FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Virtual Supervisory Information on the Net (ViSION)

OCISO

July 4, 2021

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

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

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) is an independent agency of the U.S. government that protects the funds depositors place in banks and savings associations, also known as "insured banks" or "insured depository institutions." Within FDIC, the Division of Risk Management Supervision (RMS) and Division of Depositor and Consumer Protection (DCP) have primary responsibility for examining and supervising insured banks to ensure that they operate in a safe and sound manner. The supervisory role includes reviewing, investigating and processing applications submitted by insured banks, such as an application to add a new insured bank, establish a new or foreign bank branch, or a merge with another bank. The examination role includes the periodic review of the insured bank's financial health and operations to ensure compliance with a wide range of legislative and regulatory mandates governing the banking industry.

Virtual Supervisory Information On the Net (ViSION) is a web-based system used primarily by RMS and DCP staff to assess risks to the deposit insurance fund associated with the operations of insured depository institutions and their affiliates and servicers, such as data processing servicers. Specifically, ViSION provides RMS and DCP Washington, Regional, and Field Office staff with an automated ability to track and document reports on financial institution supervision, including: applications, bank case management, safety and soundness examinations, information technology examinations, trust department examinations, offsite monitoring, management reporting, affiliated organizations, enforcement actions, and risk assessment tools. Federal and state banking agency staff also have the ability to view information in ViSION in support of their regulatory responsibilities.

This PIA is being updated to reflect a new records retention schedule that has been established for ViSION.

In support of the aforementioned RMS/DCP business functions, ViSION includes several distinct modules that collect and maintain information about insured institutions. This privacy impact assessment (PIA) is focused on ViSION's "Formal and Informal Action Tracking" (FIAT) module, as it is the only ViSION module that contains personally identifiable information (PII) stemming from FDIC enforcement actions that may be taken against individual members of the public under Section 8 of the Federal Deposit Insurance Act (FDI Act). FIAT also is used to generate various reports that can be used by the Washington, Regional and Field offices. Specific actions that may affect individuals are:

- **Section 8(e) Removal**: FDIC is authorized to issue orders to remove an institution-affiliated party (IAP), such as a director, officer, employee, controlling stockholder, or independent contractor from office, whenever FDIC or the appropriate Federal banking agency determines that the party has violated, for example, any law or regulation, engaged or participated in any unsafe or unsound practices and breaches of fiduciary duty, and caused the insured depository institution to suffer a financial loss or other damage. Section 8(e) further allows the FDIC to prohibit the party from participating in the conduct of the affairs of any insured depository institution and to assess civil and money penalties.

- **Section 10(c) Investigation Report**: FDIC is authorized to conduct a formal investigation to obtain needed information or evidence.

[1] www.fdic.gov/privacy

- **Section 8(g) Suspension/Prohibition (Criminal Proceedings)**: FDIC is authorized to suspend or prohibit an individual from participating in the conduct of affairs of any depository institution whenever an individual is subject to any information, indictment, or complaint involving certain crimes.

- **Other:** Other formal actions that can be taken against individuals include 8(i) civil money penalties (CMPs), 8(b) restitution, 8(b) personal cease-and-desist (PC&D), and prompt corrective action (PCA) dismissals.

FDIC-insured financial institutions provide records and information to FDIC about potential or confirmed Section 8 violations involving individuals. They also provide FDIC with copies of Suspicious Activity Reports (SARs) filed with the U.S. Department of Treasury Financial Crime Enforcement Network (FinCEN). A SAR, and any information that would reveal the existence of a SAR, is confidential. Hard copies of SARs are not scanned and stored in FIAT, but are maintained in the FDIC's Regional Document Distribution and Imaging System (RADD), which provides an electronic document imaging, distribution, and storage system for financial institution correspondence and final examination documents. The unauthorized disclosure of a SAR, including notifying individuals who are subjects of SARs during the investigation phase, is a violation of federal law. Both civil and criminal penalties may be imposed for SAR disclosure violations.

