FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA) for The Division of Risk Management and Supervision's (RMS) Background Investigation Process

May 8, 2022

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

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

SYSTEM OVERVIEW

Describe what this information system[1] does in terms of purpose, functionality, and PII collection/use. What is the goal of the system? What gap does it serve to close?

The FDIC's Division of Risk Management Supervision (RMS) Cyber Fraud and Financial Crimes (CFFC) Section is responsible for conducting background investigations (BIs) in connection with applications and notices submitted to the Federal Deposit Insurance Corporation (FDIC), such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act,[2] and notices subject to Section 32 of the FDI Act.[3] These investigations are conducted to determine if the proposed individuals have the experience, competence, integrity, character, financial ability, and willingness to direct and/or lead a bank's affairs in a safe, sound, and legal manner. As part of this process, an FBI Fingerprint Identification criminal history records check is required. To execute this check, FDIC contracts with a third-party vendor to collect and transmit subject fingerprints to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (CJIS) to complete the investigation through its Integrated Automated Fingerprint Identification System/Next Generation Identification (IAFIS/NGI).[4] Additionally, in order to complete the BI process, FDIC shares information with the FBI, the Department of Homeland Security's Immigration and Customs Enforcement (ICE), credit bureaus, and external BI vendors. This PIA covers the background investigation process, including the collection and maintenance of fingerprints and FDIC's use of the Background Investigation Database System (BIDS).

RMS CFFC uses BIDS to track and manage BI requests (e.g. FBI Fingerprint Checks, FBI Name Checks, and Financial History Checks) for investigations of individuals including, potential bank directors, officers, and principals (subjects of investigations). These data requests contain Social Security numbers (SSNs) and other sensitive personally identifiable information (PII) about subjects of investigations. Accordingly, BIDS requires the highest level of security possible within the FDIC and is maintained in a secured, networked environment that can be accessed only by authorized RMS personnel at Regional and Washington Office locations. Critical features of the BIDS system include:

1. Data is accessible nationwide within the FDIC (Regional Offices and Headquarters);
2. Data is stored in a secure database environment;
3. An applicant's BI case is tracked through the entire life cycle;
4. BI request documents are auto-generated (PDF);
5. Notifications to certain users is automated at key event points;
6. Legacy (converted) BI data is presented; and
7. There is a capability to generate various management reports, such as Monthly, Quarterly, and Annual Volume Reports.

[1] OMB Circular No. A-130, "Managing Information as a Strategic Resource," (July 27, 2016). The Circular defines an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[2] 12 U.S.C. § 1829
[3] 12 U.S.C. § 1831(i)
[4] For more information, please see the IAFIS/NGI PIA available at https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

BIDS is composed of a secure web front-end to capture and manage BI case data. The front-end interfaces with a secure and robust database system that has the ability to both track BIDS application activities and also provides an audit capability. BIDS relies on the Active Directory (AD) to authenticate a BIDS user's login and password. BIDS uses the AD to pull the list of approvers and case managers from the BIDS AD Groups.

Background Investigation Process

The individual undergoing the BI (subject) provides their personal information when he/she completes and submits to the FDIC a formal application and the Interagency Biographical and Financial Report (OMB No. 3064-0006). This is provided during the application process in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act,[5] and notices subject to Section 32 of the FDI Act.[6] Once the FDIC receives the required information from the individual in hard copy (typically via FedEx/UPS), an authorized RMS user manually enters the information into BIDS. Hard copies are maintained in a locked file room; separate electronic copies, when received, are not maintained. If information is missing, the FDIC case managers may contact the individual to obtain it. Additionally, authorized BIDS users will add data for tracking the requests, as well as the results of each BI processed (Fingerprints, Name Checks, or FDIC DOA Library Requests, such as credit bureau checks). BI reports and documents may be attached in BIDS. Upon receipt of information from the agencies providing BI information, case managers may enter appropriate notations into the freeform text fields.

