PRIVACY IMPACT ASSESSMENT (PIA) FOR FDIC CONTACT AND DEMOGRAPHIC INFORMATION

October 2025

FEDERAL DEPOSIT INSURANCE CORPORATION

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 the system or project 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 FDIC's mission encompasses a wide variety of activities, including: insuring deposits, examining and supervising financial institutions for safety and soundness, making large and complex financial institutions resolvable, managing receiverships, and protecting consumers. In order to facilitate the accomplishment of these activities, the FDIC is in contact with the public, financial institutions, service providers, legal representatives, as well as partners in federal, state, local, and international governmental organizations (hereinafter referred to as "partners"). Part of the FDIC's interaction with its partners involves the maintenance of contact and demographic information. This FDIC-wide PIA covers contact and demographic information stored in IT systems, web-based applications, web-portals, and collaboration tools. Additionally, this PIA discusses the privacy risks of collecting the contact and demographic information of (1) members of the public who visit FDIC facilities, submit requests or comments to FDIC, or otherwise seek information and/or services from FDIC and (2) individuals who are designated as points of contact and emergency contacts.

Coverage Requirements

The authority to collect the information lies within each program or project's legal authorities.

All programs or projects covered under this FDIC-wide PIA satisfy the following requirements:

1. The contact information is limited to PII such as name, address, telephone, and email address.
2. The collection of demographic information must be optional and customer survey participants may choose to opt out at any time.
3. FDIC projects and programs must work with the Privacy Program to ensure that the program or project meets all privacy requirements.
4. FDIC projects and programs must minimize sharing of PII.
5. FDIC projects and programs must be appropriately authorized.

[1] www.fdic.gov/privacy

6. The contact and demographic information must only be used for the purpose for which it originally was collected, i.e., to contact individuals or to conduct trend analyses. Any collection, sharing, or use exceeding this PIA will require a separate PIA.

This PIA does not cover the use of contact and demographic information maintained on social media platforms. Those uses are covered by the Privacy Impact Assessment for Social Media.

The Contact and Demographic PIA does provide coverage for a wide variety of data collections and information requests. Some broad examples that will be discussed in greater detail within the appendix are included below:

Contact and Request Information

General Contact and Request Information

FDIC maintains limited contact information in order to facilitate its operations and services to its partners. FDIC collects contact information at the time of a request. For example, a member of the public may request mail or email updates or submit a public comment regarding proposed banking regulations, or partners working on cross-agency projects may need to be able to contact their peers. In those cases, FDIC may collect general contact information, such as name, email address, and mailing address, along with details about the individual's request or public comment. Many times, names and phone numbers are not required for mass distribution lists. Other times, name and business affiliation, in addition to general contact information, will be collected in order to facilitate a working relationship between current partners or to allow an individual to visit an FDIC facility, such as for a meeting event or conference.

General information intake involves the following:

FDIC requests or receives information directly from the individual via postal mail, email, FDIC's systems, or public-facing website (www.fdic.gov). Information is limited to the minimum required to establish contact and address or respond to the individual's request or public comment. By providing the information, individuals do so voluntarily with the understanding that the PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected. For example, individuals register to provide information and conduct business with the FDIC, or individuals voluntarily submit public comments to FDIC in response to proposed FDIC rulemakings, as detailed below. FDIC requests information on individuals to be identified by FDIC partners as points of contact. In certain circumstances, some FDIC partners may have a regulatory obligation to share the general contact information of their key personnel to FDIC. FDIC partners supply this information to the FDIC and FDIC maintains the information in a spreadsheet, database, or other type of information management tool. The FDIC then accesses the information from its storage site and uses it to distribute information or contact individuals.

FDIC receives information from individuals who visit FDIC facilities to attend a meeting, event or conference. FDIC sponsors are responsible for pre-registering their visitors by providing

guest/visitor information (such as name, company, meeting purpose) to FDIC's Physical Security & Intelligence Unit in advance of the visit. FDIC maintains this limited visitor information in its visitor management system, which helps expedite the processing of visitors for meetings, events, and conferences with a personalized badge. When visitors arrive at FDIC facilities, FDIC security guards validate their proof of identity (with a driver's license or other acceptable form of identification) and confirm their arrival with their FDIC sponsor. After checking in, visitors are issued a visitor badge that must be displayed at all times.

FDIC receives information from individuals who submit public comments in response to proposed FDIC rulemakings, notices and other FDIC regulatory actions. FDIC and other government agencies must, with some exceptions, follow an open public comment process when they issue regulations.

Emergency Contact Information

In working to achieve its mission, FDIC may also collect information about emergency contacts. This information may include the following: name, work contact information, personal contact information, and relationship to FDIC personnel.

General information intake involves the following:

FDIC requests information on individuals identified by current or former FDIC personnel as emergency points of contact, including family members. Individuals supply this information to the FDIC and FDIC maintains the information in a spreadsheet, database, or other type of information management tool. The FDIC then accesses the information from its storage site and uses it to distribute information or contact those individuals in the event of an emergency.

Demographic Information

The FDIC periodically solicits voluntary feedback from its employees, contractors, external stakeholders, and the general public through the use of surveys, interviews, focus groups, and other information collection methods (hereinafter referred to as customer surveys) to improve FDIC services and operations.

Although the customer surveys assessed in this PIA are generally anonymous, FDIC sometimes collects a limited amount of contact information in order to solicit participation in the research or facilitate future communications with participants. Demographic information (e.g., age, race, income level, or type of depositary accounts) may be collected and aggregated to perform trend analyses. Trend analyses measure changes in data over time in an attempt to predict future outcomes or needs. These trend analyses are used to identify areas for improvement in FDIC processes and operations.

All systems or projects covered under this PIA will be added to the Appendix of this document. If there is an additional collection of information beyond the scope of this PIA, the FDIC Privacy Program will make a determination about additional PIA coverage.

PRIVACY RISK SUMMARY

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

- Transparency;
- Access and Amendment;
- Accountability; and
- Minimization.

Transparency Risk:

Privacy Risk: The subjects of the contact information may not know that their information has been submitted to FDIC.

Mitigation: This risk cannot be fully mitigated. Although this PIA and the SORNs listed in Question 2.2 provide some notice regarding the collection of contact information by the FDIC, no direct notice is given to the personnel of financial institutions, emergency contacts, or FDIC partners. It is incumbent upon individuals and organizations, who submit the contact information of others to FDIC, to inform those individuals that their PII was given to the FDIC. Additionally, FDIC does not use this PII to make decisions about individuals.

Privacy Risk: The subjects of the demographic information may not realize that the information they initially provide to FDIC (e.g., to seek depository insurance guidance) may later be used to contact individuals to engage in future customer surveys.

Mitigation: This risk is partially mitigated by publishing this PIA and the SORNs listed in Question 2.2. FDIC also gives all potential participants the opportunity to decline or to discontinue participation at any point, minimizing any potential harm resulting from an individual's lack of notice.

Access and Amendment Risk:

Privacy Risk: The subjects of general and emergency contact information may be unaware of the redress process.

Mitigation: The subjects of general and emergency contact information seeking access to records about himself or herself should refer to the access and redress procedures listed in the SORNs in Question 2.2. The individual's request must conform to the Privacy Act regulations set forth in 6 CFR 5. Additionally, the risk of harm to the individual is further mitigated because FDIC does not make decisions regarding these individuals based on their PII.

Privacy Risk: The subjects of the demographic information may not be able to correct any incorrect information that FDIC collected during customer surveys.

Mitigation: The risk is partially mitigated. FDIC refrains from collecting PII from individuals whenever possible and immediately aggregates any demographic information collected during customer surveys. Information given during customer surveys, therefore, will be difficult to access or amend. As discussed, PII and participant responses are provided directly from the individual, and then the PII is separated from a participant's responses. Therefore, any potential privacy harm to an individual would be minimized. FDIC ensures that all information, incorrect or not, is not associated with a single participant. FDIC collects a sufficient amount of responses during customer surveys to ensure that one participant's erroneous information will not adversely affect the statistics and analysis generated from its analysis, or have any adverse impacts on the participant.

Accountability

Privacy Risk: Systems and projects covered under this PIA may not receive the appropriate level of privacy analysis.