Most Section 8(e), CMP, restitution and PC&D enforcement actions pursued by FDIC originate from a SAR. Providing notice to individuals who are subjects of SARs or other ongoing investigations is a violation of federal law, prohibited by FDIC policy, and jeopardizes FDIC's ability to fulfill its statutory duties under the FDI Act. Therefore, FDIC does not provide notice and consent opportunities to respondents during the investigation phase of a case. Once a determination is made by FDIC that an enforcement action will be taken against an institution or IAP (also referred to as a "respondent" in this PIA), FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond. An institution or IAP may elect to stipulate to the FDIC's issuance of an order, thereby waiving the right to an administrative enforcement hearing and all rights to appeal. If the institution or IAP declines to stipulate, the FDIC issues a notice of charges, which starts the formal administrative enforcement proceeding. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing.

The determination to pursue an enforcement action against a bank or individual is initiated by RMS in coordination with FDIC's Legal Division. In advance of taking a formal enforcement action, FDIC notifies and coordinates with other impacted Federal Banking Agencies (FBAs) as applicable and in accord with the "Policy Statement on Interagency Notification of Formal Enforcement Actions" (June 2018) jointly issued by the FBAs. If it is determined that one or more other FBAs have an interest in the enforcement action, the FBA proposing the enforcement action is responsible for notifying the other FBA(s) prior to providing written notification to the financial institution or IAP. The scope of the information shared by the FBAs depends on the gravity of the interests of each FBA and is determined on a case-by-case basis by the FBA initiating the notification. At minimum, however, the information shared must be sufficient to allow the other FBA(s) to take necessary action in examining or investigating the financial institution or IAP over which they have jurisdiction. If two or more FBAs consider bringing a complementary action (e.g., action involving a bank and its parent holding company), those FBAs coordinate the preparation, processing, presentation, potential penalties, service, and follow-up of the enforcement action.

Outcomes of a formal enforcement action may include, for example, termination of an institution's federal deposit insurance; removal, prohibition, or suspension from banking; restitution; and civil money penalties. Procedures for removing IAPs and other enforcement actions are documented in the Formal Administrative Actions section of the FDIC's Manual of Examination Policies and within the Removal, Prohibition, and Suspension Actions section of the FDIC's Formal and Informal Actions Manual. All orders (stipulations and notices) issued under Section 8 of the FDI Act are required to be made public. Accordingly, the FDIC publishes, on a monthly basis, all final administrative enforcement orders against insured depository institutions and institution-affiliated parties issued during the prior month. The orders are made available on FDIC's public-facing website: www.fdic.gov.

The FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions are voluntary commitments made by an institution's Board of Directors or an IAP. Informal actions are not legally enforceable and are not publicly disclosed or published. Informal actions are used when discussions with bank management or findings and recommendations in the Report of Examination will not, by themselves, accomplish the FDIC's goal of attaining timely corrective action from management. However, informal actions generally are not appropriate when an institution's problems present serious concerns and risks, in which case a formal action should be pursued. The informal actions most commonly used by the FDIC are Bank Board Resolutions and Memoranda of Understanding. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

PRIVACY RISK SUMMARY

In conducting this PIA, we 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:

- Individual Participation
- Transparency
- Minimization

Individual Participation and Transparency Risk: ViSION contains third-party data from financial institutions and government agencies, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection and use of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC, and they are not provided with an opportunity to consent to or opt-out of FDIC's collection and use of their information.

Mitigation: In cases where PII is received from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. In addition, individuals are not provided with an opportunity to decline to provide their PII, as the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Further, SARs, including the PII contained therein, and any information that would reveal the existence of a SAR, are strictly confidential. Notifying individuals who are subjects of SARs during the investigation stage, or other ongoing investigations, is a violation of federal law and FDIC policy.

