FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Acquisition Life-Cycle Repository (ALR)

June 21, 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

The FDIC's Division of Administration (DOA) Acquisition Services Branch (ASB) is responsible for awarding and administering contracts and purchase orders to support FDIC's mission, goals and objectives. ASB provides vital procurement and business advisory services to FDIC Divisions and Offices, ensuring that fundamentally sound business practices are integrated within FDIC's acquisition of goods and services. In support of that responsibility, FDIC has implemented the FDIC Acquisition Life-Cycle Repository application (ALR) that will be used by all Divisions and Offices across the Corporation. ALR provides full procurement life-cycle support for the following FDIC procurement phases:

- Contract Pre-Solicitation Phase – In this phase, statements of work (SOW), acquisition plans, and other required documents are developed and refined.
- Solicitation Phase – In this phase detailed solicitation documents are prepared and released to facilitate the submission of responsive proposals from qualified offerors. Proposals subsequently received from offerors are evaluated on the basis of price, past performance, contractor capacity, quality and technical capability, as deemed appropriate for the respective contracts. The successful offeror is determined at the end of this phase.
- Contract Award Phase – In this phase the final award decision document is prepared and provided to the successful offeror, while unsuccessful offeror(s) are notified of the award decision.
- Contract Administration and Document Management Phase - This phase includes various contract administration activities, such as receiving deliverables, making

[1] www.fdic.gov/privacy

contract modifications, appointing/removing oversight managers, and evaluating contractor performance.
- Contract Closeout Phase- This phase includes verifying that all invoiced work was performed during the contract period of performance, verifying that payments made to the contractor are appropriate, and documenting the closed-out status of the contract.

ALR serves as the official contract file for FDIC.

PRIVACY RISK SUMMARY

In conducting this PIA of ALR, 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 and Individual Participation
- Access and Amendment
- Data Minimization
- Data Quality and Integrity
- Purpose and Use Limitation

Transparency and Individual Participation Risk:

Privacy Risk: There is a risk that individuals may not be aware and/or have provided explicit consent for the collection and use of their information within ALR.

Mitigation: ALR 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 ARL is received from vendors, the vendors are responsible for providing any applicable, 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:

Privacy Risk: In some cases, information may be received from vendors that includes PII that is subsequently entered manually to ALR by FDIC ALR users, as described in Section 1.0 of this

PIA. The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: ALR does not operate as a Privacy Act system of records. Therefore, ALR is not subject to the Privacy Act redress requirement. The FDIC relies on the vendors that initially collect and provide information to FDIC to ensure that the information they collect and provide to FDIC is correct. FDIC ALR users, however, may contact the vendors that provided their information to FDIC to facilitate the correction and validation of their information.

Data Minimization Risk:

Privacy Risk: There is a risk that the personally identifiable information maintained by ALR may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FDIC policy regarding the collection, use, and retention of records, as well as FDIC users being appropriately trained. ALR follows an approved record retention schedule for the collection, retention and disposal of records, which may contain PII. ALR users are provided training when they are initially provided access to the application. Additionally, refresher courses are provided on a periodic basis. The training courses include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

Privacy Risk: There is a potential risk that information, including PII, could be used in test or lower environments beyond that which is necessary.

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

Data Quality and Integrity:

Privacy Risk: There is a potential risk associated with data quality and integrity because information may be manually entered into the ALR by FDIC users.

Mitigation: This risk is mitigated by FDIC users being appropriately trained and by FDIC users reviewing PII contained within records prior to the records being uploaded to ALR to ensure that the information is correct and current.

Purpose and Use Limitation Risk:

Privacy Risk: There is a potential risk that PII maintained in the system could be used or accessed inappropriately.

Mitigation: This risk is mitigated by limiting FDIC user access to only that information for which there is a business need, which is facilitated through the use of role-based access. This risk is further mitigated by FDIC policies and procedures regarding the appropriate handling of sensitive information, including PII, procurement and contract information. Additionally, training courses include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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?

PII Element	Yes	No
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 (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐

Phone Number(s)	☒	☐
Email Address	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.) Potentially, in instances where a vendor is a sole proprietor.	☒	☐
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 (Potentially key personnel background investigation information)	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, video)	☐	☒
Other (Specify: ____FDIC Network ID (NTID)____)	☒	☐

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

Data Source	Description of Information Provided by Source
FDIC Users	Application users may receive information from vendors (e.g., US Mail or email) and then upload or transcribe the information to ALR. The PII entered into the application typically includes vendor contact information, such as name, phone number, and email address. Additionally, the name, contact information, and resumes of key personnel may be included with vendor proposals.
FDIC's access control tracking system	FDIC user information (employee/contractor name, NTID, work telephone number, work email address) obtained from FDIC's access control tracking system is used by ALR administrators to manually establish user accounts.

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

All FDIC information systems must achieve an Authority to Operate ATO via FDIC's Assessment & Authorization process that aligns with the Risk Management Framework. The information systems that processes ALR information was granted an ATO on May 3, 2021. 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, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

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

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

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

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

2.4 If a Privacy Act Statement[2] 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 of collection, intended uses of the information and the consequences of not providing the information) Explain.

