data, vendor data, FDIC internal organization data, professional liabilities recoveries data and Legal employee and timekeeping data. ALIS does not require the collection or maintenance of Social Security numbers (SSNs); however, in cases where an Outside Counsel firm (vendor) is a sole proprietor, their Tax Identification Number (TIN) could be their SSN.

The Outside Counsel relationship is managed within ALIS via a secure, web-based Collaboration Portal. The Portal facilitates invoice submission and the use of collaboration tools for Outside Counsel firms (i.e., approved e-billing vendors) to submit budget information. Access and authorization for the Portal by Outside Counsel firms requires approval by FDIC, but is managed by the Collaboration Portal's service provider All collaborative information between the Collaboration Portal and the core ALIS server database is securely exchanged via HTTPS and other encryption methods.

ALIS Data

ALIS contains the names of individuals, including FDIC employees and contractors, as well as business Tax Identification Numbers (TINs), associated with official FDIC legal matters. Additionally, information related to FDIC labor and employee disciplinary matters is maintained within ALIS. ALIS also contains various text fields that can be populated with information pertinent to a case, and which could potentially contain sensitive business information and/or PII.

TINs for Outside Counsel firms (vendors) that provide services to FDIC are collected and maintained within ALIS. In the event that a vendor is a sole proprietor, their TIN could be their personal SSN.

ALIS also interfaces with FDIC's Web Time and Attendance (WebTA) and allows Legal Division employees to enter hours spent on matters in WebTA. The hourly time spent by Legal Division employees on specific ALIS matters is imported into ALIS.

In addition, supporting documentation may be attached to invoices and other matters in ALIS. For example, supporting documentation provided by vendors may include invoices and travel receipts, which may contain PII such as names, home addresses, credit card information, and other information pertaining to vendor personnel. Certain Legal Division vendors, referred to as "approved e-billing vendors," log in to the Collaboration Portal of ALIS to submit invoices. Attachments or supplemental information related to FDIC labor/employee disciplinary matters and other official corporate legal matters may include a wide-range of PII, depending on the nature of the matter.

Legal Research Bank (LRB)/Private File & Drafting Assistant

The FDIC subscribes to third-party online legal research services and proprietary databases that provide access to U.S. federal and state law sources, as well as to sources of international law and the laws of a number of other jurisdictions. Sources vary by jurisdiction and may include constitutions, legislation, legislative history, statutory code, regulations, regulatory materials, cases, case digests, citators, public records, law reviews, treatises, and legal news.

The Legal Division uses these third-party services and databases to conduct legal research, as well as to organize and store legal research findings and related case materials, such as briefs, memoranda, court opinions, and correspondence. Legal maintains this information in the "Private File" database of a third-party's cloud-based system referred to herein as the Legal Research Bank. The Legal Research Bank centralizes the Legal Division's legal research findings in a single accessible location and is intended to promote information sharing and reduce duplicate research. Access to data in the Legal Research Bank is restricted to authorized FDIC Legal staff and Outside Counsel on a "need to know" basis. The FDIC retains exclusive ownership of Private File data and documents contained in the Legal Research Bank.

FDIC Legal personnel also utilize a Drafting Assistant tool provided by the aforementioned vendor. The tool formats and proofs legal documents. For example, courts across the country have different formatting requirements for briefs and memoranda. The Drafting Assistant tool can format documents for a specific court. It also can hyperlink citations in a document, pull cited documents en masse, and build a table of authorities.

Legal Research Bank/Private File Data

The Legal Research Bank contains a collection of FDIC-generated legal documents that relate to both open and closed bank matters and to the FDIC in its Corporate and Receivership capacities. Documents include, but are not limited to, Legal Division work product, briefs, opinions, memoranda, interagency agreements, court opinions, and correspondence, some of which may include FDIC information, including PII, and may be subject to attorney-client communication and work product privileges.

Legal Drafting Assistant Data

The Drafting Assistant temporarily retains data on the aforementioned vendor's servers only for long enough for the system to process the information. After that, the servers are scrubbed clean of the information. The information contained in these documents is generally of the same sort referenced above.

FDIC Document Management Repositories

As dictated by business need, the Legal Division utilizes FDIC-authorized data services and document management repositories (e.g., FDIC shared drives, document management sites and databases, collaborative sharing solutions, and enterprise business intelligence tools and platforms) to manage, research and maintain information collected as part of Corporate and Receivership litigation and other legal matters.

