# PRIVACY IMPACT ASSESSMENT

INTRODUCTION

The objective of the Privacy Impact Analysis (PIA) is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing or processing sensitive, personal data that may be considered private. Upon completion of the questionnaire and acquisition of signatures, please return to DIT Information Security Staff located in Virginia Square, Room Number A7032.

| | |
|---|---|
| **Agency:** | **Federal Deposit Insurance Corporation (FDIC)** |
| **System Name:** | **Virtual Supervisory Information On the Net (Formal and Informal Action Tracking module)** |
| **System Acronym:** | **ViSION** |
| **System Owner/Division or Office:** | **Division of Supervision and Consumer Protection (DSC)** |

## A. Information and Privacy

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

## C. System Description

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

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."

FDIC's Division of Supervision and Consumer Protection (DSC) has 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.

The Virtual Supervisory Information On the Net (ViSION) system is a web-based system used primarily by DSC 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 DSC 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.

ViSION includes several distinct modules supporting the above-mentioned DSC business functions that collect and maintain information on insured institutions. This privacy impact assessment 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 DSC enforcement actions that may be taken against individual members of the public, under Section 8 of the Federal Deposit Insurance Act (FDI Act). Specific actions that can affect individuals are:

- **Section 8(e) Removal**: FDIC is authorized to issue orders to remove an "institution-affiliated party," 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.[1]

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

- **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.[2]

- **Section 8(i) Court Enforcement**: FDIC can apply for court enforcement of Section 8 actions including Civil Money Penalties.

The determination to pursue an enforcement action taken against a bank or individual is initiated by DSC in coordination with FDIC's Legal Division. FDIC conducts administrative hearings on removal enforcement cases and all related notices and final orders of enforcement actions are published on www.fdic.gov. Enforcement actions may result in civil and criminal penalties.

For certain cases, such as Section 8(e) enforcement cases, the FDIC will coordinate and consult with the U.S. Attorney's Office and Federal Bureau of Investigation at the U.S. Department of Justice.

## D. Data in the System

1. What personal information about individuals or other information that can personally identify an individual (name, social security number, date of birth, address, etc.) is contained in the system? 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. An individual is identified in FIAT as a "respondent."

[1] 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 and Risk Management Manual of Examination Policies (Formal Administrative Actions): http://www.fdic.gov/regulations/safety/manual/section15-1.html#introduction.
[2] Ibid.

Each action record contains, but is not limited to, the following PII and non-PII on respondents:

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

2. Can individuals "opt-out" by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☐ Yes Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

☒ No Explain: Data related to Section 8 enforcement actions is collected by DSC staff as a result of their supervisory examination authority under the FDI Act. DSC staff collects and reviews 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.

3. What are the sources of the information in the system? How are they derived? Explain.

The following are sources of information for the ViSION FIAT module; hard copies of documents are not stored in FIAT, but in the related paper file maintained in secure DSC file rooms:

- **FDIC Insured Banks** – provide records and information to DSC 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 (SAR) filed with the Financial Crime Enforcement Network (FinCEN), U.S. Department of Treasury. Most Section 8 enforcement actions pursued by FDIC originate from a SAR.

- **DSC Field Office Bank Examiners** – provides information about potential or confirmed violations to the DSC Field Supervisor and Regional Case Manager based on issues found during the bank examination or on site. For example, for Section 8(e) cases, prepares a recommendation memorandum clearly explaining the facts of the case and support for a recommended action. Also, assists the Regional Office staff with outreach to the FDIC Regional Counsel and may meet directly with the individual, who may be subject to an action.

- **DSC Field Supervisors** – reviews the documentation, provides further information, makes the determination to proceed with the enforcement action and coordinates the case to the DSC Regional Case Manager.