Mitigation: This risk is mitigated. Every system and project goes through the Privacy Threshold Analysis (PTA) process. The PTA process is where privacy requirements are identified. All privacy requirements must be met before a system or project is authorized. Additionally, this PIA covers systems and projects with similar privacy risks. Conducting multiple PIAs for systems and projects with like privacy risks diverts resources away from systems and projects that have unique privacy risks.

Minimization Risk:

Privacy Risk: FDIC may collect more personal and demographic information than necessary for the purposes of process and operations improvement, as well as during the rulemaking process.

Mitigation: The risk is partially mitigated. The purpose of FDIC customer surveys is the collection of opinions and experiences of individuals, not to collect PII. Likewise, the primary objective of collecting public comments on proposed FDIC rulemakings is to help shape and improve FDIC rules, not to collect information about individuals. Although personal contact and demographic information is sometimes collected from individuals, when collected in the context of customer surveys, is typically aggregated and does not identify individuals. FDIC may also give individuals the option to voluntarily provide limited contact information to facilitate future correspondence (e.g., informational pamphlets, email notifications), but individuals are informed that they are not required to provide this information and their PII is not linked to the answers they provided during the customer surveys.

In terms of information collected during the rulemaking process, FDIC provides notice instructing those submitting public comments to limit information to only that which they

wish to make available publicly. The notice also informs public commenters that FDIC may review, redact or refrain from posting all or any portion of a comment that it deems to be inappropriate for publication, such as irrelevant or obscene material.

Privacy Risk: Collecting demographic information may allow for re-identification of an individual if the sample size is small and a specific individual's response is unique.

Mitigation: FDIC has instituted procedural safeguards to ensure the confidentiality of individuals is protected. Through the PTA process, questions that are deemed unnecessary or too specific to an individual during customer surveys are considered to be "over-collections" of information and are dropped from the questionnaire prior to distribution of the customer surveys or additional steps must be taken to remove the identifying information. Additionally, programs must work with the Privacy Section to determine appropriate thresholds to ensure that individuals cannot be re-identified.

Privacy Risk: Since FDIC programs or projects may have the ability to post information, there is a risk that such postings could contain PII that is not about members or potential members of the program or project. Additionally, there is the risk that postings of public comments submitted in response to proposed FDIC rulemakings may contain unnecessary or superfluous PII.

Mitigation: Users are provided notice, at the time of registration or information collection and prior to posting any information, that specifically instructs them to ensure that their comments and documents do not contain PII outside the scope of contact information about members or potential members of the program or project. Program or project managers periodically review shared spaces to ensure that PII is not posted and have the ability to remove inappropriate member postings.

Similarly, FDIC provides notice to individuals who submit public comments in response to proposed FDIC rulemakings, notices and other FDIC regulatory actions. This notice, provided at the time of submission and prior to posting any information, instructs individuals to submit only information that the commenter wishes to make available publicly. The notice also informs commenters that FDIC may review, redact or refrain from posting all or any portion of a comment that it deems to be inappropriate for publication, such as irrelevant or obscene material.

Privacy Risk: FDIC may not be able to control third parties' retention of contact information and customer surveys responses.

Mitigation: This risk is partially mitigated. If FDIC contracts a third-party vendor to assist in customer surveys that involve the collection of PII, then the FDIC ensures that it is the owner of all data collected. The vendor is required contractually to destroy all information associated with the information collection at the end of the contract. FDIC also contracts for the right to investigate and audit a vendor's systems to ensure they are complying with FDIC policies, procedures, and retention schedules.

Section 1.0: Information System

1.1 What information about individuals, including 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?

Contact and request information generally includes name, business affiliation, mailing address, phone number, email address, and details of the request or public comment submitted by the individual to FDIC. Personally identifiable information such as a Social Security numbers or dates of birth are not covered under this PIA. Such collections require separate PIAs analyzing the risks associated with such collections.

Additionally, FDIC may also ask FDIC customers, employees, and other stakeholders to provide optional demographic information such as age, race, country of origin, or personal occupation to gather experiences and opinions about a particular FDIC program or service.

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

PII Element	Yes
User Information (e.g., User ID, password)	☐
Specify other: User credentials, and demographic information, and request or public comment details	☒

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

Data Source	Description of Information Provided by Source
Individuals	Contact and demographic information from individuals submitting requests or public comments to FDIC or otherwise seeking information and/or services from the FDIC.
Partners	Contact and demographic information of federal, state, local, and international government personnel or legal representatives who are working collaboratively with the FDIC on various projects.
Financial Institutions	Contact and demographic information of financial institution personnel who have been identified as points of contact.
FDIC Personnel	Contact information of emergency contacts identified by current or former FDIC personnel and includes family members.
Service Providers	Contact information identified by service providers who have been identified as points of contact for FDIC business activities.

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

Contact and demographic information is maintained on authorized systems. Systems with issued ATOs that are covered by this PIA will be periodically reviewed as part of the FDIC Ongoing Authorization process.

Section 2.0: Transparency

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

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

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

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

The following SORNs apply to FDIC Contact and Demographic Information PIA:

- FDIC-002, Financial Institutions Investigative and Enforcement Records, which covers contact and demographic information from financial institutions and FDIC partners;
- FDIC-005, Consumer Complaint and Inquiry Records, which covers contact and demographic information from members of the public;
- FDIC-013, Financial Institution Resolution and Receivership Records, which covers contact and demographic information from financial institutions and FDIC partners;
- FDIC-015, Personnel Records, which covers contact information from emergency contacts; and
- FDIC-019, Potential Bidders List, which covers contact and demographic information from individuals who have purchased or submitted written notice of an interest in purchasing loans, owned real estate, securities, or other assets from the FDIC.
- FDIC-039, E-Rulemaking, which covers contact and comment information submitted to FDIC in response to proposed FDIC rulemakings, notices and other FDIC regulatory actions.
- FDIC-040, Mailing, Event, and Other Contact Lists, which covers individuals who request to receive information; subscribe to newsletters; seek materials from FDIC; register or participate in FDIC-sponsored or FDIC-funded events or contests; respond to surveys or feedback forms from FDIC or a third party contracted by FDIC; have business with the FDIC and provide their contact information; or otherwise provide contact information to facilitate future communication or collaboration with FDIC.
- FDIC-041, Personal Information Allowing Network Operations, which covers (among other things) contact information from individuals who interact with FDIC information technology resources, which includes FDIC employees, FDIC contractors, FDIC volunteers, FDIC interns, Federal and State financial regulator employees, financial institution employees, and other members of the public.

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

No, the SORNs listed in Question 2.2 do not require amendment or revision. Generally, the FDIC conducts a review of its SORNs every five 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? Explain.

When contact and demographic information is collected directly from the individual, FDIC provides the individual with a Privacy Act Statement prior to the collection of his or her contact information.

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 Directive 1213.01 FDIC Forms Management Program.

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 the FDIC Privacy website[2].

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Some subjects of contact information may not be aware of the purpose for which the information he or she submits may be used.

Mitigation: This risk is primarily mitigated by limiting the use of contact information to what is necessary for the purposes of contacting the person according to his or her voluntary subscription or request. Additionally, this PIA and the SORNs listed in Question 2.2 provide notice of the purpose of the collection, redress procedures and the routine uses associated with the collection of contact information. Notice is always provided prior to the collection of information, and consent is obtained by the individual prior to his providing information.

Privacy Risk: The subjects of the contact information may not know that their information has been submitted to FDIC.

Mitigation: This risk cannot be fully mitigated. Although this PIA and the SORNs listed in Question 2.2 provide some notice regarding the collection of contact information by the FDIC, no direct notice is given to the personnel of financial institutions, emergency contacts, or FDIC partners. It is incumbent upon individuals and organizations, who submit the contact information of others to FDIC, to inform those individuals that their PII was given to the FDIC. Additionally, FDIC does not use this PII to make decisions about individuals.

Privacy Risk: The subjects of the demographic information may not realize that the information they initially provide to FDIC (e.g., to seek depository insurance guidance) may later be used to contact individuals to engage in future customer surveys.

[2] www.fdic.gov/privacy

Mitigation: This risk is partially mitigated by publishing this PIA and the SORNs listed in Question 2.2. FDIC also gives all potential participants the opportunity to decline or to discontinue participation at any point, minimizing any potential harm resulting from an individual's lack of notice.