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 ViSION FIAT module provides a tracking mechanism for proposed and formal enforcement actions involving banks and individuals, such as a bank employee or officer. An individual is identified in FIAT as a "respondent." Each action record contains, but is not limited to, the following information related to the respondent:

- Full name
- Age/birth year
- Home address

- Net worth
- Financial institution identification number
- Basis, facts and actions related to FDIC's investigation of the case, including violation type
- Dates of FDIC legal opinions and federal/state banking agency notifications
- Dates of FDIC correspondence with the respondent
- Civil Money Penalty data (e.g., restitution amount, payments made by respondent)
- ViSION/FIAT action record number [i.e., System Identification (SYSID)]

ViSION action records could contain various types of PII, as indicated in the following table.

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☐	☒
Place of Birth	☐	☒
Social Security Number	☐	☒
Employment Status, History or Information	☐	☒
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s)	☐	☒
Email Address	☐	☒
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☒	☐
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: age/birth year, not date of birth)	☒	☐

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

The following are sources of information for the ViSION FIAT module. (Please note that hard copies of documents are not scanned and stored in FIAT, but rather are maintained in RADD.)

Data Source	Description of Information Provided by Source
FDIC-Insured Banks	FDIC-insured banks provide records and information to FDIC Field Office bank examiners about potential or confirmed Section 8 violations involving individuals. Banks also provide FDIC's Regional Offices with copies of Suspicious Activity Reports (SARs) filed with the U.S. Department of Treasury Financial Crime Enforcement Network (FinCEN).
FDIC Field Office Bank Examiners	FDIC Field Office Bank Examiners provide information about potential or confirmed violations to the FDIC Field Supervisor and Regional Case Manager based on issues found during the bank examination or on site. For example, for Section 8(e) cases, examiners prepare a recommendation memorandum clearly explaining the facts of the case and support for a recommended action. They also assist the Regional

Data Source	Description of Information Provided by Source
	Office staff with outreach to the FDIC Regional Counsel and may meet directly with the individual who may be subject to an action.
FDIC Field Supervisors	FDIC Field Supervisors review the documentation, provide further information, make the determination to proceed with the enforcement action, and coordinate the case with the FDIC Regional Case Manager.
FDIC Regional Case Managers	FDIC Regional Case Managers create, populate and manage cases in FIAT based on the supporting information and documentation provided by the FDIC Field Office. Case Managers enter a summary of the Field Office Bank Examiner recommendation memorandum and other comments as the action is developed. They consult with the Regional Counsel and the Regional Director in the course of making a determination about taking an action against an individual and ensure that the FIAT record is complete and updated in a timely manner. If a decision to pursue an action is made, they will notify other Federal banking agencies and the appropriate State Authority of the possible issuance of an action against an individual.
FDIC Legal Division Regional Counsel and Washington Office Staff	FDIC Legal Division Regional Counsel and Washington Office Staff advise on case matters and provide written legal opinions used by the Regional Case Manager.
FDIC Washington Office Reviewer	After receiving recommendation memorandum and other documents from the Regional Office, the FDIC Washington Office Reviewer enters the receipt of the case into FIAT and notifies the Washington Legal Office of the matter.
U.S. Department of Justice	The U.S. Department of Justice provides information about actions taken about an individual by the U.S. Attorney's Office or Federal Bureau of Investigation.
Federal Banking Agencies	FDIC tracks examination and supervisory activities of other banking agencies. Other Federal Banking Agencies, such as the Federal Reserve Board (FRB) and Office of the Comptroller of the Currency (OCC), provide electronic or hard copies of their Reports of Examination to RMS and DCP. A summary of the reports is manually entered into ViSION by authorized RMS/DCP personnel. In addition, the FRB National Information Center (NIC) provides structure information (i.e., bank holding company and affiliate data) about banking organizations for use in case administration.
Federal Financial Institutions Examination Council (FFIEC)	FFIEC provides "Reports of Condition and Income" (Call Report) and "Uniform Bank Performance Reports" (UBPR) data for use in supervision of insured institutions. The data contains financial information, statistics and peer group analysis about financial institutions.
State Banking Departments	State Banking Departments provide ViSION with data similar to that of the Federal Banking Agencies. See above for details.