FDIC Document Management Repositories Data

The information that Legal maintains in these repositories has the potential to include any manner of PII about internal (FDIC) and external (non-FDIC) parties, as necessary to accomplish authorized FDIC business needs related to legal matters. For example,

the information maintained in certain Legal Division document management sites pertains to Receivership investigations and litigation targeting officers, directors, and employees of open or closed banks; loans made to firms and individuals by open or closed banks; or those hired by open or closed banks (e.g., law firms, appraisers, accountants). Supporting legal artifacts and documentation, such as emails, word processing documents, PDF files, spreadsheets, presentations, database entries, or other documents, may be maintained on the sites. Depending on the nature of the litigation or investigation, the information and documents maintained in these repositories may include PII and other information about defendants/co-defendants, such as such as name, contact information, dates of restitution orders, loan maturity, statute of limitations, and prison release; balances of loans and net assets; and supporting documentation, such as Clear reports, credit reports, financial institution/banking records, and contracts. This supporting documentation may contain names, SSNs, financial information, and other types of PII about individuals. Additionally, these document management repositories may contain the names of FDIC personnel assigned to matters, as well as the names and work contact information for other third-parties involved in legal matters, such as Assistant United States Attorneys, Primary Investigator, Clerk of the Court, and Probation/Parole Officer.

FDIC is conducting this PIA to evaluate and document the impact that LRMMS has on personal privacy. In addition, FDIC has documented in multiple FDIC Systems of Records Notices (SORNs) the records about individuals that are processed or maintained within LRMMS. Such SORNs generally include: FDIC-002, *Financial Institution Investigative and Enforcement Records*;[7] FDIC-012, *Financial Information Management Records*;[8] FDIC-013, *Financial Institution Resolution and Receivership Records*;[9] and FDIC-015, *Personnel Records*.[10] The context of the data being maintained in the respective LRMMS repositories determines the applicable SORN. For example, records in LRMMS relating to labor and employment matters are covered by FDIC-015, *Personnel Records*,[11] whereas records relating to resolution and receivership matters are generally covered by FDIC-013, *Financial Institution Resolution and Receivership Records*,[12] and any records relating to FDIC risk management and

---

[7] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[8] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[9] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[10] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[11] *Ibid.*
[12] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.

supervision matters are covered by FDIC-002, *Financial Institution Investigative and Enforcement Records*.[13] FDIC-041, *Personal Information Allowing Network Operations*,[14] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of LRMMS resources by authorized individuals.

PRIVACY RISK SUMMARY

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

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

Transparency

Privacy Risk: Since LRMMS receives information from other agency recordkeeping systems and third-party sources, rather than directly from individuals, the FDIC does not always have the ability to provide individualized notice prior to the collection and use of PII within LRMMS. Therefore, individuals may not be aware that their data has been provided to FDIC or uploaded to LRMMS.

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 LRMMS.

---

[13] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[14] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

In instances where LRMMS receives 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*;[15] FDIC-012, *Financial Information Management Records*;[16] FDIC-013, *Financial Institution Resolution and Receivership Records*;[17] FDIC-015, *Personnel Records*;[18] and FDIC-041, *Personal Information Allowing Network Operations*.[19] 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 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 LRMMS 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.

Access and Amendment

Privacy Risk: There is a risk that individuals who are subjects of legal matters are not able to access and amend information about themselves within LRMMS.

Mitigation: Since LRMMS processes records from other agency recordkeeping systems and third-party sources in support of FDIC legal matters, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases

---

[15] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[16] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[17] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[18] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[19] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

where LRMMS 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. 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 LRMMS 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.

Minimization

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

Mitigation: FDIC relies on authorized LRMMS users to minimize unnecessary duplication of data. Whenever possible, users access information in the originating systems and only upload information that is necessary to support authorized business purposes. In addition, records in LRMMS are retained in accordance with FDIC policy and a National Archives and Records Administration (NARA)-approved record retention schedule. FDIC's Security and Privacy Control Assessment Team tests applicable controls, including whether systems are adhering to stated retention schedules, as part of continuous monitoring. No additional mitigation actions are recommended.