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 and/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 projectare detailed in the SORN(s) listed in Question 2.2 of this PIA. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public-facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

3.2 What procedures are in place to allow the individuals 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 Reading Room,

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: The subjects of general and emergency contact information may be unaware of the redress process.

Mitigation: The subjects of general and emergency contact information seeking access to records about themselves should refer to the access and redress procedures listed in the SORNs in Question 2.2. The individual's request must conform to the Privacy Act regulations set forth in 6 CFR 5. Additionally, the risk of harm to the individual is further mitigated because FDIC does not make decisions regarding these individuals based on their PII.

Privacy Risk: The subjects of the demographic information may not be able to correct any incorrect information that FDIC collected during customer surveys.

Mitigation: The risk is partially mitigated. FDIC refrains from collecting PII from individuals whenever possible and immediately aggregates any demographic information collected during customer surveys. Information given during customer surveys, therefore, will be difficult to access or amend. As discussed, PII and participant responses are provided directly from the individual, and then the PII is separated from a participant's responses. Therefore, any potential privacy harm to an individual would be minimized. FDIC ensures that all information, incorrect or not, is not associated with a single participant. FDIC collects sufficient number of responses during customer surveys to ensure that one participant's erroneous information will not adversely affect the statistics and analysis generated from its research, or have any adverse impacts on the participant.

Section 4.0: Accountability

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

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

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

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

The FDIC's Privacy Program supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program is 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 Privacy Impact Assessments (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 personally identifiable information (PII); (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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

Privacy risks posed by the information system or project are captured in PIAs, when conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website[3].

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

[3] www.fdic.gov/privacy

Contractors may assist in the maintenance of FDIC contact and demographic information. Additionally, FDIC may use contractors and vendors to facilitate data exchange and customer surveys.

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

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

Confidentiality agreements are required to be completed for contractors who work on systems or projects that process contact and/or demographic information. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

All FDIC employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of PII.

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. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program staff as well.

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

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

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

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

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

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using the FDIC's FOIA solution.

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

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and 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: Systems and projects covered under this PIA may not receive the appropriate level of privacy analysis.

Mitigation: This risk is mitigated. Every system and project goes through the PTA process. The PTA process is where privacy requirements are identified. All privacy requirements must

be met before a system or project is authorized. Additionally, this PIA covers systems and projects with like privacy risks. Conducting multiple PIAs for systems and projects with like privacy risks diverts time away from systems and projects that have unique privacy risks.

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 PIA and the development and review of System of Records SORNs. FDIC Directive 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:

- Federal Deposit Insurance Act (e.g., 12 U.S.C 1811, 12 U.S.C. 1819) and the rules and regulations promulgated thereunder; and
- Section 206(d) of the E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. 3501 note)
- Section 553 of the Administrative Procedure Act (5 U.S.C. 553).

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with Authority for FDIC Contact and Demographic Information.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

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

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

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?

Contact and request information generally includes name, business affiliation, mailing address, phone number, email address, and details of the request or public comment. Personally identifiable information such as Social Security numbers or dates of birth are not covered under this PIA. Such collections are required to conduct separate PIAs analyzing the risks associated with such collections. Additionally, FDIC may also ask FDIC customers, employees, and other stakeholders to provide optional demographic information such as age, race, country of origin, or personal occupation to gather experiences and opinions about a particular FDIC program or service.

Lastly, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect. The FDIC's Legal Division reviews all public comments and removes/redacts any unnecessary PII or information deemed to be inappropriate prior to posting the comments on FDIC's public-facing website. All comments that have been received, including those that have not been posted, that contain comments on the merits of a particular notice are retained in the public comment file in FDIC's shared document repository.

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.

Contact and demographic information inherit the retention schedules of the systems where they reside or the programs that develop and use them.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 FDIC Records and Information Management Policy Manual and National Archives and Records Administration (NARA)-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Directives 1210.01 and 1360.09.

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

The FDIC 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: FDIC may collect more demographic information than necessary for the purposes of process and operations improvement, as well as during the rulemaking process.

Mitigation: The risk is partially mitigated. The purpose of FDIC customer surveys is the collection of opinions and experiences of individuals, not to collect PII. Likewise, the primary objective of collecting public comments on proposed FDIC rulemakings is to help inform and enhance FDIC rulemakings, not to collect information about individuals. Although personal contact and demographic information is sometimes collected from individuals, this information, in the context of customer surveys, is aggregated and does not identify individuals. FDIC may also give individuals the option to voluntarily provide limited contact information to facilitate future correspondence (e.g., informational pamphlets, email notifications), but individuals are informed that they are not required to provide this information and their PII is not linked to the answers they provided during the customer surveys.

Further, during the rulemaking process, FDIC provides notice instructing individuals to submit only information that the commenter wishes to make available publicly. The notice also informs commenters that FDIC may review, redact or refrain from posting all or any portion of a comment that it deems to be inappropriate for publication, such as irrelevant or obscene material.

Privacy Risk: Collecting demographic information may allow for re-identification of an individual if the sample size is small and a specific individual's response is unique.

Mitigation: FDIC has instituted procedural safeguards to ensure the confidentiality of individuals is protected. Through the PTA process, questions that are deemed unnecessary or too specific to an individual during customer surveys are considered to be "over-collections" of information and are dropped from the questionnaire prior to distribution of the customer surveys or additional steps must be taken to remove the identifying information. Additionally, programs must work with the Privacy Section to determine appropriate thresholds to ensure that individuals cannot be re-identified.

Privacy Risk: Since individuals may have the ability to post information to collaboration tools, there is a risk that such postings could contain PII that is not about members or potential members of the tool. Additionally, there is the risk that public comments submitted in response to proposed FDIC rulemakings and notices may contain unnecessary or superfluous PII.

Mitigation: Users are provided notice at the time of registration and prior to posting any information that specifically instructs them to ensure that their comments and documents do not contain PII outside the scope of contact information about members or potential members of the collaboration tool. Collaboration tool administrators periodically review shared spaces to ensure that PII is not posted and have the ability to remove inappropriate member postings.

Similarly, individuals who submit public comments in response to proposed FDIC rulemakings, notices and other FDIC regulatory actions are provided notice at the time of submission and prior to posting that instructs them to submit only information that the commenter wishes to make available publicly. The notice also informs commenters that FDIC may review, redact or refrain from posting all or any portion of a comment that it deems to be inappropriate for publication, such as irrelevant or obscene material. The FDIC's Legal Division reviews all public comments and removes/redacts any unnecessary PII or information deemed to be inappropriate prior to posting the comments on FDIC's public-facing website.

Privacy Risk: FDIC may not be able to control third parties' retention of contact information and customer surveys responses.

Mitigation: This risk is partially mitigated. If FDIC contracts a third party vendor to assist in customer surveys that involves the collection of PII, then the FDIC ensures that it is the owner of all data collected. The vendor is required contractually to destroy all information associated with the information collection at the end of the contract. FDIC also contracts for the right to investigate and audit a vendor's systems to ensure they are complying with FDIC policies, procedures, and retention schedules.

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.

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 collects contact information directly from the individual to the greatest extent practicable. For individuals who have direct contact with the FDIC, the Corporation collects their PII directly from them. Emergency contacts and FDIC partners' points of contact do not have direct contact with FDIC. This individual's PII is provided by their organization or an FDIC employee or contractor. 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.

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

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

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

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

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

based on the FIPS 199 determination. In addition, guidelines on protecting the integrity of PII can be found in the FDIC Directive 1360.09 "Protecting Information."

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

The FDIC does not maintain any Computer Matching Agreements, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable risks associated with Data Quality and Integrity for FDIC Contact and Demographic Information.

Mitigation: No mitigation actions are recommended.

Section 8.0: Individual Participation

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

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

When information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from the individual authorizes the collection of the information provided.

There are systems that receive PII on individuals from FDIC employees, partners, and financial institutions. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. The FDIC does not make determinations on these individuals based on the information received from the sources listed in Question 1.1.

