FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA) for FDIC Correspondence Tracking and Approval Tools

July 11, 2021

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

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

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) operates correspondence tracking tools to assist the Corporation in tracking and responding to inquiries from the public and reviewing official documents from within FDIC, other government agencies, Congress, the public, financial institutions, and the private sector.

FDIC generates and processes a large volume of correspondence ranging from policy, guidance, memoranda, legal materials, testimony, and letters. Due to the high volume of correspondence, some of which are complex, FDIC creates systems and tools to track the documents received from the public, within FDIC, external government agencies, Congress, financial institutions, and the private-sector. These tools efficiently handle the intake of correspondence, which require analysis, storage, categorization, and coordinated responses from FDIC personnel assigned to review the correspondence on behalf of the Corporation.

This FDIC-wide PIA covers information systems and tools used to effectively track, store, manage and respond to correspondence. Employees use these systems and tools to manage and share incoming and outgoing information including:

- Briefing material for senior leaders;
- Clearance and maintenance of official documents (e.g., operational guidance, standard operating procedures, delegations of authority, memoranda, policies, legal positions, and materials);
- Documenting and responding to hard copy mail sent to FDIC;
- Enabling proper handling of Equal Employment Opportunity (EEO) case correspondence;
- Maintaining internal coordination with FDIC; and
- Enabling the appropriate handling, records management, and customer service actions generated by the correspondence.

This PIA will primarily focus on the correspondence tracking process and the privacy protections in place to safeguard these data. Please see the attached appendix to this PIA for a list and description of correspondence tracking and approval tools covered by this PIA.

Correspondence Lifecycle

Receipt & Assignment

The correspondence lifecycle begins when FDIC divisions and offices receive postal mail, email, telephone, or fax from within FDIC, the public, financial institutions, other federal agencies, Congress, financial institutions, or the private sector. Typically, correspondence are received by either FDIC mail centers or by a specific office or division within the FDIC. If sent to FDIC mail centers, FDIC personnel scan the correspondence unless correspondence are determined to be non-business related or the division or office has opted out of the scanning process. Once scanned, FDIC personnel electronically distribute the digital documents as email attachments via the email client. Each division or office has determined whether mail should be sent directly to recipients or to a shared mailbox established by the division or office. After scanning, the mail is returned to its original packaging/envelope and re-sealed and date-stamped. The original mail will be stored securely within

[1] www.fdic.gov/privacy

FDIC mail centers for 60 days from date stamped on the envelope. Employees may contact their mail center to request their original piece of mail within the 60 day timeframe. Otherwise, the mail will be destroyed on day 61.

There are some instances in which an individual or organization may have a direct relationship with a specific FDIC division or office and may send correspondence directly to the office (e.g., Congress may send documents directly to Office of Legislative Affairs, or an attorney may send correspondence directly to the FDIC Legal Division). When a division, office, or individual is tasked to review a correspondence or inquiry, FDIC commonly refers to these as "taskers."

Depending on how the FDIC receives the correspondence, a designated employee is responsible for inputting the correspondence and other relevant information into an FDIC Correspondence Tracking and Approval Tool, and assigning personnel to review and respond to the tasker. Correspondence that originates within FDIC that has recipients outside the FDIC, which requires Corporation clearance before dissemination, will also go through this process.

Review & Analysis

As described above, a tasker may be assigned to the entire Corporation, an FDIC division or office, or certain experts within a division or office. The division(s), office(s), or individual recipient(s) of a tasker is required to review and respond to the tasker within a designated timeframe. Reviews may consist of substantive comments or edits, concurrence or non-concurrence, or an official response to an inquiry received by an entity. These responses are either uploaded directly into the FDIC Correspondence Tracking and Approval Tool by the reviewing entity, or returned to the responder to consolidate all comments, edits, and questions.

Response

After a designated recipient reviews the tasker, he or she is required to upload or log an individual or office's response into the respective FDIC Correspondence Tracking and Approval Tool. The designated individual will compile all responses, if applicable, and send them back to the requestor.