The information collected, used, maintained, and disseminated by ALR is not subject to the requirements of the Privacy Act of 1974 because the system does not retrieve information by personal identifier. 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 provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that individuals may not be aware and/or have provided explicit consent for the collection and use of their information within ALR.

Mitigation: ALR 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 ALR is received from vendors, the vendors are responsible for providing any applicable, 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.

Section 3.0: Access and Amendment

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

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

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

The system or project does not have procedures for individual access. The PII maintained by ALR is not contained in a Privacy Act System of Record. Therefore, ALR is not subject to the Privacy Act individual access requirement.

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

ALR does not have procedures to correct inaccurate or erroneous information. The PII maintained by ALR is not contained in a Privacy Act System of Records. Therefore, ALR is not subject to the Privacy Act redress requirement. However, FDIC ALR users may contact vendors to facilitate the correction and validation of the information provided by the vendor.

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

ALR does not notify individuals about the procedures for correcting their information. The PII maintained by ALR is not contained in a Privacy Act System of Records. Therefore, the system or project is not subject to the Privacy Act redress requirement.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: In some cases, information may be received from vendors that includes PII that is subsequently entered manually to ALR by FDIC ALR users, as described in Section 1.0 of this PIA. The FDIC has limited ability to implement procedures to correct inaccurate or erroneous information in such cases.

Mitigation: ALR does not operate as a Privacy Act system of records. Therefore, ALR is not subject to the Privacy Act redress requirement. The FDIC relies on the vendors that initially collect and provide information to FDIC to ensure that the information they collect and provide to FDIC is correct. Acquisition decisions are not based on individual PII in ALR therefore errors or inaccurate information in ALR would not have a direct negative impact on an individual whose information may be incorrect. Additionally, FDIC ALR users may contact the vendors that provided their information to FDIC to facilitate the correction and validation of 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[3], as amended; Section 208 of the E-Government Act of 2002[4], Section 522 of the 2005 Consolidated Appropriations Act,[5] Federal Information Security Modernization Act of 2014,[6] 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.

---

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

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

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

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

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 ALR 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 responsible for configuring, operating, troubleshooting, applying corrections, and implementing enhancements for/to ALR based on evolving business requirements and the discovery of security vulnerabilities and system functionality defects.

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

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

Yes, appropriate Confidentiality Agreements have been completed and signed for contractors who work on ALR. 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.

ALR users are provided training when they are initially provided access to ALR. Additionally, refresher courses are provided on a periodic basis. The training includes information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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?

Not applicable. ALR does not operate as a Privacy Act system of records.

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?

Not applicable. ALR does not operate as a Privacy Act system of records.

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

Not applicable. ALR does not operate as a Privacy Act system of records.

Privacy Risk Analysis: Related to Accountability

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

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 USC 1819 states that FDIC can make contracts and that FDIC can make examinations of and require information and reports from depository institutions.
- 12 CFR 366 addresses the minimum standards of integrity and fitness for an FDIC contractor
- 12 USC 1820 discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 12 USC 1821 deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving financial institutions.
- 12 USC 1822 deals with FDIC as a receiver of failed financial institutions.

Privacy Risk Analysis: Related to Authority

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

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

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

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

The PII elements maintained, transmitted, or shared using ALR are restricted to those that are relevant and necessary to support FDIC's procurement and contracting function.

Additionally, through the conduct, evaluation and review of privacy artifacts,[7] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

The PII elements maintained, transmitted, or shared using ALR are restricted to those that are relevant and necessary to support FDIC's procurement and contracting function. The FDIC follows an approved record retention schedule for the collection, retention and disposal of records, which may contain PII. ALR users are provided with training when they are initially provided access to ALR. Additionally, refresher courses are provided on a periodic basis. The training courses include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

Annual Information 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, including minimizing the collection of PII and retention of PII.

Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

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

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

---

[7] Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).

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.

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.

The retention periods and disposition procedures for records in ALR are covered by FDIC Records Retention Schedule EIS1035, Automated Procurement System, and EIS1010, Contract Electronic File, which stipulates the following:

- Contract management/procurement data, including contractor name/type/award number, Minority and Women Owned Business information, expenditures, award value, closeout date, Contracting Officer, and Oversight Manager should be destroyed/deleted 20 years after the award effective date, provided the award has been closed out.

- Contractor Performance Evaluations, solicitations, awards, modification documents, Oversight Manager/Technical Monitor appointment memos, and solicitation milestone schedules should be destroyed/deleted seven years after contract closeout.

- Cancelled solicitations and draft awards should be destroyed/deleted one year after they are cancelled.

- Newsfeeds/Announcements, bulletins that announce system releases, system offline maintenance notifications, Contracting Officers tips/reminders, etc. should be destroyed/deleted when superseded, obsolete, or no longer needed.

- Pre-Award and Pre-solicitation documentation, including Requests for Proposals, Requests for Quotations, Requests for Task Order Proposals, amendments, proposals, evaluation documents, and selection approval documents should be destroyed/deleted seven years after the close of the contract.