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

Mitigation: LRMMS collects and aggregates information as necessary to satisfy litigation requirements or otherwise track and resolve FDIC legal matters. LRMMS only processes information for which FDIC already has the authority to collect and pursuant to litigation and other FDIC legal matters. In cases where LRMMS 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 LRMMS to those who have a need to use them in order to perform authorized business duties. LRMMS platforms also utilize role-based permissions to limit user access to data, including PII, on a need-to-know basis. Further, certain LRMMS platforms have the ability to generate audit trails of user activity, including the viewing of records in the system.

Section 1.0: Information System

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

LRMMS maintains a wide-range of FDIC information and PII in support of processing and resolving FDIC Corporate and Receivership legal matters. Depending on the nature of a particular legal matter, the information in LRMMS may relate to or 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 information has the potential to contain any manner of PII, including but not limited to names, dates of birth, SSNs, driver's license/state identification numbers, employee identification number, home addresses, telephone numbers, financial information, email addresses and other types of PII noted in the table below.

Since LRMMS has the potential to process information pertaining to any FDIC legal matter, 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.

Specifically, the systems and platforms that compromise LRMMS may contain the following types of PII:

ALIS

ALIS contains the names of individuals, including FDIC employees and contractors, as well as business Tax Identification Numbers (TINs), associated with official corporate legal matters. Additionally, information related to FDIC labor and employee disciplinary matters is contained within ALIS. ALIS also contains various text fields that can be populated with information pertinent to a case, and which could potentially contain sensitive business information and/or PII.

TINs for Outside Counsel firms (vendors) that provide services to FDIC are collected and maintained within ALIS. In the event that a vendor is a sole proprietor, their TIN could be their personal SSN.

ALIS also interfaces with Web Time and Attendance (WebTA) and allows Legal Division employees to enter hours spent on matters in WebTA. The hourly time spent by Legal Division employees on specific ALIS matters is imported into ALIS.

In addition, Legal personnel may attach supporting documentation to invoices and other matters in ALIS. For example, supporting documentation provided by vendors may include invoices and travel receipts, which may contain PII such as names, home addresses, credit card information, and other information pertaining to vendor personnel. Certain Legal Division vendors log in to the Collaboration Portal to submit invoices. These vendors are referred to as approved e-billing vendors. Attachments or supplemental information related to FDIC labor/employee disciplinary matters and other official corporate legal matters may include a wide-range of PII, depending on the nature of the matter. ALIS does not control what documents or data users can upload or enter into the application. The PII items in the table below reflect those PII elements that may potentially be contained in attachments or supplemental information uploaded into ALIS.

Legal Research Bank/Private File & Drafting Assistant

The Legal Research Bank/Private File contains a collection of FDIC-generated legal documents that relate to both open and closed bank matters and to the FDIC in its Corporate and Receivership capacities. Documents include, but are not limited to, Legal Division work product, briefs, opinions, memoranda, court opinions, and correspondence, some of which may include FDIC information, including PII, and may be subject to attorney-client communication and work product privileges. The Drafting Assistant temporarily retains data, which is similar in nature to that processed by the Legal Research Bank.

FDIC Document Management Repositories

The Legal Division maintains a wide-range of FDIC information related to legal matters within FDIC-approved document management repositories. This information has the potential to include any manner of PII about internal (FDIC) and external (non-FDIC) parties, as necessary to accomplish authorized FDIC business needs related to legal matters. For example, the information maintained in certain Legal Division document management sites pertains to Receivership investigations and litigation targeting officers, directors, and employees of open or closed banks; loans made to firms and individuals by open or closed banks; or those hired by open or closed banks (e.g., law firms, appraisers, accountants). Supporting legal artifacts and documentation, such as emails, word processing documents, PDF files, spreadsheets, presentations, database entries, or other documents, may be maintained on the sites. Depending on the nature of the litigation or investigation, the information and documents maintained in these repositories may include PII and other information about defendants/co-defendants, such as such as name, contact information, dates of restitution orders, loan maturity,

statute of limitations, and prison release; balances of loans and net assets; and supporting documentation, such as Clear reports, credit reports, financial institution/banking records, and contracts. This supporting documentation may contain names, SSNs, financial information, and other types of PII about individuals. Additionally, these document management repositories may contain the names of FDIC personnel assigned to matters, as well as the names and work contact information for other third-parties involved in legal matters, such as Assistant United States Attorneys (AUSA), Primary Investigator, Clerk of the Court, and Probation/Parole Officer.