Information Collected

Information collected in FDIC Correspondence Tracking and Approval Tools may include the name, mailing address, email, phone number of the individual sending the correspondence, as well as financial institution correspondence. The information collected may also contain EEO correspondence concerning current and former employees and applicants who file informal and formal complaints of discrimination. This information may include Social Security numbers and other identifying information deemed relevant to the reason for correspondence.

PRIVACY RISK SUMMARY

In conducting this PIA of correspondence tracking and approval tools, 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
- Accountability
- Data Quality and Integrity
- Security

Transparency Risk:

Privacy Risk: A sender may not be aware that someone other than the addressee will open their correspondence.

Mitigation: Correspondence marked personal or confidential is not opened or scanned by FDIC mail center staff. Mail that appears to be personal (non-FDIC business mail) or potentially sensitive but not specifically marked as such will not be scanned and reassembled into the original envelop or package. Many FDIC divisions and offices with sensitive mail have opted out the mail scanning process. Lastly, transparency into FDIC's correspondence procedures is provided through this PIA and associated SORNs.

Access and Amendment Risk

Privacy Risk: Individuals who send EEO correspondence to FDIC may not be able to correct or amend inaccurate information about them.

Mitigation: Some EEO correspondence may be exempt from access under the Privacy Act or FOIA in order to prevent harm to the investigative process. Providing individual access to such records may reveal investigative interest on the part of FDIC. Access to records could also permit the individual who is the subject of a record to impede the investigation or tamper with witnesses or evidence.

Accountability Risk

Privacy Risk: Malicious or inadvertent actions taken on a particular correspondence may not be traceable back to an individual.

Mitigation: FDIC Correspondence Tracking and Approval Tools have auditing controls where by actions taken by a user on a particular correspondence are tracked. This auditing feature maintains accountability of an action taken by an authorized user. Specific audit trails record the actions of all FDIC Correspondence Tracking and Approval Tools users to include specific audit information (user ID, time/date, and action).

Data Quality and Integrity Risk

Privacy Risk: Information may be erroneously transposed, uploaded, or scanned into FDIC Correspondence Tracking and Approval Tools and sent to an incorrect recipient.

Mitigation: In order to identify any incidents where scanned mail is sent to the incorrect recipient, a quality assurance (QA) review is conducted on a daily basis. The purpose of the QA review is to ensure, through daily random sampling, the accuracy of daily mail scanning and mail delivery to prevent the accidental release of PII to the incorrect recipient. Additionally, should FDIC discover erroneous documents in an individual's files, FDIC will manage the incident in accordance with the FDIC Breach Response Plan.

Privacy Risk: FDIC employees may be able to circumvent approvers in their normal clearance chain when routing internal documents in some FDIC Correspondence Tracking and Approval Tools.

Mitigation: FDIC provides role-based user guides and trainings for employees requesting approval of internal documents as well as employees approving documents. The user guides and trainings instruct both the requestor and approver to follow applicable standard operating procedures for routing and approving documents. Lastly, requestors are encouraged to create a standard routing path for documents that regularly go through the clearance process.

Security Risk

Privacy Risk: Hard copy mail may be left open and unattended causing a security risk.

Mitigation: Once hard copy mail has been scanned and reassembled into the original envelop or package, it is bundled together by division or office. The date received and scanned is noted on each of the bundles. All original bundled mail is held securely in the respective mail centers until a division or office's point(s) of contact retrieve their organization's mail. Division or office's point(s) of contact collect mail from the mail centers on a

regular basis (daily, weekly, or bi-monthly) depending on the volume of mail. These individuals securely store their organization's mail until an organization defined hold period is reached and then the mail is shredded. If a division or office does not retrieve its hard copy mail with sixty days, the mail center will shred the hard copy mail.

