FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment
for
Advanced Legal Information System (ALIS)

PIA-FDIC-589

11/25/2019

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

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

SYSTEM OVERVIEW

The 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, 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 Portal's operations group.

All collaborative information between the Collaboration Portal and the core ALIS server database is securely exchanged via HTTPS and other encryption methods.

PRIVACY RISK SUMMARY

In conducting this PIA, we 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
- Individual Participation

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

Mitigation: ALIS does not operate as a Privacy Act system of records. Therefore, notice, in the form of a Privacy Act Statement (PAS) or System of Records Notice (SORN), is not required. In instances where the PII in ALIS is derived from third-party data from banks, the banks are responsible for providing any applicable,

[1] www.fdic.gov/privacy

required notices to the individuals from whom they collected the information. Additionally, this PIA serves as notice of the information collection. No additional mitigation actions are recommended.

Access and Amendment Risk: ALIS does not have procedures for individuals who are subjects of cases/matters to correct inaccurate or erroneous information. In addition, since ALIS processes third-party data from banks, some of which may contain PII, FDIC relies upon these third-party entities that initially collected the PII to ensure that the PII is correct.

Mitigation: ALIS does not operate as a Privacy Act system of records. Therefore, the system is not subject to the Privacy Act redress requirement. In instances where the PII in ALIS was derived from banks, the banks that initially collected the PII are responsible for ensuring that the PII they collected is correct. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks. No additional mitigation actions are recommended.

Individual Participation Risk: There is risk related to individual participation for ALIS 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 ALIS.

Mitigation: ALIS does not operate as a Privacy Act system of records and, therefore, is not subject to the notice requirements of the Privacy of 1974, as amended. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. No additional mitigation actions are recommended.

Section 1.0: Information System

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

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 retrievable by name or Employee Identification Number from WebTA for ALIS reporting.

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 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.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☐	☒
Place of Birth	☐	☒
Social Security Number / Taxpayer Identification Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☒	☐
Criminal Information	☒	☐
Military Status and/or Records	☒	☐
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: Corporate Disciplinary Data, Supporting Documentation such as third-party invoices and travel receipts may be submitted via the Collaboration Portal as an attachment to invoice submissions; user login credentials for approved e-billing vendors are captured and managed via the Portal.)	☒	☐

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

Data Source	Description of Information Provided by Source
Legal employees	Any information related to a legal matter including labor employment matters, attorney/client privilege data, and sensitive data related to a matter
Corporate Human Resources Information System (CHRIS) HR	Legal Division Employee Data
Web Time and Attendance (WebTA)	Time and Attendance Data related to matters within ALIS
Structure Information Management System (SIMS)	Open Financial Institution Data
Communication, Capability, Challenge and Control (4C)	Financial Institution subsidiary information
New Financial Environment (NFE)/ Interface Operational Data Store (iODS)	Contract Invoice, Vendor Profile, Receivership, Accounting entity
Legal Hold System (LHS)	FDIC Oversight Attorneys, Delegated Authorities and Paralegals who are listed on matters with a Legal Hold
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 Portal.

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

The ATO was issued on April 25, 2014 and will be periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

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

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

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

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

The ALIS system does not operate as a Privacy Act system of records, nor does it require an alteration to an existing system of records. The ALIS system processes information imported from other FDIC record systems that is collected and maintained for purposes related to other business processes for which there are currently Privacy Act systems of records in existence. Such record systems include the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015).

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

Not applicable. ALIS is not being modified.

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

Not applicable. ALIS does not operate as a Privacy Act system of records. Therefore, a Privacy Act Statement is not required.

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

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

Privacy Risk Analysis: Related to Transparency

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

Mitigation: ALIS does not operate as a Privacy Act system of records. Therefore, notice, in the form of a Privacy Act Statement (PAS) or System of Records Notice (SORN), is not required. In instances where a matter in ALIS contains bank data with PII, it is incumbent upon the bank to provide any applicable, required notices to the individuals from whom they collected the information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks. Further, this PIA serves as notice of the information collection.

In instances where the ALIS system imports or derives PII from other FDIC Privacy Act systems of records (SORs), the FDIC provides notice to individuals through the respective SORNs and PASs for the source systems. Such record systems include the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015). 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 FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. No additional mitigation actions are recommended.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

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 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 cases or matters in ALIS: The system does not have procedures for individual access. The PII maintained by the system is not contained in a Privacy Act system of records. Therefore, the system is not subject to the Privacy Act individual access requirement.

In addition, in some cases, the system processes third-party data from banks. The system or project does not have procedures for individual access in these cases. Individuals should contact their bank directly for access to their personal information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks.

In cases where ALIS 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 FDIC Circular 1031.1. The FDIC publishes its System of Records Notices (SORNs) on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

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

For approved e-billing vendors: If ALIS end users enter incorrect or erroneous information, they have the ability to edit most fields. ALIS system administrators also have the ability to edit, and they also can delete data in most fields as well.

