FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Privacy Impact Assessment (PIA)

for

## Division of Information Technology (DIT)

## Enterprise Data Warehouse (EDW) Co-Location v 1.0


Date Approved by Chief Privacy Officer (CPO)/Designee:
10/19/2015

# Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

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.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

# Section 2.0: System/Project Description

**2.1 In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.**

The FDIC's Division of Information Technology (DIT) Enterprise Information Management Section (EIMS) is leading the Enterprise Data Warehouse (EDW) Co-Location project. The purpose of EDW is to create a centralized reporting environment that improves data accuracy, analysis and reporting for authorized

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

Corporate users. The scope of EDW Co-Location is comprised of five (5) data marts[3] that will be migrated, all APEX applications, and fourteen (14) data marts (specified in Section 3.3) that will be replicated (copied) into the EDW database instance. A migrated data mart is one where the data structures, data, and associated interfaces are moved to the EDW database instance, and no longer reside in the database instance they are currently located in. A replicated data mart is one where the data structures are replicated into the EDW database instance, and data is copied from the replicated data mart into the EDW. The replicated data marts will remain in the database instance as they currently are, and a copy of the data and data structures will reside in the EDW database instance. The data replicated will be copied from the upstream application reporting repositories using enterprise Extract, Transform and Load (ETL) and database technologies. When fully operational, EDW will enable end users to query, analyze, chart, and report on integrated data from these various reporting repositories from a single, centrally managed database.

# Section 3.0: Data in the System/Project

*The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.*

**3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.**

EDW will contain the following types of PII:

- Full Name
- Date of Birth
- Social Security Number (full or partial) or other number originated by a government that specifically identifies an individual
- Home Address
- Phone Numbers (e.g., phone, fax, and cell) (non-work)
- Financial Information and/or Numbers (e.g., checking account #/PINs/access or security codes/passwords)

The above PII pertains to the following categories of individuals:

**(A) FDIC Employees (active and inactive):** In addition to the types of PII listed above, EDW will contain the following additional employee personnel data:

- Employee Identification Number, Employee Demographic Information, Status, Tour of Duty, Salary, and Time & Attendance
- E-mail Address (non-work)

This information will be used to support Corporate personnel staffing analysis, workforce planning, and workload analysis. Employee information will also be utilized in supporting examination scheduling and supervision activities.

**(B) FDIC Contractors (active and inactive):** EDW will contain information (such as contractor name, personal contact information, financial/invoice information, etc.) about individuals who work under

[3] The following five (5) data marts will be migrated into EDW database instance: the Chairman's Quarterly Report (CQAR), Strategic Workforce Planning Initiative Data Mart (SWPI), Diversity and Inclusion Analytics (DIA), Reporting Data Mart Migration (RDMM), and Receivership Assets Data Repository (RADR).

contract to the FDIC. This information will be used to support examination scheduling and supervision activities, and organizational effectiveness.

**3.2 What is the purpose and intended use of the information you described above in Question 3.1?**

The purpose and intended use of this information is to support FDIC business users and applications in performing reporting and analytical analysis of FDIC operational data. Specifically, as noted in Section 3.1, the employee information described above will be used to support Corporate personnel staffing analysis, workforce planning, and workload analysis. Employee information, as well as contractor information, will also be utilized to support examination scheduling, supervision activities, and organizational effectiveness.

**3.3 Who/what are the sources of the information in the system? How are they derived?**

EDW sources information from fourteen (14) reporting databases (data marts) listed in the table below. These reporting databases will be incorporated into EDW in three release cycles[4]. EDW will extract data from these data marts on a nightly basis using batch programs.

Note: EDW will not be pulling data from any of the migrated data marts specified in Section 2.1. These marts will be migrated into the co-located environment, but will not be used as a source for EDW replicated data or available to any EDW users.

| Data Source | Data Provided by Source |
|---|---|
| Subcontractor Reporting System (SRS) | Vendor contract and performance information. The following are examples of data found in this repository:<br>• Activities<br>• Duration of Engagement<br>• Demographic<br>• Performance<br><br>This data is used for subcontractor activities and performance reporting. |
| New Financial Environment Enterprise Performance Management (NFE EPM) | Enterprise Financial Information. The following are examples of data found in this repository:<br>• Employee Demographic<br>• Employee Levels<br>• Employee Salaries<br>• Accounts Payable<br>• Vendor Demographic<br>• Vendor Payment<br>• Vendor Invoices<br><br>This data is used for enterprise financial performance analysis and reporting. |
| NFE IODS New Financial Environment Interface Operational Data Store (NFE IODS) | Enterprise Financial Information interface to legacy systems. The following are examples of data found in this repository:<br>• Employee Demographic<br>• Employee Levels<br>• Employee Salaries<br>• Accounts Payable |