Section 1.0: Information System

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

The information maintained in FDIC Correspondence Tracking and Approval Tools covered by this PIA varies based on the collection requirements for each FDIC division and office.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☒	☐
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☒	☐
Home Address	☒	☐
Phone Number(s)	☒	☐
Email Address	☒	☐
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: Other sensitive information sent by the requestor)	☒	☐

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

Data Source	Description of Information Provided by Source
Public	Correspondence from individuals seeking information and/or services from FDIC as well as individuals submitting correspondence related to EEO complaints
FDIC Personnel	Individuals who initiate or approve internal or official documents as well as individuals who submit correspondence related to EEO complaints
Financial Institutions	Correspondence from financial institutions
Federal Agencies	Correspondence from federal agencies
State and Local Governments	Correspondence from state and local governments
Foreign Governments	Correspondence from foreign governments

Executive Offices of the President	Correspondence from the Executive Offices of the President
Congress	Correspondence from Congressional offices

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

Yes. FDIC correspondence is maintained in authorized systems.

Section 2.0: Transparency

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

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

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

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

FDIC Correspondence Tracking and Approval Tools operates under the following Privacy Act System of Record Notices[2]:

- FDIC -15 Personnel Records;
- FDIC -18 Grievance Records;
- FDIC -28 Office of the Chairman Correspondence Records;
- FDIC -29 Congressional Correspondence Records;
- FDIC -05 Consumer Complaint and Inquiry Records;
- FDIC -13 Insured Financial Institution Liquidation Records;
- FDIC -24 Unclaimed Deposit Account Records;
  FDIC -12 Financial Information Management Records; and
- EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records.

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

No amendments or revisions to the SORN are required. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

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

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1, "FDIC Forms Management Program." However, since information in the FDIC Correspondence and Inquiries Tracking Tools are unsolicited and generally not provided on a government issued form

[2] https://www.fdic.gov/policies/privacy/sorns.html

containing a Privacy Act statement, notice is limited. The correspondence in FDIC Correspondence and Inquiries Tracking Tools are voluntary submissions by the public to FDIC, therefore, the submissions are inherently consensual.

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, and the Privacy Program. See https://www.fdic.gov/policies/privacy/index.html.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: A sender may not be aware of how FDIC will use and share their correspondence.

Mitigation: Notice is provided through this PIA and associated SORNs. Correspondence is sent to FDIC voluntarily and the submissions are inherently consensual.

Privacy Risk: A sender may not be aware that someone other than the addressee will open their correspondence.

Mitigation: Correspondence marked personal or confidential is not opened or scanned by FDIC mail center staff. Mail that appears to be personal (non-FDIC business mail) or potentially sensitive but not specifically marked as such will not be scanned and reassembled into the original envelop or package. Many FDIC divisions and offices with sensitive mail have opted out the mail scanning process. Lastly, transparency into FDIC's correspondence procedures is provided through this PIA and associated SORNs.

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?

Individuals desiring access to their information should write or call the program or project which initially collected the information. The program or project is in the best position to remove, edit or provide access to the information held by them on individuals. Additionally, individuals should refer to the SORN(s) listed in Question 2.2 of this PIA for access procedures.

Additionally, the FDIC provides individuals the ability to have access to their PII maintained in its systems of records as specified by the Privacy Act of 1974 and FDIC Circular 1031.1. Access procedures for this information system or projected are detailed in the SORN(s) listed in Question 2.2 of this PIA. 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?

The procedures are the same as those outlined in Question 3.1. The program or project that initially collected the information is in the best position to correct any inaccurate information. Any inquiries for correction should be made to the initial collector. Additionally, the FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in the SORN(s) listed in Question 2.2 of this PIA.

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

Individuals are notified of the procedures for correcting their information through the SORNs identified in Question 2.2, this PIA, as well as FDIC FOIA Service Center, available at https://www.fdic.gov/foia/. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: Individuals who send EEO correspondence to FDIC may not be able to correct or amend inaccurate information about them.

Mitigation: Some EEO correspondence may be exempt from access under the Privacy Act or FOIA in order to prevent harm to the investigative process. Providing individual access to such records may reveal investigative interest on the part of FDIC. Access to records could also permit the individual who is the subject of a record to impede the investigation or tamper with witnesses or evidence.

Section 4.0: Accountability

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

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

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

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

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

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

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

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

Privacy risks posed by FDIC Correspondence Tracking and Approval Tools 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/policies/privacy/index.html.