Additionally, this PIA and the SORN(s) listed in Question 2.2 serve as notice of the information collection. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third parties. According to the Administrative Procedure Act (APA). This includes publishing a statement of rulemaking authority in the Federal Register for all proposed and final rules. An agency that is in the

preliminary stages of rulemaking may publish an 'Advance Notice of Proposed Rulemaking" in the Federal Register to get more information; this Notice is a formal invitation to participate in shaping the proposed rule and starts the notice-and-comment process in motion.

The proposed rule, or Notice of Proposed Rulemaking (NPRM), is the official document that announces and explains the agency's plan to address a problem or accomplish a goal. All proposed rules must be published in the Federal Register to notify the public and to give them an opportunity to submit comments. Anyone interested (individuals or groups) may respond to the Advance Notice by submitting comments aimed at developing and improving the draft proposal or by recommending against issuing a rule. The proposed rule and the public comments received form the basis of the final rule. Individuals and entities may submit public comments to FDIC via email, postal mail, hand delivery at FDIC offices, or the FDIC's public-facing website (www.fdic.gov). Submitted comments may include the name, organization, and contact information of the commenter. FDIC provides notice to individuals at the time of comment submission, that their comments, including any personal information provided, may be posted without change to FDIC's public-facing website. The notice, therefore, advises commenters to limit information in their submission to only that which they wish to make available publicly. The notice also informs commenters that FDIC may review, redact, or refrain from posting all or any portion of comments that it deems to be inappropriate for publication, such as irrelevant or obscene material.

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 information is collected directly from the individual, the FDIC Privacy Program ensures that Privacy Act (e)(3) statements and other privacy notices are provided, as necessary, to individuals prior to the collection of PII. This implied consent from the individual authorizes the collection of the information provided.

There are systems that receive PII on individuals from FDIC employees, partners, and financial institutions. The FDIC does not have the ability to provide Privacy Act Statements or privacy notices prior to the Agency's processing of individuals' PII. The FDIC does not make determinations on these individuals based on the information received from the sources listed in Question 1.1.

Additionally, this PIA and the SORN(s) listed in Question 2.2 serve as notice of the information collection. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

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 FDIC collected the PII.

The project or system only uses PII for the purposes listed in Question 9.1. This PIA and the SORN(s) listed in Question 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[4], 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: There are no identifiable risks associated with Individual Participation for FDIC Contact and Demographic Information.

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.

[4] www.fdic.gov/privacy

The FDIC uses contact information to distribute information to the public, communicate with financial institutions' points of contact, document FDIC employees' emergency contacts, and collaborate with FDIC partners. Additionally, FDIC uses demographic information to solicit voluntary feedback from its employees, contractors, external stakeholders, and the general public through the use of surveys, interviews, and focus groups to improve FDIC services and operations.

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.

Contact and demographic information may be shared with internal FDIC divisions inasmuch as they are involved in distributing information, communicating with financial institutions' points of contact, conducting customer surveys, documenting emergency contacts, or collaborating with FDIC partners. However, FDIC does not share contact and demographic information for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose x will not be shared for use of purpose y at a later date.

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

The FDIC physical and information security policies dictate who may access FDIC computers and filing systems. Access to contact information is strictly limited by access controls to those who require it for completion of their official duties.

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.

Contact and demographic information may be shared with internal stakeholders inasmuch as those stakeholders are involved in distributing information, communicating with financial institutions' points of contact, conducting customer surveys, documenting emergency contacts, or collaborating with FDIC partners. Nonetheless, contact and demographic information is not shared for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose x will not be shared for use of purpose y at a later date.

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?

Yes, FDIC statistical or research experts aggregate and anonymize demographic data collected from participants to identify trends among groups and not individuals within those groups. The aggregated data is then analyzed, trends are documented, and recommendations may be made. A report may be distributed to appropriate FDIC stakeholders and the general public. There is no PII included in the published reports-only aggregated data is distributed in the published reports.

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.

Contact and demographic information may be shared with external governmental entities and contractors inasmuch as those entities are involved in distributing information, communicating with financial institutions' points of contact, conducting customer surveys, documenting emergency contacts, or collaborating with FDIC partners. Nonetheless, contact and demographic information is not shared for any purpose beyond which it was originally collected, i.e. contact information given by individuals for purpose x will not be shared for use of purpose y at a later date.

Additionally, through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1031.1 'Administration of the Privacy Act', and FDIC Circular 1360.17 'Information Technology Security Guidance for FDIC Procurements/Third Party Products'. The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Directive 1360.17 and FDIC Directive 1360.09.

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: Contact and demographic information may be used in ways outside the scope intended by the initial collection.

Mitigation: The risk is mitigated through several factors. FDIC stores this information on accredited systems that have sufficient security and privacy protections in place. FDIC does not make this information universally available to everyone; user access controls or other methods are in place governing who may view or access the contact and demographic information. All FDIC personnel are trained on the appropriate use of PII. Additionally, FDIC does not use the contact and demographic information to make decisions regarding individuals.

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.

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.

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 privacy risks associated with Security for FDIC Contact and Demographic Information.

Mitigation: No mitigation actions are recommended.

Appendix
Qualifying Systems or Projects (Ordered by Alphabet)

Active Directory

Active Directory (WinAD) is Active Directory Domain Services (domain controllers) running on Azure virtual machines on Windows Server 2019 operating system. WinAD manages the authentication and authorization functions for users and computers within an FDIC. WinAD replicates on premise Active Directory settings and syncs with Azure Active Directory (AAD) to allow SSO for users with prod.fdic.gov accounts. WinAD provides user access and stores directory information (user and computer objects) along with enforcing group policy settings and provides MFA enforcement to FDIC issued workstations (PIV or hard token). WinAD includes contact information about individuals that have been provided with an FDIC network account to interact with FDIC's network resources, which includes FDIC employees/contractors and various members of the public.

Alliance for Economic Inclusion (AEI) Collaboration Tool

The Alliance for Economic Inclusion (AEI) Collaboration Tool enables FDIC and AEI members to collaborate, educate, inform, and share resources on economic inclusion and community development, which may include FDIC and AEI member-created resources, past event presentations, and upcoming event calendars. AEI members are coalitions of local financial institutions, consumer, community and local government leaders who support the goal of promoting the widespread availability and use of safe, affordable, and sustainable financial products from insured depository institutions that help people achieve financial stability and build wealth. The AEI Collaboration Tool has chat, uploading, and video teleconferencing (VTC) capabilities. The AEI Collaboration Tool collects and maintains the names, telephone numbers, and email addresses of AEI member POCs in order to grant access to the platform.

Assessment Information Management System (AIMS) Cloud

The Assessment Information Management System (AIMS) is a cloud-based management application used by the Division of Finance (DOF) to invoice, manage and collect insurance premiums from more than 6,000 insured financial institutions. AIMS does not have any external users. However, authorized representatives of insured institutions are authenticated via FDICConnect (FCX) and PDFs of their respective invoices are shared with them via a bi-directional export/import with AIMS and FCX. The AIMS system maintains limited PII about members of the public, including the names and email addresses of financial institutions' points of contact.

CISR Documentum File Store (CDFS)

CSIR Documentum File Store is the system used to store, manage and analyze § 165(d) resolution plans (commonly known as living wills), § 360.10 plan analysis documents, recovery plans, and other artifacts containing sensitive firm-specific information related to Systemically Important Financial Institutions (SIFIs).

In terms of PII, the plans submitted by financial institutions may list names of principal officers (executives) along with a brief narrative of their role/title. In addition, administrative materials and artifacts stored in CDFS may contain names and business contact information (business address, email address and telephone number) for POCs at financial institutions, FDIC, and other Federal regulatory agencies.

Class Action Claims Solutions Processing System (CACSPS)

CACSPS manages litigation settlement administration for FDIC. Specifically in the case of the FDIC, this system is used to mail physical letters to individuals and businesses with non-deposit claims when a financial institution

has failed, informing them whether their claim is allowed or disallowed. The system stores full name and home address of claimants.

Consumer Affairs Reporting and Event System (CARES)

CARES is a configurable, cloud based, COTS solution for event and contact management. The tool is a SaaS-hosted platform that allows FDIC's Division of Consumer Protection to interact with the public through outreach, program activities, and engagement event execution. The CARES system collects and stores names, business addresses, email addresses, phone numbers, and information on FDIC employees and event registrants.