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

The ATO was issued on December 20, 2013 and 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 ViSION FIAT module operates under the following FDIC Privacy Act System of Records Notice: "30–64–0002, Financial Institution Investigative and Enforcement Records."

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

Not applicable. 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 individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.) Explain.

The FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.1, "FDIC Forms Management Program." However, in instances where FDIC receives information, including PII, from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. In addition, individuals are not provided with an opportunity to decline to provide their PII, as the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Providing notice to respondents who are subjects of Suspicious Activity Reports (SARs) or ongoing investigations is a violation of law, prohibited by FDIC policy, and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. Therefore, FDIC does not provide advance notice or consent opportunities to respondents during the investigation of a case. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond. As the case proceeds, the name of and action against the individual will be made public when FDIC issues certain notices (e.g., *Notice of Intention to Prohibit From Further Participation, Findings of Fact, Conclusions of Law*, and *Notice of Hearing and Order of Removal From Office and Prohibition From Further Participation*).

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, and the Privacy Program. See https://www.fdic.gov/policies/privacy/index.html. In addition, Section 8 of the FDI Act requires FDIC to publicly disclose certain orders and agreements. Accordingly, the FDIC publishes, on a monthly basis, all final administrative enforcement orders against banks and individuals issued during the prior month. The orders are made available on FDIC's public-facing website: www.fdic.gov.

Prior to publicizing the aforementioned orders and agreements, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond. An institution or IAP may elect to stipulate to the FDIC's issuance of an order, thereby waiving the right to an administrative enforcement hearing and all rights to appeal. If the institution or IAP declines to stipulate, the FDIC issues a notice of charges, which starts the formal administrative enforcement proceeding. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: ViSION contains third-party data from financial institutions and government agencies, some of which could include PII. In such cases, the FDIC does not have the ability to provide notice to these individuals prior to the collection and use of their PII. Therefore, individuals may not be aware that their data has been provided to FDIC.

Mitigation: In instances where information, including PII, is received from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collect the information. In addition, individuals are not provided with an opportunity to decline to provide their PII, as the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Providing notice to respondents who are subjects of Suspicious Activity Reports (SARs) or ongoing investigations is a violation of law, prohibited by FDIC policy, and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. Therefore, FDIC does not provide notice and consent opportunities to respondents during the investigation of a case. Once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond. As the case proceeds, the name of and action against the individual will be made public when FDIC issues certain notices (e.g., *Notice of Intention to Prohibit From Further Participation, Findings of Fact, Conclusions of Law*, and *Notice of Hearing and Order of Removal From Office and Prohibition From Further Participation*). Section 8 of the FDI Act requires FDIC to publicly disclose certain orders and agreements. Accordingly, the FDIC publishes, on a monthly basis, all final administrative enforcement orders against banks and individuals issued during the prior month. The orders are made available on FDIC's public-facing website: www.fdic.gov.

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?

Once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond. An institution or IAP may elect to stipulate to the FDIC's issuance of an order, thereby waiving the right to an administrative enforcement hearing and all rights to appeal. If the institution or IAP declines to stipulate, the FDIC issues a notice of charges, which starts the formal administrative enforcement proceeding. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions may be taken based on the findings of examinations, visitations, target reviews, offsite reviews, etc. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

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

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

Once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond, including an opportunity to correct any inaccurate or erroneous information.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions may be taken based on the findings of examinations, visitations, target reviews, offsite reviews, etc. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

In addition, the FDIC allows individuals to correct or amend PII maintained by the FDIC, the procedures for which are published in its SORNs, available on the FDIC public-facing website.