Note: The following list of PII elements is not intended to be exhaustive. As explained above, the specific PII contained in LRMMS varies based on the nature of a particular legal matter.

PII Element	Yes
Full Name	☒
Date of Birth	☒
Place of Birth	☒
Social Security number (SSN)	☒
Employment Status, History or Information	☒
Mother's Maiden Name	☒
Certificates (e.g., birth, death, naturalization, marriage)	☒
Medical Information	☒
Address	☒
Phone Number(s)	☒
Email Address	☒
Employee Identification Number (EIN)	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report)	☒
Driver's License/State Identification Number	☒
Vehicle Identifiers (e.g., license plates)	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	☒
Education Records	☒

Criminal Information	☒
Military Status and/or Records	☒
Investigation Report or Database	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒
Photographic Identifiers (e.g., image, video)	☒
User Information (e.g., User ID, password)	☒
Specify other: System User Information	☒

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

FDIC obtains the information stored in LRMMS from a variety of internal and external sources in support of managing FDIC legal matters. Such sources may include without limitation: FDIC recordkeeping systems, such as those identified in the table below; FDIC employees and contractors; FDIC outside counsel; other government agencies; and financial institutions. FDIC also may derive information in LRMMS from interviews, subpoenas, documents, research, public records, and other parties involved in legal matters.

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 LRMMS varies based on the nature of a particular legal matter.

Data Source	Description of Information Provided by Source
Corporate Human Resources Information System (CHRIS) HR	Legal Division employee data related to matters within ALIS
Web Time and Attendance (WebTA)	Time and attendance data related to matters within ALIS
Structure Information Management System (SIMS)	Open financial institution data for matters within ALIS
Communication, Capability, Challenge and Control (4C)	Financial institution subsidiary information for matters within ALIS
New Financial Environment (NFE)/ Interface Operational Data Store (iODS)	Contract invoice, vendor profile, Receivership, and accounting entity for matters within ALIS
Legal Hold System (LHS)	FDIC Oversight Attorneys, delegated authorities, custodians and paralegals who are listed on matters with a Legal Hold

Data Source	Description of Information Provided by Source
Collaboration Portal	Approved e-billing vendors have the ability to submit supporting documentation, such as third-party invoices and travel receipts, as an attachment to their invoice submission and budgets via the Collaboration Portal.
Divisional Oversight of Liability Litigation and Restitution System (DOLLARS)	Professional Liability recoveries received data related to matters in ALIS.
Legal Third Parties and Government Agencies	FDIC may receive data from third parties and government agencies related to FDIC legal matters, such as litigation associated with investigations or litigation related to a bank. FDIC also may derive information in LRMMS from interviews, subpoenas, documents, research, public records, opposing counsel and other parties involved in legal matters. This information may be maintained within LRMMS document management solutions.
Financial Institutions	FDIC may receive data from financial institutions or servicers of a bank in relation to a legal matter. This information may be maintained and accessed by Legal within LRMMS document management solutions.

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

All FDIC information systems must achieve an ATO via the Assessment & Authorization process that aligns with the Risk Management Framework. Information systems that process legal research and matter information have been granted ATO or are in the process to achieve ATO. The ATO for each FDIC system is periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

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

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

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures

notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

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

LRMMS derives or maintains information, including PII, from other FDIC record systems that are covered by Privacy Act Systems of Records Notices (SORNs). Such record systems typically include: FDIC-002, *Financial Institution Investigative and Enforcement Records*;[20] FDIC-012, *Financial Information Management Records*;[21] FDIC-013, *Financial Institution Resolution and Receivership Records*;[22] and FDIC-015, *Personnel Records*.[23] The context of the data being maintained in the respective LRMMS repositories determines the applicable SORN. For example, records in LRMMS relating to labor and employment matters are covered by FDIC-015, *Personnel Records*,[24] whereas records relating to resolution and receivership matters are generally covered by FDIC-013, *Financial Institution Resolution and Receivership Records*.[25] FDIC-041, *Personal Information Allowing Network Operations*,[26] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of LRMMS 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.

No, the system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

---

[20] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[21] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[22] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[23] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[24] *Ibid.*
[25] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[26] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

2.4 If a Privacy Act Statement[27] is required, how is the Privacy Act Statement provided to individuals before collecting their PII? 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 1213.01 "FDIC Forms Management Program."