Corporate Business Information System (CBIS) – Legacy

Corporate Business Information System (CBIS) is an FDIC Corporate Data Warehouse that contains numerous databases which are updated from multiple sources, such as the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Consumer Financial Protection Bureau (CFPB) and Federal Financial Institutions Examination Council (FFIEC), via mainframe and extract, transform, load (ETL) batch jobs. CBIS contains financial and examination data that pertains to banks, bank holding companies, savings and loans holding companies and foreign banking organizations. This data is later used to feed and refresh multiple datamarts and applications residing across multiple platforms.

Corporate Business Information System (CBIS) – Redesign

CBIS Redesign is a modernization project designed to build a foundation to eliminate FDIC's dependency on the mainframe. CBIS Redesign is a cloud-based (Cloud.gov), secure solution aligned with FDIC's modernization roadmap and enterprise architecture, which will accelerate deployment of regulatory changes. CBIS Redesign replaces scheduled batch processing with a model of near real-time availability of data for consistent data consumption and distribution. CBIS Redesign will allow flexible and adaptable data processing to accelerate the deployment of regulatory changes.

Community Contacts Database (CCD)

Community Contacts is part of the FFIEC examination procedures. The Community Reinvestment Act (CRA) requires banks to serve their communities. Community contacts are a method to assess compliance with the CRA. Community Contacts Database (CCD) is a centralized repository to collect and store community contact information and community organization data gathered through interviews during the examination process. This data includes bank name, examiner's name, and the community contact's name, work phone number, work email address, and work address and the community contact's interview summary write-up entered by examiners.

CCD is accessible by FDIC through intranet and to Office of the Comptroller of Currency (OCC) and the Federal Reserve Board (FRB) through the extranet. Community Contacts Database will pull data from the SIMS SDC tables in Data Hub. CCD will replace the legacy on-premise application known as Community Contacts Application and will reside within the cloud on cloud.gov platform.

Contact Center as a Service (CCaaS) - Solution

The CCaaS solution will transform and modernize the existing on-premises legacy telephony, contact center and communications platform into Contact Center as a Service (CCaaS) by maximizing the use cloud services. The contact center will move to cloud based services, which will allow the full decommission of the legacy infrastructure. (CCaaS) Solution is an all-in-one cloud contact center solution that enables organizations to deliver frictionless customer and employee experiences across phone, email, chat, text and more. (CCaaS) provides a simple way to deploy, operate and scale customer experience orchestration technology from a modern composable cloud platform.

Center for Disease Control (CDC) Public Access Platform

The CDC Public Access Platform (CPAP), internally referred to as archive.fdic.gov, provides for the storage and hosting of archival documents for general public consumption. The solution is hosted by the U.S. Centers for Disease Control (CDC) and utilized by several federal agencies, including FDIC. The solution provides a stable, permanent archive (institutional repository) of publications and other materials and offers the ability to search the full text of all archived collections of public documents. It operates as an extension of the FDIC public internet presence and allows FDIC the ability to reduce their maintenance of historical materials. Older public documents are also being digitized and made available using the same framework. All material that FDIC will post to archive.fdic.gov has been previously released publicly.

The system contains publicly released documents relating to the history of the FDIC (e.g., Annual Reports, Press Releases, FILs, etc.). PII contained in the collections is generally limited to the names of FDIC employees acting in an official capacity or the names of other individuals mentioned in the documents (e.g., employees or officials of other agencies, researchers). Title and contact information may also be available for the FDIC employee or individual's position at the time of release.

Citizen Development Platform (CDP)

CDP is part of the Office Support Applications suite. CDP consists of the following three main products that empower FDIC citizen developers to rapidly create content to display in a browser, mobile device, or tablet:

- CDP BI is a SaaS used to create reports and dashboards using data-driven interactive visualizations for business intelligence analytics. CDP BI includes a suite of software services, apps, and connectors that work together to turn unrelated sources of data into sets of coherent, visually immersive, and interactive insights. The customer's data sources can include lists, spreadsheets or a combination of cloud-based and on- premises hybrid data warehouses. This business analytics tools assists with data analysis and insight sharing, business monitoring, and the ability to quickly find answers using search and rich visual dashboards available on every device.
- CDP Apps is a SaaS that provides a development environment used to create custom applications. CDP Apps includes a suite of apps, services, connectors and data platform that provides a rapid application development environment to build custom apps for business needs. Using CDPApps, customers can quickly build custom business apps that connect to business data stored either in the underlying data platform (Common Data Service) or in various online and on-premises data sources (Office Support Applications). CDPApps includes the Portal, Authoring Service, and RP.
- CDP Automate is a SaaS used to automated business processes through workflows to collect data, synchronize files, receive notifications, manage robotic process, and more. The service provides a low code platform for workflow and process automation. Automated flows, button flows, scheduled flows, business flows and User Interface flows are supported by the service.

Internal access to CDP is handled via single sign-on (SSO). For individuals who do not have physical FDIC-issued PIV cards, access is granted via two factor authentication. Account creation/verification is done via O365/AD and being passed back to CDP. Audit logs collect user name and email address, which could include the user names and email addresses of members of the public. For this collection of PII, PIA coverage is provided by this PIA. Additionally, this PIA provides coverage for CDP applications or solutions that collect, use or maintain contact and demographic information not in excess of the PII elements described in this PIA.

Cloud Foundation

The Cloud Foundation system is FDIC's standard cloud hosting environment that extends FDIC's infrastructure into the cloud and facilitate the cloud adoption initiative. Cloud Foundation provides cloud infrastructure capabilities, data management, data analytics services, and a secure suite of integrated managed cloud data services to quickly deliver and handle the scale, agility, and flexibility required to combine different types of data and analytics approaches to support FDIC business needs. The Cloud Foundation system consists of landing zones along with the list of FDIC approved cloud services that can be consumed. Landing zones are the output of a multi-subscription cloud environment that accounts for scale, security governance, networking, and identity.

Cloud Log Aggregation Warehouse (CLAW)

The FDIC participates in the Cloud Log Aggregation Warehouse (CLAW) program sponsored by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In conjunction with that program, FDIC will send the security logs of FDIC's cloud service providers to CISA. The logs include the FDIC UserIds of FDIC network users, which may include the FDIC UserIds of FDIC business partners.

Cloud Enterprise Logging

Cloud Enterprise Logging is a FedRAMP authorized cloud solution used by FDIC to provide various enterprise logging capabilities. The email addresses of members of the public exchanging emails with FDIC could be included in the email header information collected and processed by this solution.

Cloud Applications Platform

Cloud Applications Platform is a flexible and customizable cloud-based Platform as a Service (PaaS)/ SaaS provider that is used by FDIC to configure new business capabilities and applications. Applications instantiated on this platform are subject to an FDIC PTA, which may indicate the need for a PIA and SORN coverage. The respective PIAs and/or PTAs will describe the applications, their uses and purposes, and the privacy risks they pose. Cloud Applications Platform collects and maintains PII in the form of audit log information.

Contractors' Workforce Dashboard (CWD)

The Office of Minority and Women Inclusion (OMWI) under Dodd-Frank Section 342(c) mandates OMWI implement procedures to ensure the fair inclusion of minorities and women in contracting with the FDIC. The objective of CWD is to improve operational efficiencies and accuracy of contractors' workforce data. This information is leveraged for the purpose of enabling OMWI to assess whether there is clear evidence the contractor has a plan, program or initiatives to ensure the "fair inclusion" of minorities and women in the workforce. Contractors with 50+ employees and $50,000 in awards must maintain a written Affirmative Action Program (Executive Order 11246). This tool enables OMWI to track and report on the contractor's Good Faith Effort (GFE) and progress toward the goal of contractor fair inclusion.

The CWD website supports the OMWI GFE review process. OMWI collects and requests the GFE Review Form details using the website. The contractor's submission of the GFE Review Form initiates the good faith effort review process. Additionally, CWD delivers a series of analytical dashboards to provide OMWI with insight into various functional components related to the fairness within FDIC's Contractors Workforce. Additionally, CWD consolidates all related data and further develop visualization solution that presents key risk and performance metrics OMWI – Stakeholders. The solution will also automate the collection of data where possible to generate these metrics for improving efficiency and accuracy. CWD processes names, email addresses, telephone numbers, and demographic information.