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

Contractor staff perform onsite scanning and processing services in the FDIC mail centers for incoming FDIC business-related mail. Contractors receive, open and sort all incoming mail by division or office under dual control following established site-specific mail center procedures contained in its contract documents with FDIC. Contractor staff review on-line training materials regarding the use of the scanners and scanning software to become familiar with the operation of the scanning equipment and software prior to using the equipment. FDIC mail centers are secured space where access is restricted only to staff approved by FDIC management in order to maintain security of hardcopy mail.

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

Per the contract, each contractor with access to FDIC Correspondence Tracking and Approval Tools data is required to sign the Contractor Confidentiality and Non-Disclosure Agreement. Contractors also must complete the Corporate Information Security and Privacy Awareness Training, which includes Rules of Behavior.

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 Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. 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 Program 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 Program develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; 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 Systems Development Life Cycle (SDLC) for FDIC and contractor-operated systems, 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. In circumstances where the FDIC relies on a contractor-operated system, the contracts include clauses placing requirements on the contractor to ensure the contractor is held to the same standards.

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and 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: Malicious or inadvertent actions taken on a particular correspondence may not be traceable back to an individual.

Mitigation: FDIC Correspondence Tracking and Approval Tools have auditing controls where by actions taken by a user on a particular correspondence are tracked. This auditing feature maintains accountability of an action taken by an authorized user. Specific audit trails record the actions of all FDIC Correspondence Tracking and Approval Tools users to include specific audit information (user ID, time/date, and action).

Privacy Risk: Correspondence practices stated in this PIA may not be followed by FDIC business divisions.

Mitigation: FDIC ensures the practices stated in this PIA are followed by leveraging standard operating procedures (SOPs). FDIC Correspondence Tracking and Approval Tools have SOPs that define scope, assign roles and responsibilities, and provides detailed procedures on how to appropriately operate the tools. The procedures detailed in the SOPs include quality assurance reviews and retention and disposition schedules that prevent harms to the individual.

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 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.S.C. 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.
- 5 U.S. Code § 7201: Deals with antidiscrimination policy; minority recruitment program.

Privacy Risk Analysis: Related to Authority

Privacy Risk: FDIC may act upon correspondence where it has no legal authority to do so.

Mitigation: FDIC staff reviews correspondence to determine if requests are in the scope of the FDIC's legal authority. Should FDIC determine that a request is not in the scope of its authority, FDIC staff will forward the correspondence to the appropriate regulatory authority.

Section 6.0: Minimization

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

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

FDIC employees may enter information into the FDIC Correspondence Tracking and Approval Tools by: (1) scanning original documents into the respective FDIC Correspondence Tracking and Approval Tools; (2) uploading the electronic version of the correspondence into the FDIC Correspondence Tracking and Approval Tools; (3) manually keying the information received into the FDIC Correspondence Tracking and Approval Tools; and (4) copying information received electronically and

pasting it into the appropriate fields in an electronic form. FDIC Correspondence Tracking and Approval Tools maintains only the PII specified in Question 1.2.

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.

6.2 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?

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 it has been legally authorized to collect.

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

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

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

All FDIC Correspondence Tracking and Approval Tools have their own retention schedules. For hard copy mail, divisions and offices securely store their organization's mail until an organization defined hold period is reached and then the mail is shredded. If a division or office does not retrieve its hard copy mail for a mail center within sixty days, the mail center will shred the mail on the 61st day. The retention and disposition of records, including PII, is addressed in Directives 1210.1 and 1360.9.

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

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 Minimization

Privacy Risk: FDIC may collect more information than necessary to process the correspondence.

Mitigation: FDIC only collects the amount of information necessary to act upon the request, correspondence, or other possible action item received by FDIC. Although each correspondence is very likely to only include basic contact information such as the name, address, and phone number, some submitters voluntarily provide PII with elevated sensitivity. Dependent upon the circumstance, this PII may or may not be placed into FDIC Correspondence Tracking and Approval Tools, or the PII will be redacted from a scanned copy of the correspondence. Each FDIC division/office has its own process for handling PII with increased sensitivity.