To obtain fingerprint results, the FDIC requires applicants to make arrangements to be fingerprinted via a third-party vendor. The applicant schedules a fingerprinting appointment at the vendor's website and uses a code RMS provides to schedule his/her fingerprint appointment. The applicant follows a standard protocol to provide identifying data that will facilitate the FBI fingerprint check. This information includes: full name, any previous or current aliases, signature, home address, name of current employer, citizenship, Social Security number (SSN), date of birth (DOB), place of birth (POB), sex, race, height, weight, eye color, hair color, and fingerprints. It is a mandatory requirement of the FBI to provide the aforementioned identifying information in order for the FBI to process the request. When the applicant arrives for fingerprinting, he/she must bring two valid forms of government-issued photo identification (i.e., driver's license, passport). A record is made only of the type of documents employed for identity (ID) validation; a copy of the actual documents is not made or retained by the third-party vendor. After the fingerprint results are complete, authorized RMS personnel retrieve the FBI fingerprinting results from the secure FDIC site/section of the third-party vendor's system.

To manage the BI process, authorized BIDS users add data for tracking the requests, as well as the results of each BI processed (Fingerprint, Name Checks, or FDIC DOA Library Requests, such as credit checks). Upon receipt of information from the entities providing BI information, case managers may enter appropriate notations into the freeform text fields. Should an applicant receive an unfavorable decision, applicants are given thirty (30) days to file a written appeal by certified mail.

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Access and Amendment;
- Data Minimization;
- Data Quality and Integrity; and
- Purpose and Use Limitation.

Access and Amendment

[5] 12 U.S.C. § 1829
[6] 12 U.S.C. § 1831(i)

Privacy Risk: Authorized RMS users manually enter or upload into BIDS background and credit information received from external business entities and other government agencies, such as the results of background name checks, fingerprint checks, credit checks, and public record searches conducted on subjects.

Mitigation: The FDIC relies upon the entities and agencies that collected the PII to ensure that the PII is correct. Individuals may contact the external entities and agencies directly to access and amend PII. The external entities and agencies that provide the background and credit information for use in BIDS have a vested interest in ensuring that the information they provide, including any PII, is correct to preclude compliance issues with Federal mandates, such as the Fair Credit Reporting Act. No additional mitigation actions are recommended.

Data Minimization

Privacy Risk: More information may be collected than is necessary to complete a background investigation.

Mitigation: FDIC limits the scope of information collected in BIDS to the amount of data necessary to complete a background investigation. Although the system stores PII provided in the application, this information is captured only where it is relevant to the investigation. Any PII identified by FDIC staff as not necessary to complete the investigation is redacted prior to input into BIDS or deleted from BIDS upon discovery.

Data Quality and Integrity

Privacy Risk: Background and credit information received from other government agencies and external entities may be inaccurate.

Mitigation: The external entities and agencies that provide the background and credit information for use in BIDS have a vested interest in ensuring that the information they provide, including any PII, is correct to preclude compliance issues with Federal mandates, such as the Fair Credit Reporting Act. Individuals should contact these external entities and government agencies directly to correct their personal information. No additional mitigation actions are recommended.

Privacy Risk: Conflicting information received from government agencies and external entities may have adverse effect on suitability status of an applicant.

Mitigation: FDIC case managers check and cross reference the information received from other government agencies and external entities to identify any discrepancies in the information. If during the review of this information FDIC staff notices discrepancies between two sources, and it requires further clarification, case managers will notify their Section Chief. The Section Chief will determine whether notification to the applicant and requesting supporting or clarifying documentation is warranted.

Privacy Risk: FDIC employees rather than the individuals themselves perform data entry of BI subjects' information and this may result in inaccurate information.

Mitigation: FDIC case managers verify the accuracy of the information at the time of collection. Case managers correct and update information if they become aware they entered inaccurate information.