- **DSC Regional Case Managers** – creates, populates and manages cases in FIAT based on the supporting information and documentation provided by the DSC Field Office. Enters a summary of the Field Office Bank Examiner recommendation memorandum and other comments as the action is developed. Consults with the Regional Counsel and the Regional Director in the course of making a determination about taking an action against an individual. Ensures that the FIAT record is complete and updated in a timely manner. If a decision to pursue an action is made, 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** – advises on case matters and provides written legal opinions used by the Regional Case Manager.

- **DSC Washington Office Reviewer** – after receiving recommendation memorandum and other documents from the Regional Office, enters the receipt of the case into FIAT and notifies the Washington Legal Office of the matter.

4. What Federal agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

    - **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.

The following Federal agencies also provide information for ViSION, but the information is not used by FIAT nor contains PII:

- **Federal Banking Agencies** – DSC tracks examination and supervisory activities of other banking agencies. The Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision and (OTS) provide electronic or hard copies of their *Reports of Examination* to DSC. A summary of the reports are manually entered into ViSION.

- **Federal Reserve Board National Information Center** (NIC) – provides structure information (e.g., bank holding company and affiliate data) about banking organizations for use in case administration.

- **Office of Thrift Supervision (OTS)** – provides structure information (e.g., thrift holding company and affiliate data) about thrift organizations for use in case administration.

- **Federal Financial Institutions Examination Council (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.

5. What state and local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

   State Banking Departments provide ViSION with data similar to that of the Federal Banking Agencies.

6. What other third party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

   No other third party sources provide data for ViSION.

## E. Access to Data:

1. Who will have access to the data in the system (e.g., users, managers, system administrators, developers, contractors, other)? Explain their purpose for having access to this information.

The following FDIC users will have access to the ViSION FIAT module:

- **DSC Regional Case Managers** – can view and edit data in support of the examination and supervisory process and to analyze and make determinations concerning Section 8 enforcement actions. FDIC Regional Offices have primary responsibility for processing enforcement actions.

- **DSC Field Supervisors** – can view data in support of the examination and supervisory process, including enforcement actions.

- **DSC Field Office Bank Examiners** – can view data in support of the examination and supervisory process. The examination process is normally the starting point for identifying Section 8 issues.

- **DSC Washington Office Reviewer** – can view and edit data in support of the examination and supervisory process, including enforcement actions.

- **FDIC Division of Insurance Research staff** – can view data and reports in support of banking research and statistical activities.

- **FDIC Division of Resolutions and Receivership staff** – can view data and reports in support of bank closing activities.

- **FDIC Legal Division Regional and Washington Office staff** – can view data in support of their work on enforcement actions.

- **FDIC Office of Inspector General Staff** – can view data in support of their investigatory activities.

- **Federal Banking Agencies (FRB, OCC, and OTS) and State Banking Department staff** – can view data in support of their examination and supervisory mission.

Other authorized internal FDIC users (employees and contractors) will be in the Division of Information Technology, which is responsible for providing technical support during the construction of the system, confirming adherence to FDIC policies and standards (e.g., security and privacy), and providing system administration and maintenance support.

2. How is access to the data determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Explain the process.

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 DSC 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.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

   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.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access? (Please list processes and training materials) Explain the controls that have been established and how are they monitored or reviewed.

   An audit trail process captures data manipulations (i.e., Insert, Update or Delete), identifying who performed the data manipulation and when the data manipulation was performed. FDIC Security Awareness Training and Privacy Orientation are 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. Superusers (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.

5. Do other systems share data or have access to the data in the system? If yes, explain the purpose for the need to have access.

   ViSION shares information with the following FDIC systems:

- **FDIC Legal Information Management System (LIMS):** The ViSION FIAT module shares enforcement case data with LIMS 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:

- **DSC General Examination System (GENESYS):** provides examination summary data.

- **DSC 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.

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

- **DSC 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.

6. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Has policy or procedures been established for this responsibility and accountability? Explain.