If an approved e-billing vendor submits an invoice in ALIS, 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 simply 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 ALIS: The system does not have procedures to correct inaccurate or erroneous information. The system does not operate as a Privacy Act system of records. Therefore, the system is not subject to the Privacy Act redress requirement.

In addition, in some cases, the system receives third-party data from banks. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information in these cases. Individuals should contact their bank directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks.

In instances where ALIS processes information about individuals imported from other FDIC Privacy Act systems of records, the FDIC allows these individuals to correct or amend PII maintained by the FDIC in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The procedures for correcting inaccurate data are provided in related SORNS: the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015). 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 ALIS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

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

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 ALIS: In some cases, the system receives third-party data from banks. The system or project does not have procedures for individual access in such cases. Individuals should contact their bank directly for access to their personal information. The PII maintained is not contained in a Privacy Act system of records. Therefore, the system or project are not subject to the Privacy Act individual access requirement. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks.

Because the ALIS system 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 FDIC systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The notification procedures are provided in related SORNS: the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015). 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 ALIS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: The system does not have procedures for individuals who are subjects of cases/matters to correct inaccurate or erroneous information.

Mitigation: ALIS does not operate as a Privacy Act system of records. Therefore, the system is not subject to the Privacy Act redress requirement. In cases where information pertaining to individuals is 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 of records as specified by the Privacy Act and FDIC Circular 1031.1. The notification procedures are provided in related SORNS: the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015). 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 ALIS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office. No additional mitigation actions are recommended.

Privacy Risk: In some cases, the system processes third-party data from banks, some of which may contain PII. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information in these cases.

Mitigation: In instances where the PII in ALIS was derived from banks, the banks that initially collected the PII have a responsibility and vested interest in ensuring that the PII they collected is correct to preclude compliance issues with Federal mandates. Individuals should contact their bank directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks. No additional mitigation actions are recommended.

Section 4.0: Accountability

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

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

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

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy and guidance. This includes the Privacy Act of 1974[2], as amended; Section 208 of the E-Government Act of 2002[3], Section 522 of the 2005 Consolidated Appropriations Act,[4] Federal Information Security Modernization Act of 2014,[5] Office of Management and Budget (OMB) privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

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

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

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

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

Privacy risks posed by ALIS are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/about/privacy/index.html.

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

Contractors are employed by the FDIC Division of Information Technology (DIT) to provide development and maintenance support for ALIS and the Collaboration Portal. Programmers are restricted to the development and quality assurance environment using test data and do not have access to operate in the production environment.

Due to the contractors' access to PII, contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts

[2] The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

[3] Section 208 of the E-Government Act of 2002, Public Law No. 107-347, 44 U.S.C. Ch. 36.

[4] Consolidated Appropriations Act, 2005, Public Law No. 108-447, Division H, Title V, Section 522.

[5] The Federal Information Security Management Act of 2014, Public Law No: 113-283, 44 U.S.C. § 3554.

and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs. Privacy and security requirements for contractors and Outsourced Service Providers are mandated and are documented in relevant contracts.

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?

Contractors are employed by the FDIC Division of Information Technology (DIT) to provide development and maintenance support for ALIS and the Collaboration Portal. Confidentiality Agreements have been completed and signed for contractors who work on the information system. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

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

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

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

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

ALIS has a firewall set up in the user security setting when users are given access to ALIS, which prohibits various business units from accessing matters that belong to a particular firewalled business unit(s). For example, all matters that belong to the Labor Employment and Administration

Section (which contains sensitive data) are firewalled off from the rest of the Legal Division. Once the user security is set up during account creation, the user security is automated throughout the application.

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 records under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using FOIAExpress.

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 FDIC Circular 1031.1.

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 FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Accountability

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

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 personally identifiable information (PII) are legally authorized through the conduct and documentation of Privacy Impact Assessments (PIA) and the development and review of System of Records Notices (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:

- 12 U.SC. 1819: states that FDIC can make examinations of and to require information and reports from depository institutions.
- 12 U.S.C. 1820: discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 12 U.S.C. 1821: deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 U.S.C. 1822: deals with FDIC as a Receiver of failed banks.
- Executive Order 9397: stipulates the requirement for the use of SSNs.

- 12 CFR 330: clarifies the rules and define the terms necessary to afford deposit insurance coverage under the Act and provide rules for the recognition of deposit ownership in various circumstances.
- 12 CFR 366: deals with FDIC contractors.

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Data Minimization

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

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

Depending on the type of matters the end user may be working on, such as labor and employment matters, users may enter data or upload documents that may contain PII necessary for their case. In addition, some vendors may submit supporting documentation for a third-party vendor and travel expense receipts that may also contain PII. The supporting documentation is necessary to approve the payment of vendor expenses.