[4] As of the date of this document, three (3) data marts are in Production status. The remaining 11 data marts are scheduled for the third and fourth quarter of 2015. Due to the scope and breadth of the data sourced from these data marts, individual tables and columns are not listed. For example, EDW sources over two-hundred and ten (210) tables from the NFE EPM data mart, over fifty (50) tables from the NFE IODS data mart, and over fifty (50) tables from the 4C data mart below. These tables alone represent multiple thousand columns.

| | |
|---|---|
| | • Vendor Demographic<br>• Vendor Payment<br>• Vendor Invoices<br><br>This data is used for enterprise financial performance analysis and reporting, as well as for enterprise financial data provisioning to legacy systems. |
| Communication, Challenge, Control, and Capabilities (4C) | Closed bank asset, counterparty, and closure information. The following are examples of data found in this repository:<br>• Fund/Financial Institution<br>• Asset<br>• Receivership<br>• Servicer<br>• Third Party Ownership<br><br>This data is used for receivership's asset sales and services performance analysis and reporting. |
| Financial Data Warehouse (FDW) | Legacy Enterprise Financial Information. The following are examples of data can be found in this repository:<br>• Employee Demographic<br>• Employee Levels<br>• Employee Salaries<br>• Accounts Payable<br>• Vendor Demographic<br>• Vendor Payment<br>• Vendor Invoices<br><br>This data is used for legacy enterprise financial performance analysis and reporting. FDW was replaced by NFE, and the repository is being retained for historical reporting. |
| Virtual Supervision Information on the Net Financial and Management Reporting (ViSION-FMR) | Risk Examination Information. The following are examples of data found in this repository:<br>• Financial Institution<br>• Examiner Demographic<br>• Risk Examination<br>• Organizational Hierarchy<br><br>This data is used for examination performance analysis and reporting. |
| System of Uniform Reporting and Compliance (SOURCE) | Compliance Examination Data. The following are examples of data found in this repository:<br>• Financial Institution<br>• Examiner Demographic<br>• Compliance Examination<br>• Organizational Hierarchy<br><br>This data is used for examination performance analysis and reporting. |
| Summary of Deposits (SOD) | Summary of Deposits (Branches). The following are examples of data found in this repository:<br>• Financial Institution<br>• Deposit Information<br>This data is used for financial institution's deposit analysis and reporting. |
| Summary of Deposits | Summary of Deposits (Savings & Loan Branches). The following are examples of data |

| | |
|---|---|
| for Savings and Loan (SOD-SL) | found in this repository:<br>• Financial Institution<br>• Deposit Information<br><br>This data is used for financial institution's (Legacy Savings and Loans) deposit analysis and reporting. This is historical deposit information for Savings and Loans. |
| Corporate Business Information System (CBIS) | Call Report Data. The following are examples of data found in this repository:<br>• Financial Institution<br>• Shared National Credit<br>• Call Data<br>• Examiner View<br>• Third Party Demographic<br><br>This data is used for financial market trends, research, analysis and reporting. |
| Research Information System (RIS) | Call Report, Examination, and Institution Data. The following are examples of data found in this repository:<br>• Financial Institution<br>• Call Data<br>• Examiner View<br>• Third Party Demographic<br><br>This data is used for financial market trends, research, analysis and reporting. |
| Structure Information System Distribution Center (SIMS-SDC) | Structured Institution Data. The following are examples of data found in this repository:<br>• Financial Institution<br>• Holding Company<br>• Branch<br>• Location<br>• Institution Officer<br><br>This data is used for financial institution reporting. |
| Division of Supervision and Compliance Hours (DSC Hours) | Employee Time Reporting Information. The following are examples of data found in this repository:<br>• Examination<br>• Examiner<br>• Time and Attendance<br><br>This data is used for examination (compliance and risk) performance analysis and reporting. |
| Thrift Financial Report Internet Application (CALL-TFR-IA) | Condition and Income and the Thrift Financial. The following are examples of data found in this repository:<br>• Thrift Demographic<br>• Financial<br>• Holding Company<br>• Organizational Hierarchy<br><br>This data is used for financial thrift analysis and reporting. |

**3.4 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used?** Explain.

No external agencies are providing data directly to EDW.