Since LRMMS maintains information collected from other agency record systems and third-party sources in support of FDIC legal matters, it is not always possible or practical to provide notice to individuals prior to the collection and processing of their information within LRMMS. Nonetheless, the FDIC provides notice to individuals at the original point of collection wherever possible. For example, in cases where LRMMS receives 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 LRMMS.

When LRMMS 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 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

[27] *See* 5 U.S.C. §552a(e)(3). The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

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

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Since LRMMS receives information from other agency recordkeeping systems and third-party sources, rather than directly from individuals, the FDIC does not always have the ability to provide individualized notice prior to the collection and use of PII within LRMMS. Therefore, individuals may not be aware that their data has been provided to FDIC or uploaded to LRMMS.

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 LRMMS.

In instances where LRMMS receives 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*;[28] FDIC-012, *Financial Information Management Records*;[29] FDIC-013, *Financial Institution Resolution and*

[28] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[29] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.

Receivership Records;[30] FDIC-015, *Personnel Records*;[31] and FDIC-041, *Personal Information Allowing Network Operations*.[32] 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 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 LRMMS 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?

For approved e-billing vendors: Within the Collaboration Portal described in Section 1.0, vendors have the ability to login and access a report view of data specific to them with information that they will need to submit an invoice, such as the matter number, the timekeeper ID, and timekeeper rates. They can also track where their invoices are in the invoice payment process. If the vendor notices a discrepancy, they can simply correct the amount and resubmit the corrected budget via the Portal. If the invoice

[30] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[31] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[32] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

was submitted in error, the vendor can contact an FDIC Financial Specialist to reject the invoice so that the vendor can resubmit the correct invoice.

For individuals named in/subjects of matters in LRMMS: Since LRMMS contains records gathered from other agency recordkeeping systems and third-party sources for purposes of litigation and other legal matters, it is not designed and does not have procedures for individual access. However, in cases where LRMMS 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. 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, LRMMS 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 individuals to correct inaccurate or erroneous information?

For approved e-billing vendors: Once an approved e-billing vendor submits an invoice via the Collaboration Portal described in Section 1.0, they no longer have access to that invoice. If the invoice was submitted in error, the vendor can contact an FDIC Financial Specialist to reject the invoice so that the vendor can resubmit the correct invoice. ALIS has some automated validation of FDIC business rules set up upon invoice submission and when it lands in ALIS. Invoices with inaccurate or erroneous information are either rejected during submission or sent to the Error Manager in ALIS to be reviewed and corrected. The same business rules are applied to paper invoices entered by the Financial Specialists.

E-billing vendors may possibly submit an inaccurate or erroneous budget. When the approving FDIC attorneys review the submitted budget, if the budget amount is

incorrect, the attorney may reject the budget and the firm is notified via an email from ALIS. The firm can correct the amount and resubmit the corrected budget via the Collaboration Portal. For paper billing firms, the attorney will contact the firm by phone or email and have the firm resubmit a corrected budget by mail.

For individuals named in cases/subjects of matters within LRMMS: Since LRMMS maintains records gathered from other agency recordkeeping systems and third-party in support of litigation and other legal matters, the system is not designed to allow individuals to correct inaccurate or erroneous information about themselves. However, in cases where LRMMS receives 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*;[33] FDIC-012, *Financial Information Management Records*;[34] FDIC-013, *Financial Institution Resolution and Receivership Records*;[35] FDIC-015, *Personnel Records*;[36] and FDIC-041, *Personal Information Allowing Network Operations*.[37] 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 LRMMS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In cases where LRMMS 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 LRMMS. 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?

---

[33] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[34] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[35] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[36] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[37] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

For approved e-billing vendors: Upon submitting an invoice, if it doesn't meet certain business rules, the invoice is immediately rejected by the Collaboration Portal and the vendor is notified along with an error message as to why the invoice was rejected. The vendor also has access to a report view of data specific to them with information that they will need to submit an invoice such as the matter number, the timekeeper ID, and timekeeper rates. They can also track where their invoices are in the invoice payment process. The same validation process is used for paper invoices that are entered by FDIC Financial Specialists; however, for paper invoices, the Financial Specialists will contact the firm directly.

If an FDIC attorney rejects a budget that was submitted electronically, the firm is notified via an email from ALIS. The firm can simply correct the amount and resubmit the corrected budget via the Portal. For paper billing firms, the attorney will contact the firm by phone or email and have the firm resubmit a corrected budget by mail.