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.

A quality assurance (QA) review for scanned correspondence is conducted on a daily basis. The purpose of the QA review is to ensure, through daily random sampling, the accuracy of daily mail scanning and delivery to prevent the inadvertent release of PII to the incorrect recipient.

After mail scanning is completed for the day, FDIC mail center staff reviews no less than a 10% sample of all emails sent that day to verify the accuracy of the recipient of the email. The reviews are recorded on a standardized daily log, which includes a worksheet for daily mail scanned along with a worksheet for QA checks. The sample size covers multiple divisions/offices, different scanned batches, and different times of the day if scanning occurs more than once a day. An FDIC mail center Site Supervisor completes the QA log and electronically signs or initials to acknowledge the accuracy of the sample review each day.

The FDIC reviews privacy artifacts for adequate measures 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?

FDIC Correspondence Tracking and Approval Tools collects PII directly from the individual. However, there are cases where the system collects PII from third parties. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

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

FDIC assumes the information received in the original correspondence is true and accurate for the purposes of processing correspondence, unless follow-up documentation or correspondence indicate otherwise. Should an inaccuracy be discovered, FDIC will follow up with the submitter (using the contact information provided) to verify any inaccuracies.

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.

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: Information may be erroneously transposed, uploaded, or scanned into FDIC Correspondence Tracking and Approval Tools and sent to an incorrect recipient.

Mitigation: In order to identify any incidents where scanned mail is sent to the incorrect recipient, a quality assurance (QA) review is conducted on a daily basis. The purpose of the QA review is to ensure, through daily random sampling, the accuracy of daily mail scanning and mail delivery to prevent the accidental release of PII to the incorrect recipient. Additionally, should FDIC discover erroneous documents in an individual's files, FDIC will manage the incident in accordance with the FDIC Breach Response Plan.

Privacy Risk: FDIC employees may be able to circumvent approvers in their normal clearance chain when routing internal documents in some FDIC Correspondence Tracking and Approval Tools.

Mitigation: FDIC provides role-based user guides and trainings for employees requesting approval of internal documents as well as employees approving documents. The user guides and trainings instruct both the requestor and approver to follow applicable standard operating procedures for routing and approving documents. Lastly, requestors are encouraged to create a standard routing path for documents that regularly go through the clearance process.

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 correspondence in FDIC Correspondence Tracking and Approval Tools are voluntary submissions by the public to FDIC, therefore, the submissions are inherently consensual.

Additionally, this PIA and the SORN(s) listed in 2.2 serve 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.

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.

When the FDIC collects information directly from the individual, it describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII. This PIA and the SORN(s) listed in 2.2 serve 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 project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

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 viewers to direct privacy questions to the FDIC Privacy Program through the Privacy@FDIC.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Since information in FDIC Correspondence Tracking and Approval Tools is generally not provided on a government issued form containing a Privacy Act statement, there is limited opportunity for individual participation.

Mitigation: FDIC Correspondence Tracking and Approval Tools do not generally collect PII directly from individuals. Rather, correspondence is generally collected via postal mail. The FDIC does not have the ability to provide privacy notices prior to the Corporation's collection of individuals' PII found in correspondence. Individuals actively choose to submit correspondence and can limit how much of their personal information to provide when doing so. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

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.

FDIC uses the information to facilitate efficient, accurate, and timely handling of incoming correspondence from other government agencies, financial institutions, Congress, the public, the private sector, and current and former employees and contractors. FDIC uses correspondence tracking and approval tools to maintain a record of the contacts, enable follow-up correspondence from the Corporation, or to forward the correspondence to the appropriate division or office for action. FDIC Correspondence Tracking and Approval Tools use PII to track incoming correspondence, assist FDIC in analyzing requests, storing the large volume of correspondence, and categorizing and responding to individuals and entities. The collection of PII also facilitates FDIC's ability to forward correspondence, by uniquely identifying the record.

The information in the FDIC Correspondence Tracking and Approval Tools also enable clearance and maintenance of official documents (e.g., operational guidance, standard operating procedures, memoranda, delegations of authority, policies, legal positions, and materials).