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 ALIS 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 employees are required to complete the annual FDIC IT Security and Privacy Awareness Certification. This is required for ALIS end users in order to get access to ALIS. The online certification has a section that covers how to determine what constitutes PII and how to handle it. In addition, password usage and exposing information is covered in great detail with different scenarios.

There is built-in user security set up in ALIS to manage which sections can or cannot see matters of firewalled sections. These user security permissions are managed by the ALIS System Administrator when a user account is created or updated. For example, attorneys supporting the Labor and Employment Section may enter data or documents that may contain PII, but there is a built-in firewall in ALIS that only allows members of that section to have access to those matters.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect. Whenever possible, users access information in the originating systems. Information is not uploaded into ALIS except as needed to support authorized business purposes.

6.3 How often does the information system or project evaluate the PII holding contained in the information system or project to ensure that only PII identified in the notice is collected and

retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

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

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

ALIS has a 15-year retention period where matters that have been closed with no activity for 15 years should be purged.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9. Additionally, detailed guidance is provided to users in the Privacy Section-issued guide titled 'Protecting Sensitive Information in Your Work Area.'

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

Use of sensitive data outside the production environment requires the management approval via a waiver. Any production data, including PII, may not be used outside of the production environment unless a waiver has been approved by management, and appropriate controls have been put in place.

Privacy Risk Analysis: Related to Data Minimization

Privacy Risk: There is a potential risk related to data minimization for ALIS 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 ALIS beyond the stated retention periods for those respective source systems.

Mitigation: FDIC relies on authorized ALIS 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 ALIS are retained in accordance with FDIC policy and a National Archives and Records Administration (NARA)-approved record retention schedule. No additional mitigation actions are recommended.

Section 7.0: Data Quality and Integrity

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

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

Technical controls within 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. All data modifications are logged to provide usable audit trails.

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 ALIS: Data is not always collected directly from individuals. For example, in some cases, the system receives third-party data from banks. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their bank directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the banks.

In other cases, ALIS processes information about individuals imported from other FDIC Privacy Act systems of records. The FDIC allows these individuals to correct or amend PII maintained by the FDIC in these respective systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The procedures for correcting inaccurate data are provided in related SORNS: the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015). 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 ALIS PIA is published on FDIC's publicly facing Privacy Program page, which provides contact information for the Privacy Office.

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

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

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

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

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

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer prescribes administrative and technical controls for the system or project based on the FIPS 199 determination. In addition, guidelines on protecting the integrity of PII can be found in the FDIC Circular 1360.9 "Protecting Sensitive Information."

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 and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable risks associated with data quality and integrity for ALIS.

Mitigation: No mitigation actions are recommended.

Section 8.0: Individual Participation

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

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

The system collects information directly from individuals in some instances (e.g., approved e-billing vendors who are sole proprietors), but does not operate as a Privacy Act system of records and, therefore, is not subject to the notice requirements of the Privacy of 1974, as amended. The FDIC Privacy Program ensures that privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from individuals authorizes the collection of the information provided. Additionally, this PIA serves as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

In addition, the system receives third-party data from banks. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII in such cases. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice of the information collection.

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.

The system collects information directly from individuals in some instances (e.g., approved e-billing vendors who are sole proprietors), but does not operate as a Privacy Act system of records and, therefore, is not subject to the notice requirements of the Privacy of 1974, as amended. The FDIC Privacy Program describes in privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

In addition, the system receives third-party data from banks. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII in such cases. 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.

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

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

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

The system collects information directly from individuals (e.g., approved e-billing vendors who are sole proprietors) in some instances, but does not operate as a Privacy Act system of records and,

therefore, is not subject to the notice requirements of the Privacy of 1974, as amended. The FDIC Privacy Program describes in privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

In addition, the system receives third-party data from banks. The FDIC does not have the ability to provide privacy notices prior to the Agency's processing of individuals' PII in such cases. 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.

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

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

Privacy Risk Analysis: Related to Individual Participation

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

Mitigation: The system does not operate as a Privacy Act system of records and, therefore, is not subject to the notice requirements of the Privacy of 1974, as amended. In instances where a matter in ALIS includes PII derived from third-party data from banks, the FDIC does not have the ability to provide privacy notices or obtain explicit consent prior to its processing of these individuals' PII. 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.

In cases where information pertaining to individuals is derived from other FDIC Privacy Act systems of records, the FDIC provides notice to individuals via the respective source systems of records' Privacy Act Statements and other applicable privacy notices, which describe the choices available to the individual, and obtain implicit or explicit consent with respect to the collection, use, and disclosure of PII. Such record systems include the Financial Institution Investigative and Enforcement Records (30-64-0002), Financial Information Management Records (30-64-0012), Insured Financial Institution Liquidation Records (30-64-0013), and Personnel Records (30-64-0015), and are available on the FDIC public-facing website. No additional mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

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

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

Data contained within ALIS is necessary for the purposes of sustaining 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 personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or

project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

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.