For individuals named in/subjects of matters and cases within LRMMS: Because LRMMS 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*;[38] FDIC-012, *Financial Information Management Records*;[39] FDIC-013, *Financial Institution Resolution and Receivership Records*;[40] FDIC-015, *Personnel Records*;[41] and FDIC-041, *Personal Information Allowing Network Operations*.[42] 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 LRMMS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

In some cases, LRMMS processes data from banks, government agencies or other third-party entities. The system or project does not have procedures for individual

---

[38] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[39] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[40] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[41] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[42] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

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 who are subjects of legal matters are not able to access and amend information about themselves within LRMMS.

Mitigation: Since LRMMS processes records from other agency recordkeeping systems and third-party sources in support of FDIC legal matters, it is not designed to allow individuals to access and amend inaccurate or erroneous information about themselves. However, in cases where LRMMS 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. 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 LRMMS 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 supports the SAOP in the management and execution of the FDIC's Privacy Program.

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

Risk analyses are an integral component of FDIC's Privacy Program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

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

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

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

Contractors may be employed to provide support and maintenance for LRMMS. Due to contractors' access to PII, contractors take mandatory annual information security and privacy training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles,

responsibilities, and access requirements are documented in relevant PIAs.

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

Yes, appropriate Confidentiality Agreements have been completed and signed for contractors who work on LRMMS. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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 litigation and legal matter procedures, resources, and training materials, as applicable. Legal also provides users with system-specific training for certain LRMMS systems and platforms to which they have access. Additionally, annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program as well.

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

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA, and regular reporting to the SAOP, the

CISO, and the Information Technology Risk Advisory Committee.

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

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and 12 C.F.R. § 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 LRMMS.

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 SORN applies. For example, records in LRMMS relating to labor and employment matters are covered by FDIC-015, *Personnel Records*,[43] whereas records relating to resolution and receivership matters are generally covered by FDIC-013, *Financial Institution Resolution and Receivership Records*.[44] FDIC-041, *Personal Information Allowing Network Operations*,[45] covers any logs, audits, or other security data regarding use of FDIC information technology resources, including access to and use of LRMMS resources by authorized individuals.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority for LRMMS.

Mitigation: No mitigation actions are recommended.

---

[43] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[44] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[45] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

Section 6.0: Minimization

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

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

LRMMS only collects information for which the FDIC has the authority to collect and use pursuant to FDIC legal matters. LRMMS 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 LRMMS systems and data contained therein to only those authorized users with a need-to-know. Certain LRMMS systems and platforms also have the capability to generate a robust audit trail of user activity.

Additionally, through the conduct, evaluation, and review of privacy artifacts, [46] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected. Information is not uploaded into LRMMS except as needed to support authorized business purposes.

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 LRMMS 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, the training addresses breach prevention. The LRMMS systems and platforms have built-in user security features to help manage and restrict what information users have access to on a "need-to-know" basis and according to their work responsibilities. These user security permissions are controlled by LRMMS system administrators.

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

Additionally, through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected. Whenever possible, users access information in the originating systems. Information is not uploaded into LRMMS except as needed to support authorized business purposes.

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

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

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

FDIC maintains data in LRMMS for the duration of the legal matter. The law or ruling also establishes the retention guidelines. FDIC also retains the records in LRMMS 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). Specifically, within LRMMS, the master files of matters in ALIS fall under a fifteen (15) year retention period, which requires Legal to purge matters that have been closed with no activity for 15 years. Documents maintained in the Legal Research Bank/Private File are considered non-record materials and are destroyed/deleted when no longer needed for reference, but not longer than the record copy. Documents processed by the Drafting Assistant are also considered non-record materials and are temporarily retained only for long enough for the system to process the information, after which they are automatically deleted. Data maintained in the LRMMS document management repositories has the potential to include a wide variety of data that may be subject to different retention requirements. It is the responsibility of the respective LRMMS users to maintain and dispose of the records they create in accordance with applicable retention schedules for their program area and the source system or data. Records subject to legal hold are retained for the life of the legal hold. Retention periods as set forth, resume upon release of the legal hold.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with National

Archives and Records Administration (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 Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and NARA-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9.