- Post Award information, including contracts, modifications, Oversight Manager and Technical Monitor nomination documentation, other contact administration documents, and correspondence should be destroyed/deleted seven years after the close of the contract.

- Oversight Manager file information, including invoice related documents, deliverables, tracking of contractor personnel, tracking of FDIC-furnished property, and performance documentation should be destroyed/deleted seven years after the close of the contract.

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?

PII maintained, transmitted or shared by ALR is not used for testing, training, or research unless appropriately authorized. However, the FDIC has developed an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that the personally identifiable information maintained by ALR may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FDIC policy regarding the collection, use, and retention of records and FDIC users being appropriately trained. FDIC follows an approved record retention schedule for the collection, retention and disposal of records, which may contain

PII. FDIC users are provided training when they are initially provided access to ALR. Refresher courses, provided on a periodic basis, include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function. Additionally, Job Aids are provided to users to follow in determining information to be stored in ALR.

Privacy Risk: There is a potential risk that information, including PII, could be used in test or lower environments beyond that which is necessary.

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

Section 7.0: Data Quality and Integrity

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

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

In instances where vendor information is manually entered into ALR, users review PII contained within the records prior to the records being uploaded to ensure that the information is accurate, relevant, timely, and complete. Additionally, FDIC ALR users may contact vendors that provide information to FDIC to validate the information and to facilitate its correction if necessary.

FDIC users are provided training when they are initially provided access to ALR. Additionally, refresher courses are provided on a periodic basis. The training courses include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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?

ALR does not collect PII directly from individuals. Documentation is received from vendors and manually uploaded into the application by FDIC users.

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

ALR does not collect PII directly from individuals. Documentation is received from vendors and manually uploaded into the application by ALR users. ALR users review PII contained within the vendor records prior to the records being uploaded to ensure that the information is accurate, relevant, timely, and complete.

Further, the FDIC reviews privacy artifacts to ensure adequate controls are in place 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 PII. The Office of the Chief Information Security Officer validates the configuration of administrative and technical controls for the system 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 received from vendors is manually entered into the application by ALR users.

Mitigation: This risk is mitigated by the application users being appropriately trained and by users reviewing PII contained within records prior to the records being uploaded into the application to ensure that the information is correct and current. Acquisition decisions are not based on individual PII in ALR therefore errors or inaccurate information in ALR would not have a direct negative impact on an individual whose information may be incorrect. Additionally, FDIC ALR users may contact the vendors that provided their information to FDIC to facilitate the correction and validation of their information.

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.

ALR does not collect PII directly from individuals. ALR receives data from vendors, which is manually uploaded into the application by ALR users. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant vendor 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.

ALR does not collect PII directly from individuals. ALR receives data from vendors, which is manually uploaded into the application by ALR users. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant vendor 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, 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 this 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.

ALR does not collect PII directly from individuals. ALR receives data from vendors, which is manually uploaded into the application by ALR users. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant vendor 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/policies/privacy/index.html, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There are no identifiable risks related to individual participation.

Mitigation: No mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the

notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

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

Acquisition-related information, including PII, is collected and maintained in ALR and may be used throughout the various phases of the acquisition life cycle, in conjunction with FDIC's insurer, supervision, examination, and resolution responsibilities set forth in 12 U.S.C. 1819, 12 U.S.C. 1820, 12 U.S.C. 1821, and 12 U.S.C. 1822. The information collected, maintained and used by the application is necessary to accurately document, award, manage, and administer procurement actions.

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 purposes 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.

Access to all ALR information is based on a business need to know and the principle of least privilege. Users are responsible for assuring proper use of the data in the application and, if applicable, for determining what data can be shared with other parties.

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.

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

Access to ALR is controlled via FDIC single sign on, which authenticates user account credentials via FDIC's Active Directory. As such, users must be active users on FDIC's network. Information within the application is dependent upon a person's need to know and the principle of least privilege. The Corporation's access control tracking system is used to facilitate the tracking and management of FDIC employees that are users.

Access requests must be submitted by users and approved by managers in order to gain access to the application. User access is further controlled and restricted according to specific user and administrative roles that have been defined and established within the application, and which are based on the functions needed to perform specific jobs. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☒ No
☐ Yes Explain.

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

No, ALR does not aggregate or consolidate data in order to make program-level decisions.

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

No, ALR does not share personally identifiable information (PII) with third parties.

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.

ALR users are provided training when they are initially provided access to the application. Additionally, refresher courses are provided on a periodic basis. The training courses include information that addresses the collection, maintenance and

protection of PII in conjunction with the procurement and contracting function.

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 potential risk that PII maintained in the application could be used or accessed inappropriately.

Mitigation: This risk is mitigated by limiting FDIC user access to only that information for which there is a business need, which is facilitated through the use of role-based access. This risk is further mitigated by FDIC policies and procedures regarding the appropriate handling of sensitive information, including PII, procurement and contract information. Additionally, ALR training courses will include information that addresses the collection, maintenance and protection of PII in conjunction with the procurement and contracting function.

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

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

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

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

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

Privacy Risk Analysis: Related to Security

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

Mitigation: No mitigation actions are recommended.