Purpose and Use Limitation

Privacy Risk: FDIC's third party fingerprinting vendor may use BI subjects' data for unauthorized purposes.

Mitigation: FDIC's third-party fingerprinting vendor is an authorized channeler on behalf of the Federal Bureau of Investigation (FBI) and as such, undergoes rigorous oversight by the FBI. The FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard), which must be adhered to by the vendor, forbids the use of BI subject's data for commercial purposes. Additionally, FDIC's third-party fingerprinting vendor is bound contractually to use BI subjects' data only for the collection and transmission of fingerprints to the FBI.

Section 1.0: Information System

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

The background investigation information contained in BIDS includes the following PII pertaining to the individuals being investigated (BI subjects): subject name, maiden/alias name, Social Security number (SSN), passport number, date/place of birth, home and business address, maiden name of mother, name of father, name of spouse, employment status/records, investigative reports, legal documents/records/notes, date/place of prior convictions, and name(s)/address(es) of business(es) with which the BI subject is associated. In addition, BIDS contains the results of background name checks, fingerprint checks, credit checks, and public record searches conducted on subjects. Reports on BI results may be attached, and associated comments may be input.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☐	☒
Email Address (non-work)	☐	☒
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☐	☒
Driver's License/State Identification Number	☒	☐
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☐	☒
Criminal Information	☒	☐
Military Status and/or Records	☐	☒
Investigation Report or Database	☒	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒	☐
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: System User Information)	☒	☐

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

Data Source	Description of Information Provided by Source
ViSION (FIAT)[7]	ViSION (FIAT) provides PII data (full name) and non-PII data (user ID, work location, employment status, bank location) to BIDS for people matching a BIDS individual's first

[7] To learn more about ViSION, visit www.fdic.gov/privacy.

	and last name. ViSION (FIAT) also provides PII data (full name) and non-PII data (user ID) for FDIC Case Managers.
Structured Information Management System (SIMS)[8]	Listing of States of USA and all the Countries in the world.
Active Directory (AD)	BIDS uses the AD to pull a list of approvers and Case Managers from the BIDS AD groups to authenticate a BIDS user's login and password. For each user, BIDS retrieves the full name, office phone number and email address.
Corporate Reference Database (CRD)	List of addresses and work phone numbers of FDIC Supervisory Areas

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

All FDIC information systems must achieve an Authority to Operate (ATO) via the Assessment and Authorization process that aligns with the Risk Management Framework. Information systems that process background investigation information have been granted ATO or are in the process to achieve ATO. The ATO for each FDIC system is periodically reviewed as part of the FDIC Ongoing Authorization Process.

Section 2.0: Transparency

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

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

Through the conduct, evaluation and review of PIAs 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 SORN(s) apply to the system or project: FDIC 30-64-0002, Financial Institution Investigative and Enforcement Records System of Records, which covers (1) individuals who participate or have participated in the conduct of or who are or were connected with financial institutions, such as directors, officers, employees, and customers, and who have been named in suspicious activity reports or administrative enforcement orders or agreements. Financial institutions include banks, savings and loan associations, credit unions, other similar institutions, and their affiliates whether or not federally insured and whether or not established or proposed; and (2) individuals, such as directors, officers, employees, controlling shareholders, or persons who are the subject of background checks designed to uncover criminal activities bearing on the individual's fitness to be a director, officer, employee, or controlling shareholder.

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

No, the system is not being modified at this time. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

2.4 If a Privacy Act Statement is required, how is the Privacy Act Statement provided to individuals before collecting their PII? (The Privacy Act Statement provides formal notice to

[8] To learn more about SIMS, please see the FDIC Contact and Demographic Information PIA available at www.fdic.gov/privacy.

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.

A Privacy Act Statement is provided to the applicant in the application documents (detailed in Section 1) that are completed by the applicant. 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). See https://www.fdic.gov/policies/privacy/index.html.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There are no identifiable privacy risks related to transparency for the RMS's Background Investigation Process.