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

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

Privacy Risk Analysis: Related to Minimization

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

Mitigation: FDIC relies on authorized LRMMS users to minimize unnecessary duplication of data. Whenever possible, users access information in the originating systems and only upload information that is necessary to support authorized business purposes. In addition, records in LRMMS are retained in accordance with FDIC policy and a National Archives and Records Administration (NARA)-approved record retention schedule. FDIC's Security and Privacy Control Assessment Team tests applicable controls, including whether systems are adhering to stated retention schedules, as part of continuous monitoring. No additional mitigation actions are recommended.

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

Mitigation: LRMMS only collects and aggregates information as necessary to satisfy litigation requirements or otherwise track and resolve FDIC legal matters. LRMMS only processes information for which FDIC already has the authority to collect and pursuant to litigation and other FDIC legal matters. In cases where LRMMS 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 LRMMS to those who have a need to use them in order to perform authorized business duties. LRMMS platforms also utilize role-based permissions to limit user access to data, including PII, on a need-to-know basis. Further, certain LRMMS platforms have the ability to generate audit trails of user activity, including the viewing of records in the 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, LRMMS does not collect personal information directly from individuals, but instead receives copies of records obtained from other FDIC recordkeeping systems and third-party sources.

Technical controls within certain LRMMS systems, such as ALIS, ensure that required data is collected before a record can be saved. Access is based on a need to know and is controlled by technical controls within the software program. Data modifications are logged to provide usable audit trails.

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

creation.

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

For approved e-billing vendors: The information system collects PII directly from individuals via the Collaboration Portal. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

For individuals named in cases/subjects of matters within LRMMS: Data is not always collected directly from individuals. For example, in some cases, the system receives third-party data from financial institutions. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their financial institution directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the financial institutions.

In other cases, LRMMS derives information about individuals 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*;[47] FDIC-012, *Financial Information Management Records*;[48] FDIC-013, *Financial Institution Resolution and Receivership Records*;[49] FDIC-015, *Personnel Records*;[50] and FDIC-041, *Personal Information Allowing Network Operations*.[51] 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 LRMMS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

---

[47] FDIC SORN-002, *Financial Institution Investigative and Enforcement Records*, 86 Fed. Reg. 19619 (April 14, 2021), https://www.fdic.gov/about/privacy/records.html.
[48] FDIC SORN-012, *Financial Information Management Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[49] FDIC SORN-013, *Financial Institution Resolution and Receivership Records*, 87 Fed. Reg. 66178 (November 2, 2022), https://www.fdic.gov/about/privacy/records.html.
[50] FDIC SORN-015, *Personnel Records*, 84 Fed. Reg. 35184 (July 22, 2019), https://www.fdic.gov/about/privacy/records.html.
[51] FDIC SORN-041, *Personal Information Allowing Network Operations*, 88 Fed. Reg. 27509 (May 2, 2023), https://www.fdic.gov/about/privacy/records.html.

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

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

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

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

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

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

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a potential risk associated with data quality and integrity because information processed by LRMMS could be inaccurate or incomplete.

Mitigation: LRMMS maintains records obtained from other agency recordkeeping systems and third-party sources in support of FDIC legal matters. By design, therefore, LRMMS contains only copies of records from these originating systems and sources and, with the exception of the Collaboration Portal, does not collect information directly from individuals. Uploading information into LRMMS 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.

Section 8.0: Individual Participation

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

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

Since LRMMS maintains information collected from other agency record systems and third-party sources in support of FDIC legal matters, 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 LRMMS. Wherever feasible, FDIC provides notice and relevant consent options to individuals at the original point of collection. For example, in cases where LRMMS receives 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 LRMMS 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 LRMMS.

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, LRMMS maintains information collected from other agency record systems and third-party sources in support of FDIC legal matters. Therefore, opportunities for providing individualized notice and consent options may be limited or non-existent. In cases where LRMMS 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. Refer to Section 8.1 for additional information.

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

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

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

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

notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

When LRMMS 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, http://www.fdic.gov/privacy/, instructs individuals to direct privacy questions to the FDIC Privacy Program through the privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There is risk related to individual participation for LRMMS 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 LRMMS.

Mitigation: This PIA serves as notice to the general public regarding the collection and use of information in LRMMS 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 LRMMS 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.

LRMMS collects, processes and maintains PII as necessary to track, manage, research and resolve a wide-variety of FDIC Corporate and Receivership legal matters, and sustain the FDIC Legal Division's business functions; this includes maintaining records of matters, people, organizations, events, narratives, invoices, and budgets.