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.

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" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

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 business divisions are responsible for establishing and promulgating the procedures for controlling access to the data contained in correspondence tracking and approval tools. Correspondence tracking and approval tools have auditing controls. Access to the data is restricted on a "need to know" basis, in conjunction with Active Directory group membership. The user profiles associated with correspondence tracking and approval tools are based on the user's job requirements, managerial decisions, and dependent on the purpose for which access to the data is needed. Access requires management approval, and is facilitated using the FDIC's Access Request and Certification System (ARCS), which is used to grant, manage and monitor access by users to correspondence tracking and approval tools.

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, FDIC does not aggregate data to make programmatic level decisions.

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

FDIC does not grant external organizations access to the FDIC Correspondence Tracking and Tools. However, FDIC may share documents maintained in the tools to respond to an external organization's request for information. If FDIC shares information with an outside entity, such as Congress or another federal agency, it is done by email, fax, or hand-delivery, and not done using the correspondence tracking and approval tool. When shared externally, only the minimum amount of PII is provided. If FDIC receives an inquiry from a member of Congress, the reply may include PII depending upon the topic of the correspondence and whether the underlying individual has provided consent for release of his/her information.

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

Annual Information Security and Privacy Awareness Training is mandatory for all staff 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: Users of FDIC Correspondence Tracking and Approval Tools may engage in unauthorized browsing for information on specific or groups of information for non-official purposes. This is possible since some FDIC Correspondence and Tracking Tools allows users to search every case file and folder stored within the tool.

Mitigation: FDIC employs role-based access controls and limits access to selected groups for prescribed functions. FDIC also provides initial and follow-on privacy and security awareness education for all of its employees.

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).

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.

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 accordance with the FDIC's Breach Response Plan**.**

Privacy Risk Analysis: Related to Security

Privacy Risk: Hard copy mail may be left open and unattended causing a security risk.

Mitigation: Once hard copy mail has been scanned and reassembled into the original envelop or package, it is bundled together by division or office. The date received and scanned is noted on each of the bundles. All original bundled mail is held securely in the respective mail centers until a division or office's point(s) of contact

retrieve their organization's mail. Division or office's point(s) of contact collect mail from the mail centers on a regular basis (daily, weekly, or bi-monthly) depending on the volume of mail. These individuals securely store their organization's mail until an organization defined hold period is reached and then the mail is shredded. If a division or office does not retrieve its hard copy mail with sixty days, the mail center will shred the hard copy mail.

Appendix
Qualifying Systems or Projects (Ordered by Alphabet)

Chairman's Correspondence System

The Federal Deposit Insurance Corporation (FDIC) Office of Legislative Affairs (OLA) serves as the agency's congressional liaison and responds to legislation important to the FDIC. OLA is responsible for the Chairman Correspondence System. The Chairman's Correspondence System is designed to support the FDIC Chairman's Office in its processing and tracking of letters received from all members of the public asking for information or assistance. Incoming correspondence arrives on a variety of topics, such as, comments on proposed rulemakings, questions about the banking industry or the economy and requests for testimony, speeches and briefings on banking topics. The Chairman's Correspondence System is an electronic tool for handling correspondence that would be handled manually in the absence of the application.

Congressional Correspondence System (CCS)

The Corporation places a very high priority on timely and complete responses to Congressional inquiries. All Congressional correspondence addressed to the FDIC is delivered to the FDIC Office of Legislative Affairs (OLA) upon receipt. In order to assure the consistency of the FDIC's contacts with Members of Congress and their staff, the Congressional Correspondence System (CCS) was implemented. OLA assigns Congressional inquiries to the appropriate FDIC Division/Office through CCS. Material in the CCS application consists of incoming correspondence sent to the FDIC, documents assigning preparation of a draft response to the incoming correspondence (where appropriate), and the final response sent to the correspondent. While this application does not solicit information from the public, unsolicited information may arrive as part of the incoming documents. Letters are filed in CCS by the date that they were received and can be retrieved in the system by the date of receipt or by the assigned due date. They can also be retrieved by using the name of the correspondent and/or by an FDIC-assigned classification.