Mitigation: No mitigation actions are recommended.

Section 3.0: Access and Amendment

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

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

For information received directly from the applicant: The applicant provides their information to RMS (typically in hardcopy format) as part of the application process described in Section 1. An authorized RMS user manually enters the applicant's information into BIDS and uploads any applicable reports and/or documents as attachments to the BI case in BIDS. If any information is missing, the FDIC Case Manager contacts the individual to obtain the information necessary to conduct the BI.

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.

For information received from external entities/government agencies: Authorized RMS users enter appropriate information and upload any applicable reports and/or documents as attachments to the BI case in BIDS received from other government agencies and external entities, such as the results of background name checks, fingerprint checks, credit checks, and public record searches conducted on subjects. The FDIC does not have the ability to implement procedures for individual access and amendment in such cases. Individuals should contact these external entities and government agencies directly for access to and amendment of their personal information.

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

For information received directly from the applicant: The applicant provides their information to RMS (typically in hardcopy format) as part of the application process described in Section 1. An authorized RMS user manually enters the applicant's information into BIDS and uploads any applicable reports and/or documents as attachments to the BI case in BIDS. If any information is missing, the FDIC Case Manager contacts the individual to obtain the information necessary to conduct the BI.

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.

For information received from external entities/government agencies: Authorized RMS users enter appropriate information and upload any applicable reports and/or documents as attachments to the BI case in BIDS received from other government agencies and external entities into BIDS, such as the results of background name checks, fingerprint checks, credit checks, and public record searches conducted on subjects. FDIC relies upon the external entities and agencies that provided the information to ensure that the information is correct. Individuals should contact these external entities and agencies directly to correct any erroneous or inaccurate information.

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

For information received directly from the applicant: The applicant completes and submits their information to RMS (typically in hardcopy format) as part of the application process described in Section 1. An authorized RMS user manually enters the applicant's information into BIDS and uploads any applicable reports and/or documents as attachments to the BI case in BIDS. If any information is missing, the FDIC Case Manager contacts the individual to obtain the information necessary to conduct the BI.

Additionally, the FDIC has a process for disseminating corrections or amendments of collected PII to other authorized users, the procedures for which are published in the SORN(s) listed in Section 10.4 of this PIA. This is in accordance with the Privacy Act and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: Authorized RMS users manually enter or upload into BIDS background and credit information received from external business entities and other government agencies, such as the results of background name checks, fingerprint checks, credit checks, and public record searches conducted on subjects.

Mitigation: The FDIC relies upon the entities and agencies that collected the PII to ensure that the PII is correct. Individuals may contact the external entities and agencies directly to access and amend PII. The external entities and agencies that provide the background and credit information for use in BIDS have a vested interest in ensuring that the information they provide, including any PII, is correct to preclude compliance issues with Federal mandates, such as the Fair Credit Reporting Act. No additional mitigation actions are recommended.

Section 4.0: Accountability

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

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

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

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy and guidance. This includes the Privacy Act of 1974, 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). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system. The Privacy Program's goal is to have PTAs in place for all IT systems or collections with 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. PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/policies/privacy/index.html.

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

Contractors have been the main source for system design and construction tasks. Contractors will support the maintenance of the system, but will not have access to the production environment.

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

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

Yes, a confidentiality agreement has been completed and signed for contractors who work on the information system or project. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

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

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

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

The FDIC Privacy 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. Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program 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; and regular reporting to the SAOP, the CISO, and the Information Security Manager's Council.

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

BIDS uses the Active Directory (AD) to pull a list of approvers and Case Managers from the BIDS AD groups to authenticate a BIDS user's login and password. For each user, BIDS retrieves the full name, office phone number and email address.

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 12 C.F.R. § 310. 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 12 C.F.R. § 310.