Customer Service Contact System (CSCS)

The Customer Service Contact System (CSCS) is used by the Division of Resolutions and Receiverships to maintain an inventory of historical data related to failed financial institutions, (i.e., chain of title receiverships, mergers, acquisitions, changes in ownership, locating of financial successor) and applicable points of contact. Contact information related to claims, loans, real estate, subsidiaries, closings, and oversight within the FDIC is also maintained by the system. Contact information includes name, and work phone number, email address, and physical address.

Data Gathering Tool (DGT)

The FDIC Data Gathering Tool (DGT) is a pre-examination tool developed by the Division of Depositor and Consumer Protection (DCP) and will be utilized by the Division of Risk Management Supervision (RMS). The DGT gathers and displays financial information and is used by examiners to define the scope of upcoming bank examinations. The only PII the DGT displays is the name of bank presidents, bank compliance officers, and a bank provided telephone number.

Electronic Deposit Insurance Estimator (EDIE)

Electronic Deposit Insurance Estimator (EDIE) is designed to give an accurate deposit insurance calculation, assuming it is properly used and the account information is correctly entered. However, the results and conclusions generated by EDIE are strictly advisory. All actual claims for deposit insurance shall be governed exclusively by information set forth in the FDIC-insured institution's records and applicable federal statutes and regulations then in effect. EDIE Estimator can calculate your FDIC insurance coverage for each FDIC-insured bank where you have deposit accounts. EDIE lets you know in a printable report for each bank whether your deposits are within or exceed coverage limits.

Electronic Pre-Exam Package (ePREP)

The tool employs scoping questions to facilitate tailoring the lists to the specific profile of the institution to be examined and is designed to support a community bank focus while allowing users to customize the request package for larger and more complex institutions. It also houses an interface for the ePREP Workgroup to manage request list content. ePREP pulls in data from the Enterprise Data Warehouse (EDW) in order to produce documents required for examinations of financial institutions. ePREP automatically pulls bank name, bank address, examination start date, employee name, employee title, and work phone number. In addition, financial information is pulled on each financial institution from the call report to automatically scope the examination. Finally, ePREP allows manual entry of non-sensitive bank contact information, exam scope, and request list items.

Electronic Visitor Management System (EVMS)

EVMS facilitates the management of granting temporary visitor privileges to FDIC buildings. EVMS is an automated system capable of managing pre-registration of visitors and is essential to the success of FDIC facility's use by the public and other government agencies. EVMS maintains information about visitors to FDIC facilities, such as their names, company, visit purpose, and name of their FDIC sponsor.

Enterprise Development Platform

The Enterprise Development Platform is a low-code/no-code platform with tools that allow FDIC employees and contractors to automate business processes, build applications, and analyze data. Enterprise Development Platform use cases are subject to evaluation, which may indicate the need for other PIA and SORN coverage. User names and email addresses are collected by Enterprise Development Platform audit logs.

Enterprise Directory Services

Enterprise Directory Services include contact information about individuals that have been provided with an FDIC network account so that they may interact with FDIC's network resources. FDIC network users include FDIC employees, FDIC contractors and various members of the public.

Enterprise Logging

FDIC uses a FedRAMP-authorized cloud solution that provides enterprise-logging capabilities, such as event log repository functionality, threat detection, forensic functionality, and automated log analysis, reporting, and alerting. The solution may collect the email addresses of members of the public that exchange emails with FDIC.

External Application Menu (EXTAM)-Cloud

EXTAM-Cloud is an FDIC application menu that provides external FDIC users with a secure entry point to specific FDIC applications to which they have been authorized access. EXTAM-Cloud processes the following types of PII: full name, email address, and user ID.

Extranet Identity Management (EIDM) and EIDM-Cloud

The EIDM and EIDM-Cloud applications provide authentication, authorization and account management for external users accessing FDIC applications. The main purpose of EIDM and EIDM-Cloud is to enhance FDIC's Identity Management capability for external users. EIDM and EIDM-Cloud collect, process and maintain information to authenticate and provide access for users external to FDIC (non-FDIC employees and non-FDIC contractors). Such information includes the user's full name, phone number, email address, User ID, timestamp, server name, server IP address, resource/application accessed, and session ID.

FDIC Emergency Notification System

The Emergency Notification System (ENS) enables the timely reporting of emergencies to FDIC employees and contractors. It provides for multiple communication device (voice, email, text) notification to registered FDIC personnel during and after local, regional or national emergency events and security incidents, disseminates time sensitive information, provides personnel accountability and status during emergency events, and conducts communication tests. ENS may contain PII about FDIC employees and contractors, as well as their emergency contacts, such as full names, phone numbers, and email addresses.

Federal Financial Institutions Examination Council's (FFIEC) Central Data Repository (CDR) GovCloud

The FFIEC CDR is used to collect, validate, manage, and distribute data reported by financial institutions, and is hosted at: https://cdr.ffiec.gov. The CDR supports processing the Reports of Condition and Income (Call Reports), Uniform Bank Performance Reports (UBPRs) and Summary of Deposits for FDIC-insured institutions. The CDR is overseen by an interagency steering committee under the auspices of the Federal Financial Institutions Examination Council that prescribes uniform principles, standards and report forms for the federal examination of financial institutions. The steering committee consists of representatives of the FDIC, the Board of Governors of the Federal Reserve System (FRB) and the Office of the Comptroller of the Currency (OCC). Call Report data is submitted by the financial institutions on a quarterly basis and SOD is submitted annually. Information related to individuals is obtained from two sources in the CDR: (1) user-specified information collected at the time of account creation and (2) contact information about individuals responsible for submitting reports on behalf of financial institutions. The PII consists of the following contact information: name, organizational affiliation (e.g., the name of the financial institution or agency where that person is employed), professional title, work address, work phone number, work fax number, and work email.

Financial Institution Diversity Self-Assessment (FID-SA)

Financial Institution Diversity Self-Assessment (FID-SA) is a portal that enables banks to complete their voluntary yearly diversity assessment. FDIC uses the information submitted by financial institutions to monitor progress and trends in the financial services industry with regards to diversity and inclustion in employment and contracting activities. The information collected by the FID-SA portal includes: financial institution name and address; points of contact information for the participating financial institution (names, titles, and work-emails/phone and fax numbers); yes/no responses with comments; and diversity data (workforce and procurement supplier).

GovDelivery

GovDelivery is an e-mail subscription management service enabling internal and external subscribers to sign up to receive FDIC publications, thereby reducing the load on FDIC Outlook servers. GovDelivery is a FedRAMP-

authorized Software as Service (SaaS) cloud service provider, which provides an outsourced e-mail subscription service to distribute FDIC information. E-mail addresses are entered manually by users when they subscribe to a publication, which can either be work or personal e-mail addresses. GovDelivery provides subscribers the option to receive news releases, Financial Institution Letters, statistical publications and other information.

Government Cloud Security

Government Cloud Security is a cyber resilience platform tailored to support federal institutions like the FDIC by securing internal system records and ensuring operational continuity. Combining backup and cybersecurity capabilities, it provides robust protection against cyber threats and system disruptions critical to the FDIC's mission. The Government Cloud Security will protect the Office Support Applications.

GSA api.data.gov

GSA forwards to FDIC the names, email addresses, and IP addresses of api.data.gov users that would like to access FDIC data that is made publicly available on GSA's api.data.gov website or that have questions or comments regarding FDIC data made publicly available on GSA's api.data.gov website. FDIC uses that information for data usage analytics and to respond to questions or comments submitted by individuals regarding FDIC data made publicly available on GSA's api.data.gov website.

Help Desk Ticketing Software

Help Desk Ticketing Software is a cloud provider of Information Technology Service Management (ITSM) ticketing software, and is used to track information technology helpdesk tickets (Incidents, Changes, Problems, and Service Requests), track information technology assets and configurations, manage reservations for individual workspaces, meeting rooms, and parking spaces. Additionally, ITSM manages resource requests and workflow for projects and enhancements, application implementation work, performance trend analysis, and related technical communications needed to perform IT Service Management, IT Operations Management, IT Business Management and IT Asset Management with internal stakeholders. The Old Ticketing Software (OTS) system was replaced in functionality by Help Desk Ticketing Software and remains now only for historical data retention. OTS was used to manage FDIC security incidents, breach investigations, vendor security assessment, business continuity/disaster recovery operations and security artifacts related to FDIC information systems. OTS did collect and maintain names, email addresses, and telephone numbers of FDIC employees, contractors, or members of the public if they are associated with an FDIC incident or breach.