   While the DSC ViSION Program Manager/Data Owner is responsible, all parties of the interfaces are responsible for protecting the privacy rights of the public affected by the interfaces. All users who have system access must complete required training that covers the system rules of behavior. These rules in addition to FDIC Corporate policies establish responsibility

[3] A Privacy Impact Assessment for LIMS is available upon request on www.fdic.gov.
[4] A Privacy Impact Assessment for the 4C system is available upon request on www.fdic.gov.

and accountability. Additionally, the system manager is provided logs of predefined audit events.

7. If other agencies use the data, how will the data be used? Who establishes the criteria for what data can be shared? Have non-disclosure agreements been effected? Explain the purpose for the need to share the data?

   Authorized Federal Banking Agency (FRB, OCC, OTS) 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.

8. Who is responsible for assuring proper use of the data? Is this individual fully accountable should the integrity of the data be compromised? Explain.

   The DSC ViSION Program Manager/Data Owner is responsible for management and decision authority over a specific area of corporate data. The DSC Program Manager/Data Owner and DSC 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 Security Training and Privacy Orientation and/or ViSION specific security training and rules of behavior to ensure proper use of the data.

9. Explain the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally. Would the reputation of the corporation be affected?

   Due to the sensitive nature of certain Section 8 enforcement actions, disclosure of privacy related data could have a significant harmful impact on the reputation of the affected individual and financial institution, as well as, the Corporation's reputation and trust with the public. Therefore, appropriate safeguards are maintained to protect the confidentiality of an individual's information during the investigation of a case.

   Once a determination is made by DSC that an enforcement action will be taken against an individual, the DSC Regional Case Manager will notify the respondent by letter of the FDIC's intent to take a Section 8 action. As the case proceeds, the name of and action against the individual may be made public when FDIC issues, for example, a *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*.

10. What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

    Contractors are employed by FDIC's Division of Information Technology to provide system design and maintenance support. 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 Security Training and Privacy Orientation which includes Rules of Behavior. Programmers are restricted to the development and quality assurance environment using test data and do not have access to operate in the production environment.

11. Explain whether or not the data owner is contacted if it is not clear if other agencies share or have access to the data.

    Yes - the DSC ViSION Program Manager/Data Owner is contacted and responsible for reviewing and approving any system access or data sharing requests from agencies. To date, only the Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision and State Banking Agencies are approved to have access to ViSION/FIAT.

## F. Accuracy, Timeliness, and Reliability

1. How is the data collected from sources other than FDIC records verified? Has action been taken to determine its reliability that it is virus free and does not contain malicious code? Who is responsible for this making this determination? Explain.

   Data is manually entered into the ViSION FIAT module by DSC Regional Case Managers. There are no automated feeds of records containing PII into FIAT. 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 reliability.

2. How will data be checked for completeness? How is this being measured? What is the source for ensuring the completeness of the data? Explain the method used.

   The ViSION FIAT module includes automated checks to ensure that the data entered by DSC 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.

## G. Attributes of the Data?

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? Is this part of the system design? Is this documented, if so, where is the document located? Explain.

   Yes. ViSION was designed to support the supervisory mission of FDIC. The FIAT module was designed to track and document Section 8 enforcement actions. Use of the personal information described above is relevant and necessary for these critical business functions, including making and executing Section 8 actions. This use is documented in the system design document and user manual. These and other ViSION system documents, including the system architecture and security plan, are maintained in FDIC's official system document repository.

2. Will the system derive personal identifiable information from any new data previously non-inclusive, about an individual through aggregation from the information collected? What steps are taken to make this determination? Explain.

   No – the only personal information contained in the system (e.g., name and home address) is already known and obtained from the insured institution.

3. Can the system make privacy determinations about employees that would not be possible without the new data? If so, explain.

   No – ViSION is not applicable to FDIC employees.

4. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Does the consolidation of data result in personal identifiable information? Explain.

   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 PII and non-PII about the facts, dates and status of the case and investigation.