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

Once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and grants them an opportunity to respond, including an opportunity to correct any inaccurate or erroneous information. The individual may respond in writing and/or as part of a hearing, as applicable. The individual may elect to stipulate to the FDIC's issuance of an order, thereby waiving the right to an administrative enforcement hearing and all rights to appeal. If the individual declines to stipulate, the FDIC issues a notice of charges, which starts the formal administrative enforcement proceeding. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing to be adjudicated by a judge.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions may be taken based on the findings of examinations, visitations, target reviews, offsite reviews, etc. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

In addition, 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 listed in Section 2.2 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: There are no identifiable privacy risks related to access and amendment, as FDIC provides individuals the ability to access and amend their PII. ViSION's PIA is publicly available at https://www.fdic.gov/policies/privacy/index.html.

Mitigation: No 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 PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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

Privacy risks posed by ViSION are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, https://www.fdic.gov/policies/privacy/index.html.

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

Contractors are employed by FDIC's Division of Information Technology to provide system design and maintenance support. Programmers are restricted to the development and quality assurance environment using test data and do not have access to operate in 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?

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

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

The ViSION Program Manager/Data Owner is responsible for management and decision authority over a specific area of corporate data. The ViSION Program Manager/Data Owner and Information Security Manager serve as the sources of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing. Although they share this data responsibility, all system users are responsible for abiding by FDIC data protection rules that are outlined in Corporate Information Security and Privacy Awareness Training and/or ViSION specific security training and rules of behavior to ensure proper use of the data.

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

All users who have system access must complete required ViSION security awareness training that covers the system rules of behavior. These rules, in addition to FDIC Corporate policies, establish user responsibility and accountability. Annual role-based training is taken by users, including external users.

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 (SAOP) Report, as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the Chief Information Security Officer (CISO); 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?

The ViSION FIAT module includes automated checks to ensure that the data entered by RMS and DCP Regional Case Managers is complete. Also, controls are in place and tested at each system release and every three years in the security testing and evaluation process to ensure data completeness.

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 records under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1 Disclosures are tracked and managed using FOIAXpress.

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: There are no identifiable privacy risks related to accountability, as the FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices and is compliant with applicable privacy laws.

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).

Section 8 of the Federal Deposit Insurance Act (FDI Act). Further information about Section 8 of the Federal Deposit Insurance Act may be found at: http://www.fdic.gov/regulations/laws/rules/1000-900.html.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There is a potential privacy risk related to authority because FDIC could collect PII in excess of its legal authority under Section 8 of the FDI Act.

Mitigation: Section 8 of the FDI Act provides the FDIC with broad enforcement powers, including the authority to take various formal and informal enforcement actions, such as issuing cease and desist orders and removing institution-affiliated parties or prohibiting their participation in bank affairs. These activities necessitate the collection of sensitive data, including PII, pertaining to IAPs. Parts 303 and 308 of the FDIC Rules and Regulations detail various rules and procedures relating to various types of enforcement actions, and FDIC has implemented policies, procedures and training to ensure that FDIC examiners thoroughly understand the scope and boundaries of their authority under Section 8 and only collect PII that is relevant and necessary to fulfilling FDIC's statutory duties. No additional 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?

Data related to Section 8 enforcement actions is collected by RMS and DCP staff as a result of their supervisory examination authority under the FDI Act. ViSION uses an access control system to restrict user view and edit rights to the minimum necessary to perform daily work tasks, based on predefined roles and restrictions on FDIC division and regulatory authority. This includes limiting access to the FIAT module to only those authorized users with a need-to-know.

Additionally, through the conduct, evaluation and review of privacy artifacts,[2] 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?

Data related to Section 8 enforcement actions is collected by RMS and DCP staff as a result of their supervisory examination authority under the FDI Act. RMS and DCP staff collect and review records and information obtained directly from insured banks. For example, individuals subject to an investigation related to a Section 8(e) removal enforcement actions generally do not provide personal information directly to the FDIC and, therefore, do not have an opportunity to opt-out.

Additionally, 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.

The retention periods and disposition procedures for records in ViSION are covered by the following FDIC records retention schedule: Electronic Information Systems (EIS) 1062, Virtual Supervisory Information on the Net. Accordingly, records are maintained in ViSION for thirty (30) years after the close of the examination. Summary Analysis of Examination Reports (SAERs) are copied to RADD upon completion of the examination and maintained permanently.