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 12 C.F.R. § 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to accountability for RMS's Background Investigation Process

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws and regulations:

- The FDIC in considering approval of Federal Deposit Insurance Applications is required by Section 5(ad) of the Federal Deposit Insurance Act (FDI Act) (12 U.S.C. 1815(a)(4) to consider certain statutory factors under Section 6 of the FDI Act (12 U.S.C. 1816), including the general character and fitness of management of the institution, its capital adequacy, and risk to the Deposit Insurance Fund. The FDIC is also required to conduct, investigate, and independently verify the accuracy and completeness of information submitted by persons named in Change in Control Notices under Section 7(j) of the FDI Act (12 U.S.C. 1817(j)). The FDIC uses background investigation information as part of its evaluation of the competence, experience, integrity, and financial ability of individuals involved in the organization, management, or control of institutions for which a Federal Deposit Insurance Application is submitted, or each person named in a Change in Control Notice.

- Under Section 19 of the FDI Act (12 U.S.C. 1829), any person convicted of any criminal offense involving dishonesty, breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with the prosecution of such offense, may not become an institution-affiliated party of an insured depository institution; own or control, directly or indirectly, any insured depository institution; or otherwise participate, directly or indirectly, in the conduct of the affairs of any insured depository institution without the prior written consent of the FDIC. The FDIC uses background investigation information in connection with applications subject to Section 19.

- Section 32 of the FDI Act (12 U.S.C. 1831i) also requires an insured depository institution to notify the FDIC of the proposed addition of an individual to an insured state bank or state savings association's board of directors or senior management at least 30 days before such addition if the insured state bank or state savings association fails to meet minimum capital requirements; is troubled; or the FDIC determines, in connection with its review of a capital restoration plan required under Section 38 of the FDI Act (12 U.S.C. 1831i) or otherwise that such prior notice is appropriate. The FDIC is required to disapprove a Section 32 Notice if the FDIC determines that the competence, experience, character, or integrity of the individual involved indicates that it would not be in the best interest of the depositors of the institution

or public if the individual is permitted to be employed by, or associated with, the insured state bank or state savings association. The FDIC also uses background investigation information to determine whether grounds exist for a Section 32 Notice to be disapproved.

- Sections 5, 6, 7(j), 19, and 32 of the FDI Act require FDIC action as stated above and background investigation information is essential to the performance of the FDIC's statutory responsibilities. This information is also covered by Part 309 of the FDIC's regulations (12 C.F.R. Part 309), which safeguard confidential information. For all background investigations conducted by the FDIC, the subject signs a consent for the background investigation to be performed as part of the Federal Deposit Insurance Application, Notice of Acquisition of Control, Section 19 Application, and Section 32 Notice.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority for RMS's Background Investigation Process.

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?

BIDS only collects the minimum PII elements needed to accomplish authorized tasks. BIDS only collects PII that is directly relevant and necessary to accomplish specified purpose(s). BIDS does not duplicate files containing PII and uses the minimum elements necessary for legally authorized purposes.

Additionally, through the conduct, evaluation and review of privacy artifacts,[9] 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?

BIDS only collects the minimum PII elements needed to accomplish authorized tasks. BIDS only collects PII that is directly relevant and necessary to accomplish specified purpose(s). BIDS does not duplicate files containing PII and uses the minimum elements necessary for legally authorized purposes.

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

6.3 How often does the information system or project evaluate the PII 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?

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

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

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

The following is the approved retention schedule for BIDS:

Unclassified hardcopy and electronically retrieved background investigation results are retained for one (1) year after the data has been incorporated into the system and verified. All classified hardcopy background investigation results are retained for thirty (30) years after the close of the investigation.

Additionally, the FDIC third-party fingerprinting vendor maintains the record of the applicant's criminal history check on their secure website. Per FDIC requirement, the vendor is to destroy each record as soon as it has been retrieved by the FDIC. In addition, the FBI requires the vendor to maintain an activity log that consists of a simple chronology of who was fingerprinted and when. The log contains only of the name of the individual fingerprinted. No other PII is included.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with NARA guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

Lastly, 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 management has approved a waiver, and appropriate controls have been put in place.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: More information may be collected than is necessary to complete a background investigation.