How Money Smart Are You - Cloud

How Money Smart Are You? (HMSRU) is a public-facing application that provides financial education in the form of 14 interactive games created in Articulate Storyline. The games, with related resources, are collectively called HMSRU? Users can create an account or play without an account. If users choose to create an account, they can log in and out as often as they want and their place is saved in the game-play. Creating an account and logging in is required to receive certificates of completion.

Intranet Web Content Management System

The Office of Communications (OCOM) utilizes a web content management system (WCMS) to build and maintain content on FDIC's intranet website. The information and data on the FDIC intranet (internal) website is used by FDIC staff and contractors and can only be accessed when logged into the FDIC network. As a WCMS, FDIC divisions and offices are able to manage the information and data on their respective pages within the FDIC intranet website more efficiently than without a WCMS. The FDIC intranet website provides FDIC staff and contractors with information that is needed to carry out their duties more effectively.

Joint Cybersecurity Authorization & Management (JCAM)

JCAM is a web-based tool developed and managed by the U.S. Department of Justice (DOJ) to support federal agencies with information systems security GRC functions. JCAM is used by FDIC to support Risk Management Framework functions and tasks in support of security categorization, controls selection, systems security documentation, findings, risk assessments, and Plans of Actions & Milestones and Acceptances of Risk. JCAM collects and maintains the names, email addresses and telephone numbers of FDIC employees and contractors. Additionally, the JCAM audit logs for FDIC collect the network IDs of DOJ JCAM administrators supporting the FDIC's use of JCAM.

Large Insured Depository Institutions (LIDI)

The LIDI Program is designed to provide comprehensive analysis of the risk profiles of insured depository institutions (IDIs) with total assets of at least $10 billion. The timely and thorough analysis of these institutions supports these objectives:

- Identify, monitor, and control the largest risks to the Deposit Insurance Fund (DIF);
- Support discretionary adjustments to deposit insurance premium assessments;
- Inform potential resolution-planning decisions and estimate potential losses;
- Identify emerging risks and trends in the banking industry; and
- Document and communicate risks to senior FDIC management.

LIDI collects and maintains PII in the form of: full name and employment information.

Joint Venture Transaction Program

Joint Venture Transaction Program is resolution process that creates single-purpose entities into which assets from one or more failed institutions are conveyed via an Asset Contribution (and Sale) Agreement. LLCs with single family or commercial assets are required to report detailed information about these assets monthly to the Division of Resolutions and Receiverships (DRR). The Federal Deposit Insurance Corporation (FDIC), as receiver for one or more failed institutions, owns an equity interest and/or other financial interest in structured transactions LLCs. The Pre- and Post-Closing Support Contractor (CSC) and others in the DRR monitor the financial performance of individual LLCs. Each month, the LLC uploads monthly reports and data files to FDIC's Resolution Transaction Submission Portal (RTSP). The CSC retrieves those files and saves them to their FDIC SharePoint site, which is the official repository for all LLC documents. The CSC then performs a review of the monthly reports and, upon completion, prepares a summary report and uploads it to their SharePoint site. DRR utilizes the Transaction Program, which is a repository that is used to input and store the aggregate financial and accounting data submitted monthly by each Managing Member (MM). The data that is aggregated within the Transaction Program is a subset of the entire monthly report.

Mainframe

The FDIC Mainframe System supports the processing of high volume, centrally controlled transactions for FDIC legacy and client-server applications. The logon IDs and passwords of FDIC business partners requiring access to those applications are collected and maintained by the Mainframe System.

Mailroom Application (FedRAMP)

The Mailroom Application is a web-based application and user-friendly interface that helps Mailroom Agents to process, track and monitor packages that are either received or sent. It also allows them to print Stamps using Stamp Sheets or Stamp Roll stock that are standalone for any of the shipments. Analytics is also available to them to view and track mailing activity.

MOU Repository

MOU Repository is a central source of Memoranda of Understandings (MOUs) and Interagency Agreements (IAAs) and a database for reporting to which FDIC is a party. The repository contains official case files of MOUs and IAAs, which include original signed agreements. The system contains the names and contact information such as phone, email, and business address for parties to the MOU and IAA.

MRM Tool - Minority and Women-Owned Business (MWOB) Application Implementation

The mission of the FDIC's Office of Minority and Women Inclusion (OMWI) is to ensure equal employment opportunity for all employees and applicants for employment; to achieve and maintain a diverse workforce and inclusive workplace; to increase participation of minority-owned and women owned businesses in FDIC programs and contracts; and to assess the diversity policies and practices of FDIC-regulated financial institutions. MRM (Minority- and Women-Owned Business (MWOB) Relationship Management (MRM) Tool) will enable OMWI to capture and manage contact information and capability statements provided to the FDIC by those MWOBs at technical assistance events, and through market research and vendor communications (in person, email, and phone). The MRM Tool will support OMWI targeted acquisition planning activities by enabling OMWI Specialists to identify viable MWOBs for contracting opportunities by searching the lists of capabilities provided by those MWOBs. MRM Tool collects and maintains PII in the form of: full name, work phone number, and work email address.

Office Support Applications

Suite of software applications used for word processing, spreadsheets, presentations, email, calendars, contact lists, and collaboration. Office Forms is a web-based application included in the Office Support Applications suite that is designed to easily create surveys, quizzes, polls, and questionnaires. It allows users to efficiently gather feedback and data from various stakeholders such as employees. Forms has many features: it allows users to import data from other Support Application products; it can be pre-answered with the most common response; Quiz Practice Mode is a feature for educational and training purposes, allowing respondents to practice skills or test their knowledge with immediate feedback; Forms can be inserted into any Office Support Applications Product such as slideshows or meeting software for interactive engagement and real-time feedback during meetings and training sessions.

Online Ordering System (OOS)

The FDIC offers free publications to the general public and banking industry to promote public confidence, disseminate consumer protection information, and educational material. OOS will be supported using an enterprise shared service to deliver the functions necessary for a public facing Online Ordering System in which users can order print products and download digital versions of print publications. The solution will also include an internal OOS application used to manage and administrate the public-facing portal.

Public Comment Solutions

FDIC's Legal Division may utilize spreadsheets, databases, and FDIC-approved document repositories and platforms to track and manage FDIC rulemakings, notices and other regulatory actions, along with the public comments that are received for them. For example, the FDIC uses the NPR Comments Review solution to assign and track reviews of certain rulemakings and public comments that are received for them. Authorized users within the Legal Division are able to manually create records within the system and import information from the public comment file, which is maintained in an FDIC shared document repository. Public comments received by FDIC generally contain the names of the entities or individuals submitting the comments, their comment, and organization and contact information (if provided in the submission).

Pre-Examination Planning (PEP)

Pre Examination Planning (PEP) is an automated tool for generating the pre-examination interview and information and document request package for Compliance and CRA examinations of financial institutions conducted by DCP staff.

Premise Tracker/Repudiations (PREMISE)

PREMISE is an application used by DRR's Asset Management branch. It provides a centralized repository to maintain and track institution-specific information about owned and leased bank premises held by failed institutions as well as all contracts and leases held by the failed institutions. Documents related to premise inspections are stored in Documentum.

Qualified Financial Contracts Compliance Tracking Application (QFCCT)

Qualified Financial Contracts Compliance Tracking Application (QFCCT) allows users to administer the progress of insured depository institutions (IDIs) that receive notification letters under 12 CFR Part 371: Recordkeeping for Qualified Financial Contracts (QFCs). The primary purpose of the application is to record and report on the status of each institution in its efforts to satisfy the recordkeeping requirements of the rule. The FDI Act requires FDIC to make a determination on QFC contracts within one day from receivership. The QFCCT database monitors the progress of institutions that were notified under Part 371 to ensure compliance with the FDI Act's requirements. QFCCT application system is also used to: 1) quickly ascertain the volume and types of QFCs reported in the IDI's quarterly call reports and 2) determine the composite ratings of IDIs (needed to determine the extent/scope of required QFC recordkeeping reporting, and the period of time permitted to come into compliance with Part 371). PII that may be collected and maintained within QFCCT includes: full names, business addresses, phone numbers, and email addresses of the Chief Executive Officer of the financial institution.