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. Additionally, detailed guidance is provided to users in the Privacy Section-issued guide titled "Protecting Sensitive Information in Your Work Area."

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?

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

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

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond what is necessary.

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

Section 7.0: Data Quality and Integrity

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

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

FDIC Case Managers review ViSION FIAT records to ensure that information is complete, accurate and updated in a timely manner. In addition, the ViSION FIAT module includes automated checks to ensure that the data entered by RMS and DCP Regional Case Managers is complete. Further, controls are in place and tested at each system release and every three years in the security testing and evaluation process to ensure data completeness and reliability. 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?

Data related to Section 8 enforcement actions is collected by RMS and DCP staff as a result of their supervisory examination authority under the FDI Act. RMS and DCP staff collects and reviews records and information obtained directly from insured banks. Individuals subject to an investigation related to Section 8(e) removal enforcement actions generally do not provide personal information directly to the FDIC.

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 PIAs and SORNs 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 prescribes administrative and technical controls for the system or project based on the FIPS 199 determination.

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

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

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There are no identifiable privacy risks related to data quality and integrity.

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.

RMS and DCP staff collect and review records and information obtained directly from insured banks. Individuals are not provided with an opportunity to decline to provide their PII, as the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Providing notice and consent opportunities to respondents who are subjects of Suspicious Activity Reports or ongoing investigations is a violation of FDIC policy and law and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and provides them with an opportunity to respond. In response to the FDIC's letter that provides the IAP with an opportunity to respond to a proposed civil money penalty or restitution, the IAP may voluntarily provide a personal financial statement, which may contain PII. The FDIC uses the personal financial statement to assess the IAP's financial capacity and ability to pay a civil money penalty or restitution. Some of this information may be entered into ViSION. The formal administrative enforcement proceeding starts when FDIC issues a notice of charges. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing to be adjudicated by a judge.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions may be taken based on the findings of examinations, visitations, target reviews, offsite reviews, etc. Informal actions are

voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

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.

RMS and DCP staff collect and review records and information obtained directly from insured banks. Individuals are not provided with an opportunity to decline to provide their PII because the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Furthermore, providing notice and consent to respondents who are subjects of Suspicious Activity Reports or ongoing investigations is a violation of law and FDIC policy and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and provides them with an opportunity to respond. In response to the FDIC's letter that provides the IAP with an opportunity to respond to a proposed civil money penalty or restitution, the IAP may voluntarily provide a personal financial statement, which may contain PII. The FDIC uses the personal financial statement to assess the IAP's financial capacity and ability to pay a civil money penalty or restitution. Some of this information may be entered into ViSION. Refer to Section 8.1 for additional details.

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.

RMS and DCP staff collect and review records and information obtained directly from insured banks. Individuals are not provided with an opportunity to decline to provide their PII because the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Furthermore, providing notice and consent to respondents who are subjects of Suspicious Activity Reports or ongoing investigations is a violation of law and FDIC policy and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and provides them with an opportunity to respond. In some cases, responses to the FDIC's letter may include an IAP's personal financial statement, which may contain PII. Refer to Section 8.1 for additional details.

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.

RMS and DCP staff collect and review records and information obtained directly from insured banks. Individuals are not provided with an opportunity to decline to provide their PII because the FDIC is required to collect and maintain the PII in order to fulfill its statutory duties under Section 8 of the FDI Act. Furthermore, providing notice and consent to respondents who are subjects of Suspicious Activity Reports or ongoing investigations is a violation of law and FDIC policy and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and provides them with an opportunity to respond. In some cases, responses to the FDIC's letter may include an IAP's personal financial statement, which may contain PII. Refer to Section 8.1 for additional details.

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: In cases where individuals do not provide personal information directly to the FDIC, they may be unaware that the FDIC maintains their PII. Additionally, individuals are generally not provided with an opportunity to consent to or opt out of the FDIC's collection and use of their PII as part of enforcement actions.