Congressional Analyses and Unified Correspondence Utility System (CAUCUS)

Congressional Analyses and Unified Correspondence Utility System (CAUCUS) is a custom Salesforce application used to track and monitor the progression of bills of interest to the FDIC, analyze those specific bills, track Congressional and Chairman's correspondence, and record testimonies provided by the FDIC to Congress. It includes personally identifiable information from Congressional members and their staff, and members of the public who engage with the FDIC. Access to the records and documents is restricted to authorized users and controlled via roles and profiles.

Digitize Mail Project

FDIC mail centers have the capability to perform high speed scanning of paper mail to convert it to a digitized format and disseminate it electronically to the intended FDIC addressees (FDIC employees/contractors). The scans will be stored, processed, and transported through a workstation connected directly to the scanner. The scanners and dedicated workstations are maintained in locked rooms with controlled access within each of FDIC's existing mail centers. Personal (non-FDIC business) mail, mail labeled as "personal" or "confidential" or mail addressed to divisions or offices that opted out of mail digitization will not be scanned. Otherwise, mail will be opened by an FDIC employee or contractor. The mail is scanned using the scanner attached to the workstation by mail clerks in a two-step process to ensure quality and accuracy. There is also an end of day quality assurance review.

Equal Employment Opportunity Application (EEO)

Pursuant to the regulations of the Equal Employment Opportunity Commission (EEOC), 29 CFR Part 1614, FDIC operates an EEO program. The FDIC Office of Minority and Women Inclusion (OMWI) directs the FDIC's EEO program, including the development and implementation of FDIC EEO policy. Aggrieved persons who believe they have been discriminated against must file complaints with OMWI within 45 days of the matter alleged to

be discriminatory. The EEO application is utilized to track both incoming and outgoing correspondence to individuals who have submitted a complaint against the FDIC. The application will also track the complainant progress through the informal compliant process and through the formal complaint process where a decision is made. The information contained in the EEO concerns current and former employees and applicants who file informal and formal complaints of discrimination. PII of complainants/representatives, witnesses, and FDIC personnel involved in the investigation is captured within the records stored in EEO. Information collected in this system includes the following: full name; Social Security Number (SSN) (to verify the same person); work address; work phone number; email address; home address; home phone number; and other identifying information, as relevant to the investigation.

FDIC Automated Correspondence Tracking Application (ACT)

ACT is a corporate solution to streamline the tracking, routing, review/approval and reporting on document correspondence including documents that have traditionally been routed using "blue folders". ACT is a cloud-based application used to track and route inquiries/requests/approvals with related attached documentation for FDIC information and services, business recommendations, and correspondence and internal memoranda that require follow-up action and/or management approval. The inquiries and requests processed by ACT are received from a variety of internal parties and relate to corporate activities. All FDIC divisions who have a need to route documents for executive review and approval may use ACT. ACT facilitates the routing process and allows for electronic signature.

Regional Document Distribution and Imaging System (RADD)

RADD is the correspondence repository for the Division of Risk Management and Supervision (RMS) as well as the Division of Depositor and Consumer Protection (DCP). Correspondence is stored in RADD in PDF format with hard copy documents stored temporarily in the FDIC Regional Offices. Long-term storage of hard copy documents (correspondence only) is offsite at Iron Mountain. RADD also supports the FDIC's examination and supervision mission by providing an electronic document imaging, distribution, and storage system for financial institution correspondence and final examination work paper documents.

Track and Route Authorization Cases (TRAC)

TRAC is an FDIC developed web-based tracking tool used to manage and approve cases under Delegation of Authority. FDIC's Division of Resolutions and Receiverships (DRR) and Legal Division use the system to log and route business items that require follow-up action and/or management approval related to Corporate and Receivership activities. TRAC also stores business records from the FACTS-DRR system that have not reached the expiration of their retention schedules related to lien releases, records research, depositor claims, Congressional inquiries, Freedom of Information Act (FOIA) requests, and Temporary Liquidity Guarantee Program (TLGP) claims.