

**Privacy Impact Assessment (PIA)
for
FDIC Contact and Demographic Information**



PIA-FDIC-1261

July 5, 2020

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 website¹, which describes FDIC's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The 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, 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 the public, financial institutions, and 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, SharePoint sites, and collaboration tools. Additionally, this PIA discusses the privacy risks of collecting the contact and demographic information of (1) members of the public who seek information and/or services from FDIC and (2) individuals who are designated as points of contact and emergency contacts.

Contact Information

General Contact Information

FDIC maintains limited contact information in order to facilitate its operations and services to the public, financial institutions, and its partners. For example, a member of the public may request mail or email updates regarding proposed banking regulations, or partners working on cross-agency project may need to be able to contact their peers. In those cases, FDIC collects general contact information such as name, email address, and mailing address. 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.

General information intake involves the following:

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 its 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.

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

¹ www.fdic.gov/privacy

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. Individuals who provide information during customer surveys do so voluntarily with the understanding that their responses will be kept confidential.

Although the customer surveys assessed in this PIA is 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, gender, 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.

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 surveys participants may discontinue participation for the duration of the interaction.
3. FDIC projects and programs must work with the Privacy Section to ensure that program or project meet all privacy requirements.
4. FDIC projects and programs must set limits on the posting and sharing of PII.
5. FDIC projects and programs must be appropriately authorized.
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.
7. This PIA does not cover the use of contact and demographic information maintained on social media platforms. A separate PIA will be required for this use.

All systems or projects covered under this PIA will be added to the Appendix of this document.

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 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 individual 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 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 to 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 or operational 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 demographic information than necessary for the purposes of process and operations improvement.

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. Although personal contact and demographic information is sometimes collected from individuals, this information 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.

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.

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 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.

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 1.0: Information System

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

Contact information generally includes name, business affiliation, mailing address, phone number and email address. Personally identifying information such as a 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, gender, race, country of origin, or personal occupation to gather experiences and opinions about a particular FDIC program or service.

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Place of Birth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Social Security Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother’s Maiden Name	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Home Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number(s)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

PII Element	Yes	No
Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Driver's License/State Identification Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Education Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Criminal Information	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Military Status and/or Records	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Investigation Report or Database	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other (Specify: User credentials and demographic information)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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 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.

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.

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 Privacy Act SORN 30-64-0002, Financial Institutions Investigative and Enforcement Records, which covers contact and demographic information from financial institutions and FDIC partners;

- FDIC Privacy Act SORN 30-64-0005, Consumer Complaint and Inquiry Records, which covers contact and demographic information from members of the public;
- FDIC Privacy Act SORN 30-64-0013, Insured Financial Institutions Liquidation Records, which covers contact and demographic information from financial institutions and FDIC partners;
- FDIC Privacy Act SORN 30-64-0015, Personnel Records, which covers contact information from emergency contacts; and
- FDIC Privacy Act SORN 30-64-0019, 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.

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 three years or as needed.

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

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 Circular 1213.1 '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, the Privacy Act System of Records (SOR) Clearance Officer, and the Privacy Program (Privacy@fdic.gov). The Protecting Privacy subpage discusses general practices related to the Privacy Act and PII. See <https://www.fdic.gov/about/privacy/protecting.html>.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: 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.

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

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

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

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

Individuals are notified of the procedures for correcting their information through the SORNs identified in Question 2.2, this PIA, as well as FDIC FOIA Reading Room, available at <https://www.fdic.gov/foia/readingroom.html>. 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 to 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 research, or have any adverse or operational 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 Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional Information Security Managers located within the agency's divisions and offices.

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

Risk analyses are an integral component of FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and 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, <https://www.fdic.gov/about/privacy/index.html>.

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

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

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

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

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

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: 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 Circular 1360.20 'FDIC Privacy Program' mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws:

- Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

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 information generally includes name, business affiliation, mailing address, phone number and email address. Personally identifying information such as a 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, gender, 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.

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 Circulars 1210.1 and 1360.9.

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

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

Privacy Risk Analysis: Related to Minimization

Privacy Risk: FDIC may collect more demographic information than necessary for the purposes of process and operations improvement.

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. Although personal contact and demographic information is sometimes collected from individuals, this information 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.

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.

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.

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 Circular 1360.9 "Protecting Sensitive Information."

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable risks associated with Data Quality and Integrity for 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 personally identifiable information (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.

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

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: 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.

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

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

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 Circular 1360.17 and FDIC Circular 1360.9.

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

Annual information security and privacy awareness training is mandatory for all 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 personally identifiable information (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.