Mitigation: In cases where PII is received from financial institutions and government agencies, those entities are responsible for providing any applicable, required notices to the individuals from whom they initially collected the information. In addition, the FDIC is required to collect and maintain the PII in accordance with a legally authorized purpose under Section 8 of the Federal Deposit Insurance Act. Providing notice and consent to respondents who are subjects of Suspicious Activity Reports (SARs) or ongoing investigations is a violation of law and FDIC policy and could jeopardize FDIC's ability to fulfill its statutory duties under Section 8 of the FDI Act. However, once a determination is made by FDIC that an enforcement action will be taken against an individual respondent, FDIC notifies the respondent by letter of the FDIC's intent to take a Section 8 action and provides them with an opportunity to respond. The individual may elect to stipulate to the FDIC's issuance of an order, thereby waiving the right to an administrative enforcement hearing and all rights to appeal. If the individual declines to stipulate, the FDIC issues a notice of charges, which starts the formal administrative enforcement proceeding. The notice is a public document that contains a statement of facts constituting the alleged actionable misconduct and schedules the date and location for an administrative enforcement hearing to be adjudicated by a judge.

FDIC also may use informal procedures in a measured effort to address weak operating practices, deteriorating financial conditions, or actionable misconduct. Informal actions may be taken based on the findings of examinations, visitations, target reviews, offsite reviews, etc. Informal actions are voluntary commitments made by the institution's Board of Directors or an IAP. Informal actions are neither publicly available nor legally enforceable in a federal administrative enforcement proceeding or in a federal or state court. Additionally, although not considered an informal action, the FDIC also may send a supervisory letter to an institution or IAP as a means of communicating a supervisory concern when circumstances do not warrant a formal action.

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 ViSION FIAT module provides a tracking mechanism for proposed and formal enforcement actions involving banks and individuals, such as a bank employee or officer. Refer to Section 9.5 for details on the information systems with which ViSION shares information.

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.

ViSION is used primarily by RMS and DCP staff to assess risks to the deposit insurance fund associated with the operations of insured depository institutions and their affiliates and servicers, such as data processing servicers. Specifically, ViSION provides RMS and DCP Washington, Regional, and Field Office staff with an automated ability to track and document reports on financial institution supervision, including: applications; bank case management, safety and soundness examinations, information technology examinations, trust department examinations, offsite monitoring, management reporting, affiliated organizations, enforcement actions and risk assessment tools.

Federal and state banking agency staff also have the ability to view information in ViSION, in support of their regulatory responsibilities. Users also have the ability to upload attachments. In addition, authorized users in other FDIC Divisions, including the Division of Finance (DOF), Division of Insurance and Research (DIR), Division of Resolutions and Receiverships (DRR) and Office of the Ombudsman (OO), are provided read-only access to ViSION in order to review examination-related information. DOF personnel have access to review bank structural information. DRR uses ViSION to review enforcement actions, but this use is limited.

Authorized Federal Banking Agency (FRB and OCC) and State Banking Department staff have access to ViSION, including the FIAT module, in support of their examination and supervisory mission. A Memorandum of Agreement exists between FDIC and external banking agencies that defines the purpose, use and restrictions on data shared.

ViSION includes several distinct modules supporting RMS and DCP business functions that collect and maintain information on insured institutions. ViSION's FIAT module is the only ViSION module that contains PII stemming from RMS and DCP enforcement actions that may be taken against individual members of the public, under Section 8 of the Federal Deposit Insurance Act (FDI Act).

The ViSION Program Manager/Data Owner is responsible for management and decision authority over a specific area of corporate data. The ViSION Program Manager/Data Owner and Information Security Manager serve as the sources of information for data definition and data protection requirements and are collectively responsible for supporting a corporate-wide view of data sharing. Although they share this data responsibility, all system users are responsible for abiding by FDIC data protection rules that are outlined in the Corporate Information Security and Privacy Awareness Training and/or ViSION-specific security training and rules of behavior to ensure proper use of the data.