Mitigation: FDIC limits the scope of information collected in BIDS to the amount of data necessary to complete a background investigation. Although the system stores PII provided in the application, this information is captured only where it is relevant to the investigation. Any PII identified by FDIC staff as not necessary to complete the investigation is redacted prior to input into BIDS or deleted from BIDS upon discovery.

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.

Authorized RMS users review the applicant's information into BIDS to ensure accuracy and completeness. If any information is inaccurate or missing, an FDIC case manager contacts the individual to obtain the correct information.

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?

RMS collects PII directly from individuals (subjects of investigations) for use in BIDS. The FDIC reviews privacy artifacts to ensure each collection of PII is directly from the individual to the greatest extent practicable.

RMS also receives information from external entities and other government agencies, which authorized RMS users manually input into the system. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information in such cases. Individuals should contact these entities and government agencies directly to correct any erroneous or inaccurate information.

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 Information Security Officer validates the configuration of administrative and technical controls for the system or project based on the FIPS 199 determination.

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

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: Background and credit information received from other government agencies and external entities may be inaccurate.

Mitigation: The external entities and agencies that provide the background and credit information for use in BIDS have a vested interest in ensuring that the information they provide, including any PII, is correct to preclude compliance issues with Federal mandates, such as the Fair Credit Reporting Act. Individuals should contact these external entities and government agencies directly to correct their personal information. No additional mitigation actions are recommended.

Privacy Risk: Conflicting information received from government agencies and external entities may have adverse effect on suitability status of an applicant.

Mitigation: FDIC case managers check and cross reference the information received from other government agencies and external entities to identify any discrepancies in the information. If during the review of this information FDIC staff notices discrepancies between two sources, and it requires further clarification, case managers will notify their Section Chief. The Section Chief will determine whether notification to the applicant and requesting supporting or clarifying documentation is warranted.

Privacy Risk: FDIC employees rather than the individuals themselves perform data entry of BI subjects' information and this may result in inaccurate information.

Mitigation: FDIC case managers verify the accuracy of the information at the time of collection. Case managers correct and update information if they become aware they entered inaccurate information.

Section 8.0: Individual Participation

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

8.1 Explain how the information system or project provides means, 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 individuals authorizes the collection of the information provided. Additionally, this PIA and the SORN(s) listed in 2.2 serve as notice of the information collection. Lastly, the FDIC Privacy Program also reviews PIAs to ensure that PII collection is conducted with the consent of the individual to the greatest extent practicable.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

When the FDIC collects information directly from individuals, it describes in the Privacy Act Statement and other privacy notices the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of PII.

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

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

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

The project or system only uses PII for the purposes listed in Section 9.1. This PIA and the SORN(s) listed in 2.2 serve as notice for all uses of the PII. Additionally, the FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

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

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

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There are no identifiable privacy risks related to individual participation for RMS's Background Investigation Process.

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 Corporation conducts background investigations in connection with applications and notices submitted to the FDIC, such as applications for federal deposit insurance, notices of acquisition of control, applications subject to Section 19 of the Federal Deposit Insurance (FDI) Act, and notices subject to Section 32 of the FDI Act.

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

Through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information" with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

RMS Assistant Regional Directors (ARDs) are responsible for managing who has access to BIDS in their regions and are required to manage that access in accordance with current FDIC privacy and security policies/procedures and the knowledge that BIDS contains sensitive PII and requires the highest level of security/privacy possible within the FDIC.