5. How is the data retrieved? Can it be retrieved by a personal identifier (e.g., social security number)? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

   There is no retrieval of an enforcement action record by an individual name. The ViSION FIAT module action records are retrieved by a financial institution identification (ID) number, such as the FDIC insured institution certificate (CERT) number, FDIC institution number (UNINUM), or ViSION/FIAT System Identification (SYSID) number.

   Retrieval of a record using the CERT or UNINUM will result in the display of all actions related to an institution being tracked in FIAT. Upon retrieving the record, the user must perform an additional step (such as Add/Update) to retrieve individual respondent information that is maintained in a separate table within the FIAT database.

   Retrieval of a record using the ViSION/FIAT SYSID will result in the display of a single action against a bank or individual. Upon retrieving the action, individual respondent information is not immediately displayed, but is accessible from this page.

   When a user creates a new action record in FIAT, he/she is able to perform a "Search for Respondents" in order to avoid creating a duplicate respondent entry. The user enters the respondent's name, which results in a listing of all records with the same name. No other FIAT record information is retrieved using this search function.

6. What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? Explain how they are distributed.

   A standard report can be generated by authorized ViSION/FIAT users internal and external to FDIC with criteria that allow the displaying Section 8 actions, which the user can select the individual to the action to be displayed.

**H. Maintenance and Administrative Controls:**

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? Will the same controls be used? Explain.

   The system is housed at only one FDIC facility utilizing existing physical security controls. This includes restricted access to FDIC facilities and additional access restrictions (badges) to enter data center areas. The data in ViSION/FIAT will be access by authorized FDIC users from across the

country. Consistent data access and use controls will be applied, in accord with FDIC policies and procedures.

2. What are the retention periods of data in this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? Explain.

   ViSION/FIAT follows the guidance in FDIC's Records Retention and Disposition Schedule published by FDIC's Division of Administration. The link below provides on-line access to the entire Records Retention Schedule: http://fdic01/division/doa/adminservices/records/index.html.

   Records are stored in electronic media and in paper format within individual file folders. Records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with National Archives and Records Administration and FDIC Records Retention and Disposition Schedules. Disposal is by shredding or other appropriate disposal systems.

3. What are the procedures for disposition of the data at the end of the retention period? How long will any reports produced be maintained? Where are the procedures documented? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the procedures? Explain.

   ViSION/FIAT follows the guidance in FDIC's Records Retention and Disposition Schedule published by FDIC's Division of Administration. The link below provides on-line access to the entire Records Retention Schedule: http://fdic01/division/doa/adminservices/records/index.html, in conjunction with NARA guidance.

4. Is the system using technologies in ways that the Corporation has not previously employed (e.g., Monitoring software, SmartCards, Caller-ID, biometrics, PIV cards, etc.)? Explain.

   No.

5. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology? Explain.

   Not applicable – there is no use of technologies not previously employed by FDIC.

6. If monitoring is being performed, describe the data being collected. Is monitoring required? If so, describe the need for the monitoring and identify the requirements and explain how the information is protected.

Daily or periodic monitoring of individuals within ViSION/FIAT is not performed by users; however, ViSION/FIAT maintains an audit trail of all enforcement case activity and data. The audit trail is not modifiable and is accessible only to authorized users. ViSION/FIAT also has system level auditing which includes user names and login history and security level auditing.

7. If monitoring is not required, explain the controls that will be used to prevent unauthorized monitoring?

   The system is only accessible by those individuals who have been authorized and given specific privileges.

8. In the Federal Register, under which Privacy Act Systems of Record (SOR) does this system operate? Provide number and name.

   The ViSION FIAT module operates under the following Privacy Act System of Records Notice: "30–64–0002 Financial Institution Investigative and Enforcement Records."

9. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

   Yes – the Privacy Act SORN will require updating to reflect the use of financial institution identification numbers as another method for retrieving FIAT records.

## I. Business Processes and Technology

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

   No.

2. Does the completion of this PIA potentially result in technology changes?

   No.