Qualified Financial Contracts – Dodd Frank Act (QFC-DFA)

The Qualified Financial Contracts - Dodd Frank Act (QFCDFA) solution was established to receive and analyze detailed qualified financial contract information required under the QFC recordkeeping rules outlined in 31 CFR Part 148 (Department of the Treasury ("Treasury"), applicable to non-bank financial companies) and 12 CFR Part 371 (Federal Deposit Insurance Act (FDIA), applicable to Insured Depository Institutions). QFC data set submissions are used to: 1) confirm a firm's ability to comply, and ongoing compliance, with the respective recordkeeping rules; and 2) prepare the analyses required to complete a QFC Determination in the event of a financial firm failure. PII that may be collected and maintained within QFCDFA includes: full names, business addresses, phone numbers, and email addresses of the point of contact or trading desk for each of the QFC positions. This information is used for clarification purposes, and notification of the FDIC's intent to transfer or repudiate contracts under receivership powers

Receivership of Assets in Litigation (RAIL)

Receivership of Assets in Litigation is the FDIC's repository for all asset litigation. RAIL tracks, monitors and reports outstanding asset litigation related matters overseen by National Servicers, Contractors, Receivership field sites, the FDIC Legal Division and FDIC Account Officers that assists all areas of Asset Management and Marketing and Owned Real Estate (ORE) in the asset resolution process. RAIL captures a number of data elements pertaining to the tracking of assets that are involved in various types of litigation. This information includes descriptive and tracking factors such as Case Number, Asset ID Number, Matter Number, values, and applicable dates. The system also collects some PII on personnel, including the name and email of FDIC employees who access and utilize the system; ORE point of contact information; and third-party legal counsel name, address, phone number, and email.

Resolution Information Tracking Application (RITA)

RITA supports DRR Resolution Strategy Branch (RSB) in customer relationship management, institution monitoring, resolution tracking, data management and reporting. RITA is a Customer Relationship Management (CRM) solution that provides consistent and responsive risk monitoring, sales, and marketing management for Federal Deposit Insurance Corporation (FDIC) personnel with responsibility for the resolution of failing financial institutions. The RITA solution addresses DRR's responsibilities related to the regulatory outreach, bank monitoring and resolution planning business capability by enabling an end to end Monitoring and Risk Analysis and Franchise Marketing process.

Resolution Plan Review Program (RP2)

Resolution Plan Review Program (RP2) is a web-based tracking tool used to store the reviews of Dodd-Frank Act filings of resolution plans for large financial institutions. The purpose of the resolution plans authorized under the Dodd-Frank Act is to ensure the covered companies can be resolved rapidly and orderly under the bankruptcy code. The purpose of the resolution plans authorized under the Federal Deposit Insurance Act is to ensure the FDIC has the information necessary to conduct a resolution of a large bank that provides depositors prompt access to their funds and maximizes returns to creditors. RP2 provides management reports summarizing the status of these reviews. RP2 includes the names of the FDIC POC, responsible for the resolution plan review, and bank resolution plan contact, who has been designated as the liaison with the FDIC on the resolution plan. FDIC uses this information to contact the liaison at the bank periodically throughout the review process with questions regarding the resolution plan.

Survey Software

The survey software is proprietary and externally hosted. It provides the ability to generate and manage web-based surveys, and a variety of reporting and analytic tools that allow authorized FDIC users to track survey results and configure custom reports.

Structure Information Management System (SIMS)

Structure Information Management System (SIMS) (Legacy) maintains all structure data for financial institutions insured, supervised, and monitored by FDIC. Structure data is used by the Data Collection and Analysis Section. It is non-financial and public in nature and encompasses attribute, classification, and ownership information. SIMS collects contact information from senior financial institution staff as well as basic organizational information.

Structure Information Management System (SIMS) Redesign

SIMS maintains all structure data for financial institutions insured, supervised, and monitored by FDIC. Structure data is used by the Data Collection and Analysis Section. It is non-financial and public in nature and encompasses attribute, classification, and ownership information. The purpose of the replacement of legacy SIMS ("SIMS Redesign"), is to automate the collection and processing of financial institution structure information. The initial release has automated 6 types of changes across 5 different source systems and tracks all other changes which need to be made against the legacy DB2 database. TheMarch 2020 release, has replaced DB2 with the redesign as the system of record and improve the distribution of information to the downstream applications. Once all the downstream applications have migrated to the new redesigned interface, the legacy DB2 will be retired.

Supervision360

Supervision360 is a large, business process modernization program that has been initiated on the Intelligent Business Process Management System (iBPMS). Phase 1 of S360 includes: Regulatory Filings which are documents submitted to the FDIC by an insured depository institution as required by law or policy. These are to inform of a new or change in activity, others are to ask permission to engage in an activity, and others fulfill

ongoing one time or recurring notification/reporting requirements; Risk Related Premium Rating Validation for CAMELS ratings of insured depository institutions for FDIC quarterly assessments; and Institution 360 which is a comprehensive view of a regulated entity distilled into a single display.

Two Factor Authentication (2FA)

2FA is a two-factor authentication service used by FDIC to validate users external to FDIC (non-FDIC employees and non-FDIC contractors) and facilitate their secure access to FDIC applications. 2FA collects, processes and maintains the user's full name, phone number, and email address.

Travel Administration System

The Division of Finance (DOF) within FDIC is responsible for providing assistance to FDIC employees at all headquarters, regional and field office sites when making reservations for airline tickets, hotel accommodations, and automobile rentals for official travel. FDIC/DOF has contracted with a vendor to assist FDIC employees (travelers) in making official travel arrangements, consistent with FDIC travel policies, cost considerations, and employee preferences. The vendor provides FDIC travelers and travel specialists with a secure, self-service online booking engine (OBE) for making reservations (air, rail, lodging, car rental, etc.), preparing travel authorizations and vouchers, producing itineraries, and obtaining tickets and receipts. The system maintains information about FDIC employees/travelers, along with their emergency contact information (full name, home address, and home telephone number), for which this PIA provides coverage.

Virtual Training Classroom Environment

The Virtual Training Classroom Environment is a web-based service that offers FDIC's Corporate University (CU) instructors a platform to conduct training courses for examiners and also have leadership-type courses where they can present the material and have PowerPoint slides displayed during instruction. CU administrators will set up and configure the virtual classrooms and are able to upload the training course material for participating students (both FDIC and non-FDIC) to download the materials for their use. The virtual classroom is regulated based on the way it is configured. Some instructors will require a login, while other instructors will assign a display name along with instructions on how to use their assigned display name. Participating students will receive the virtual classroom information, including the URL, any required login information, or assigned display name information, after they are registered for the course.

Vulnerability Disclosure Policy (VDP) platform

The Vulnerability Disclosure Policy (VDP) Platform is a service offered by the DHS Cybersecurity and Infrastructure Security Agency (CISA) to federal agencies to improve the security of federal agencies' internet accessible systems through a centrally managed vulnerability intake system. CISA's VDP Platform is a software-as-a-service application designed to allow security researchers and members of the public to alert FDIC about issues on their internet facing systems. All members of the public are eligible to participate in reporting potential vulnerabilities through the VDP platform. They may submit their findings anonymously or create a user account on the VDP platform. The creation of a user account allows the reporter to track and receive status updates related to their reporting of a potential vulnerability. In instances where a user creates an account, the VDP platform will collect the user's first name, last name and email address.

Zero Trust Network Access (ZTNA)

Zero Trust Network Access enhances access control to resources in the cloud and the data centers. It reduces reliance on internal firewalls by filtering and securing website access and consolidates other capabilities into the platform, to include always on patching and access to security tools when an Internet connection is made. ZTNA

is an agency identified function of the Zero Trust Network pillar intended to comply and align with OMB M-22-09 and NIST SP 800-207.