Access to BIDS is facilitated, tracked, and managed using the Corporation's Access Request and Certification System (ARCS). Management approval is required for access to the BIDS application, which is role-based according to job function, and contingent on a business need to know. Those individuals identified under the heading of 'Approved BIDS Users' will upon beginning their position be notified that among their responsibilities will be submitting an ARCS request for BIDS access. Other

individuals may obtain access to BIDS by submitting an ARCS request, based on their job responsibility to conduct background investigations.

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.

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

RMS Assistant Regional Directors (ARDs) are responsible for managing who has access to BIDS in their regions and need to manage that access in accordance with current FDIC privacy and security policies/procedures and the knowledge that BIDS contains sensitive PII and requires the highest level of privacy/security possible within the FDIC.

All access is granted on a need-to-know basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

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

☐ No
☒ Yes Explain. BIDS pulls data from SIMS (lists of countries and states). BIDS also pulls from CRD the list and addresses and phone numbers of FDIC Supervisory Areas. Additionally, BIDS queries the FIAT database (part of ViSION) and pulls matching records (the record ID and address) for people matching a BIDS individual's first name and last name.

BIDS relies on the Active Directory (AD) to authenticate a user's login and password, upon a login request. Additionally, BIDS uses the AD to pull the list of approvers and Case Managers from the BIDS AD Groups. For each one of these users, BIDS retrieves the full name, office phone number and email address.

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

No, FDIC does not aggregate data to make programmatic level decisions.

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

The Corporation shares PII only for 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.

BIDS shares PII externally with the following organizations in order to obtain background investigation information from these external sources:

Data Destination	Description of Shared Data
Federal Bureau of Investigation (FBI)	The FDIC uses the FBI National Name Check Program (NNCP) to perform background investigations. This includes Name, SSN,

Data Destination	Description of Shared Data
	Date of Birth, Place of Birth, Alias Name, Home Address, Residential History, Employment History, and Business Affiliations and Addresses. The FDIC and FBI have a memorandum of agreement for the FBI background investigation services that is renewed annually.
Immigration and Customs Enforcement Agency (ICE)	Name Check forms (FDIC Form 6700/01) are printed by authorized Headquarter BIDS users and delivered via secure email with password protected PDF documents to ICE to perform background investigations. This includes Name, SSN, Date of Birth, Place of Birth, Maiden Name, Alias Name, Spouse Name, Home Address, Residential History, Employment History, Business Affiliations and Addresses, Date and Place of Prior Convictions, Father's Name, Mother's Maiden Name, Passport Number, (Asian) Identification Number, Chinese Commercial Code Number, and Country of Citizenship.
LexisNexis	Library Publications Order Form (FDIC 3020/11) is electronically delivered by BIDS to the FDIC Library to perform background investigations. This includes Name, Home Address, SSN, and Date of Birth. The FDIC Library has an agreement with LexisNexis.
Dun and Bradstreet/Experian; Fitch, Moody's, Standard's & Poor's (S&P)	Library Publications Order Form (FDIC 3020/11) is electronically delivered by BIDS to the FDIC Library to perform background investigations. This includes Business Name and Business Address. The FDIC Library has an agreement with Dun and Bradstreet/Experian.
Credit Bureau (Equifax)	Consumer Credit Report Request Form (FDIC 3020/03B) is electronically delivered by BIDS to the FDIC Library. The FDIC Library has a contract with Equifax.

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: FDIC's third party fingerprinting vendor may use BI subjects' data for unauthorized purposes.

Mitigation: FDIC's third-party fingerprinting vendor is an authorized channeler on behalf of the Federal Bureau of Investigation (FBI) and as such, undergoes rigorous oversight by the FBI. The FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard), which must be adhered to by the vendor, forbids the use of BI subject's data for commercial purposes. Additionally, FDIC's third-party fingerprinting vendor is bound contractually to use BI subjects' data only for the collection and transmission of fingerprints to the FBI.

Section 10.0: Security

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

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

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

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

The FDIC Privacy Program updates the 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 related to security for RMS's Background Investigation Process.

Mitigation: No mitigation actions are recommended.