The ALIS Data Owner/System Manager serves as the primary source of information for data definition and data protection requirements and is 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 ALIS bear responsibility for assuring proper use of the data and abiding by the FDIC data protection rules. These rules are outlined in ALIS-specific Security Awareness training. Additionally, all ALIS 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.

FDIC employees must have the approval of their respective Supervisors, as well as the Program Manager/System Owner before access is granted to ALIS. Access is recertified by the employee's Supervisor/Manager on an annual basis. In addition, ALIS has defined business roles for each user, which limits the user's access to specific functions and information, on a need to know basis. The majority of FDIC ALIS users have "read" or "read/write" privileges, while a few users have "delete" privileges. Administrator or security privileges are provided to a limited number of ALIS users.

While most information within ALIS is currently available to those FDIC employees who have been set up as ALIS users, some information is restricted to specific individuals or roles, such as information associated with the Labor and Employment group. Only FDIC employees assigned to specific roles have read or write access to the restricted information. Additionally, matters marked "private" by a user will only be accessible to the FDIC employees assigned to that matter.

Access to ALIS requires the user to be an active user of the FDIC network, since the software uses the Windows Active Directory (AD) login credentials. Aside from an AD login, users must be members of a specific network group for ALIS users, hold software licenses and be entered as users in the application database and have assigned roles within FDIC Legal sections (which confer privileges).

The Corporation's Access Request and Certification System (ARCS) is used to facilitate the tracking and management of FDIC employees that are ALIS users. ARCS requests must be submitted by users and approved by managers in order to gain access to ALIS. User access is further controlled and restricted according to the groups specified above.

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. (LSAs have a life of up to 2 years). 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. Access to information within ALIS for Outside Counsel firms is restricted to invoicing, timekeeping, and budgeting information as it relates to a particular case or cases.

In general, access to data in ALIS is managed in accord with current FDIC information security and privacy policies and practices. The following policies are applicable:

- FDIC 1360.1 Automated Information Systems (AIS) Security Program
- FDIC 1360.8 Information Security Categorization
- FDIC 1360.9 Protecting Sensitive Information
- FDIC 1360.12 Reporting Computer Security Incidents
- FDIC 1360.15 Access Control for Information Technology Resources
- OMB Circular A-130 Managing Information as a Strategic Resource

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 and Paralegals listed on Legal Hold matters

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?

The system or information system does not engage in data aggregation or data consolidation activities.

9.6 Does the information system or project share personally identifiable information (PII) externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used. Please explain.

Approved FDIC vendors who have signed up for the e-billing services have access to several view-only reports associated with their firms, such as individuals approved on the firm's 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 Legal Services Agreement (LSA) with the FDIC. LSAs have a life of up to 2 years.

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.

All ALIS users with access to the system must complete (a) the FDIC's annual Information Security and Privacy Awareness Training, or (b) a comparable privacy and security training as detailed in their contractual agreement with the FDIC. This training has specific information regarding the compromise of data and the prevention of misuse of data.

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

FDIC Information Security and Privacy Awareness Training is mandated for all FDIC users of ALIS. In addition, both FDIC and external users are required to take annual security training specific to ALIS that covers the rules of behavior. Super users (those with read and edit roles) are required to take additional training. Users that do not comply are not granted access until the training is completed. Contractors also must complete the Corporate Information Security and Privacy Awareness Training which includes Rules of Behavior.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a limited, potential risk associated with use limitation for ALIS because sensitive information, including PII, stored in ALIS could potentially be used for a purpose not compatible with the original purpose 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." Additionally, only authorized Legal Division employees and FDIC-approved Outside Counsel firms have access to information maintained within ALIS. ALIS has defined business roles for each user, which limits the user's access to specific functions and information, on a need to know basis. Certain information is further restricted to specific individuals or roles, such as information associated with the Labor and Employment group. Only FDIC employees assigned to specific roles have read or write access to this restricted information. In addition, ALIS allows users to mark matters as "private," which makes the matter accessible only to specific FDIC employees assigned to that matter.

FDIC Information Security and Privacy Awareness Training is mandated for all FDIC users of ALIS. In addition, both FDIC and external users are required to take annual security training specific to ALIS that covers the rules of behavior. Super users (those with read and edit roles) are required to take additional, specialized training. Users that do not comply are not granted access until the training is completed. No additional mitigation actions are recommended.

Section 10.0: Security

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

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

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

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

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

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

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

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

Responses to privacy incidents (breaches) are addressed in an organized and effective manner in accord 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 ALIS.

Mitigation: No mitigation actions are recommended.