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

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

LRMMS includes the Legal Division's principal information system, ALIS, containing all types of information related to the Legal Division's business functions, such as records of matters, people, organizations, events, narratives, invoices, and budgets. It is a highly configurable, externally hosted, web-based application that integrates the Division's matter management, budgeting, and invoice processing into a single application.

Supervisory attorneys in the Legal Division assign attorneys and paralegals to individual cases and matters. The assigned attorneys and paralegals have access to records in LRMMS on a "need to know" basis in order to track, manage, research and/or report on FDIC legal matters. FDIC Legal Information Technology Unit (LITU) personnel may be granted access to certain LRMMS platforms in order to assist with importing and uploading information and to conduct other system administration functions such as adding users to the system, system upgrades, and troubleshooting user reported problems. In addition, a limited number of users in the FDIC Division of Information Technology (DIT) may have access to certain LRMMS systems/platforms for system administration and troubleshooting purposes.

When contractors have access to PII, contractors are required to take mandatory annual Information Security and Privacy Awareness 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 LRMMS 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 LRMMS 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 respective LRMMS systems and platforms. Additionally, all LRMMS System Administrators with access to the system must complete the FDIC's 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.

LRMMS users are granted access to specific roles set within the respective LRMMS systems and platforms. All internal and external users who have access to LRMMS must have the approval of their Manager/Supervisor, as applicable, and the FDIC Program Manager/System Owner for the LRMMS platform to which they require access. Additionally, the functional security of certain LRMMS platforms 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. FDIC follows Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

Additionally, access to ALIS by Outside Counsel firms is managed and monitored by the Service Provider's Collaboration Portal. Outside Counsel firms must have an approved Legal Services Agreement (LSA) with the FDIC. Further, firms that want to e-bill must provide appropriate documentation that requires approval by FDIC. Once FDIC has approved that documentation, FDIC notifies the Service Provider and the Service Provider works with the firm to provide appropriate access via the Collaboration Portal. This access is restricted to invoicing and budgeting information as it relates to a particular case or cases.

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.

- Corporate Human Resources Information System (CHRIS)
  Personnel records

- Web Time and Attendance (WebTA)
  Matter and employee timesheet tracking data

- Virtual Supervisory Information On the Net (ViSION)
  Enforcement data

- Structure Information Management System (SIMS)
  Open financial institution data

- Communication, Capability, Challenge and Control (4C)
  Financial institution subsidiary information

- New Financial Environment (NFE)
  Vendor and closed bank information and payment information

- Legal Hold System (LHS)
  FDIC Oversight Attorney, Delegated Authorities, Paralegals and Custodians (and email addresses) listed on Legal Hold matters

- Divisional Oversight of Liability Litigation and Restitution System (DOLLARS) Professional Liability recoveries received data

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?

LRMMS receives and has the potential to aggregate data from multiple sources in support of investigatory, litigation and other FDIC legal matters. 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 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 LRMMS data with courts, retained counsel, 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.

Approved FDIC vendors who have signed up for the LRMMS e-billing services have access to several view-only reports associated with their firms, such as individuals approved on the firm's Legal Services Agreement (LSA) rate matrix, which includes their name, title, timekeeper ID, approved rates, and whether the firm is a sole proprietor. Outside Counsel firms must have an approved LSA with the FDIC.

Additionally, through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1360.20 "Privacy Program," and FDIC Circular 1360.17 "Information Technology Security Guidance for FDIC Procurements/Third Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

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

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

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a risk that information in LRMMS could be used or disclosed for a purpose not compatible with the original purposes for which the information was collected.

Mitigation: Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information." LRMMS restricts access to data to users with a “need-to-know” who require the information to perform their job responsibilities. Any disclosures outside of LRMMS 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.

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

Mitigation: To help prevent unauthorized access and use of information, LRMMS employs role-based permissions to restrict access to LRMMS and the data contained therein to only authorized FDIC personnel who have a “need-to-know” in order to fulfill their job responsibilities. LRMMS administrators grant access to users, and each individual user must be properly credentialed. In addition, all FDIC 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. Certain LRMMS systems and platforms generate and maintain detailed audit logs that are capable of capturing a user's unauthorized use of information contained within the respective platform.

Section 10.0: Security

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

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

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

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

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

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

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

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

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

Privacy Risk Analysis: Related to Security

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

Mitigation: No mitigation actions are recommended.