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

ViSION users are granted access by specific roles set within the ViSION Security Manager module. All internal and external users who have access to ViSION must have the approval of their Manager/Supervisor and the ViSION Program Manager/Data Owner before access is granted to the system. Additionally, ViSION's functional security limits a user's access to specific functions and regulates a user's ability to update data for a specific function based on job responsibilities and limited to information needed to perform position duties.

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.

The ViSION FIAT module provides a tracking mechanism for proposed and formal enforcement actions involving banks and individuals, such as a bank employee or officer. ViSION shares information with the following FDIC systems:

- **Advanced Legal Information System (ALIS):** The ViSION FIAT module shares enforcement case data with ALIS that includes individual respondent data for the purpose of case tracking.[3]

- **FDIC Division of Resolutions and Receiverships Communication, Capability, Challenge and Control (4C) system:** ViSION shares supervisory data with 4C that does not include FIAT data containing PII on individuals.[4]

In addition, several FDIC systems interface with ViSION, but the data sharing does not involve sensitive *PII* and not all interface with FIAT:

- **Examination Tools Suite (ETS):** provides examination summary data.

- **Structure Information Management System (SIMS)**: provides structure data about financial institutions.

- **Federal Financial Institution Examination Council (FFIEC) Central Data Repository (CDR)**: provides Call Report and UBPR data about financial institutions.

- **Regional Economic Conditions (RECON) system**: provides charts, tables and data concerning economic conditions in the U.S.

- **System of Uniform Reporting of Compliance and CRA Exams (SOURCE)**: provides compliance rating and Community Reinvestment Act (CRA) rating for a financial institution.

- **DSC Hours**: provides bank examiner name and grade level for case management purposes.

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?

Not applicable. There is no data consolidation taking place that results in personally identifiable information not already known in the system. The respondent file in the ViSION FIAT module reflects a consolidation of the known facts, dates and status of the case and investigation.

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.

Yes. Authorized Federal Banking Agencies (FRB, OCC) and State Banking Department staff have access to ViSION, including the FIAT module, in support of their examination and supervisory mission.

A Memorandum of Agreement exists between FDIC and external banking agencies that defines the purpose, use and restrictions on data shared.

[3] A PIA for ALIS is available at https://www.fdic.gov/policies/privacy/assessments.html.
[4] A PIA for the 4C system is available at https://www.fdic.gov/policies/privacy/assessments.html.

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.

FDIC Information Security and Privacy Awareness Training is mandated for all FDIC users of ViSION. In addition, both FDIC and external users (e.g., Federal and state banking regulatory staff) are required to take annual security training specific to ViSION that covers the rules of behavior. Super users (those with read and edit roles) are required to take additional training. Users that do not comply are not granted access until the training is completed. Contractors also must complete the Corporate Information Security and Privacy Awareness Training, which includes Rules of Behavior.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There is a potential privacy risk associated with use limitation because an FDIC employee could exceed his or her authority by using or disclosing sensitive information, including PII, for a purpose not compatible with the original purpose for which the information was collected (e.g., unauthorized disclosure of information contained in a SAR).

Mitigation: Section 8 of the FDI Act provides the FDIC with broad enforcement powers. Specifically, the FDIC has the authority to take various formal and informal enforcement actions, including but not limited to issuing cease and desist orders and removing institution-affiliated parties or prohibiting their participation in bank affairs. Parts 303 and 308 of the FDIC Rules and Regulations detail various rules and procedures relating to various types of enforcement actions, and FDIC has implemented policies, procedures and training to ensure that FDIC examiners thoroughly understand the scope and boundaries of their authority under Section 8. In addition, and as emphasized in FDIC training and policy, there are civil and criminal penalties associated with unauthorized disclosures of SARs. No additional mitigation actions are recommended.

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 Section 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.

Mitigation: No mitigation actions are recommended.