**3.5 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 third-party sources are providing data directly to EDW.

**3.6 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (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: Individuals are not provided with an opportunity to opt out of EDW by declining to provide information or consenting only to a particular use of their data. Information in EDW is not obtained directly from individuals. Rather, this data is obtained and replicated from other internal FDIC systems. This information is necessary for supporting the Corporation's various data analysis and reporting requirements.

# Section 4.0: Data Access and Sharing

*The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.*

**4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.**

The primary users of EDW will be authorized Corporate employees from all FDIC Divisions and Offices. Authorized users will use the data to analyze operational activities and generate operational reports related to supervision, insurance, and resolution activities. All authorized users will have "read-only" access to the data. Only select authorized users will have access to the data that is deemed confidential/sensitive in EDW. Access to all data will be approved in accordance with standard internal access control processes and policies. In addition, Division of Information Technology (DIT) contractors will have access to the system for purposes of system maintenance.

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

The business owners of the data have defined secure and general access roles for the data. These roles have been registered in the FDIC's Identity Access Management System (IAMS) for users to request. Once an IAMS request is submitted, the business owners of the upstream transaction system (e.g., NFE, 4C) will review/approve the IAMS request. Once an IAMS request has been approved by the business, database administrators will add the account to the requested role.

**4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.**

☐ No ☒ Yes Explain. EDW users will use existing enterprise reporting and database query tools to access the data [e.g., Business Objects, Tableau, SQL Developer, TOAD, Advanced Query Tool (AQT)]. These reporting and database tools generally do not retain data and are not considered systems, with the exception of Tableau. For more information, refer to FDIC's Privacy Impact Assessment for Tableau.

**4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.** Not applicable.

No external agencies or entities will have access to data in EDW.

**4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.**

All authorized users who have access to EDW must have the approval of their manager/supervisor and the business owner of the authoritative application system source. The FDIC's Identity Access Management System (IAMS) security application is utilized to support access requests. IAMS requests must be submitted by users and approved by managers in order for users to gain access to RDMM.

Further, access to EDW is controlled through role-based filtering. Access to data in EDW adheres to current FDIC information security policies and practices. The following policies are applicable:

- FDIC 1360.1 Automated Information Systems (AIS) Security Program
- FDIC 1360.8 Information Security Categorization
- FDIC 1360.9 Protecting Sensitive Information
- FDIC 1360.12 Reporting Computer Security Incidents
- FDIC 1360.15 Access Control for Information Technology Resources
- OMB Circular A-130 Management of Federal Information

**4.6 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?**

DIT contractors will support the design and maintenance of EDW. These DIT contractors are categorized as "EHR" (exceptionally high risk), which means they undergo specialized training given the level of access they have to enterprise data, and are required to sign FDIC Confidentiality Agreements.

## Section 5.0: Data Integrity and Security

*The following questions address how data security and integrity will be ensured for the system/project.*

**5.1 How is data in the system verified for accuracy, timeliness, and completeness?**

Data is replicated into EDW from upstream source systems (authoritative sources), which have existing production controls to ensure data is timely, accurate, and complete. EDW maintains the integrity of data as it is replicated from the upstream transaction system into EDW via the following technical controls:

- Technical processes detect error conditions and raise appropriate alerts which are communicated to operators;
- Checks are in place to identify anomalous update activity (e.g., thresholds are used to detect an unusually high volume of updates); and
- Automated reconciliation checks are run on a weekly basis to ensure data matches the upstream source system.

**5.2 What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.** The following controls are used to manage access to the EDW:

- EDW is hosted at one FDIC facility utilizing existing physical security controls. This includes restricted access to FDIC facilities and additional access restrictions (e.g., badges) to data centers. The data in EDW will be accessed only by authorized FDIC users from across the country. Consistent data access and use controls will be applied, in accordance with FDIC policies and procedures.

- All access requests will be initiated and managed via the FDIC's Identity Access Management System (IAMS). System access to EDW for data exchange between internal FDIC organizations requires a Memorandum of Understanding (MOU).

- Standard Database auditing is utilized in EDW to capture login/logout information.

- The ability to edit/manipulate data is not granted to any user.

- Weekly reports are generated to publish access information at the database object level.

- The Corporate Information Security and Privacy Awareness Training, which includes the Rules of Behavior, are mandated for all users of FDIC systems, including EDW. This training has specific information regarding compromise and the prevention of misuse of data.

- In addition, authorized Corporate users will be provided with targeted orientation/training on the roles and responsibilities for utilizing APEX (or other sanctioned reporting tools).

## Section 6.0: Data Maintenance and Retention

*The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.*

6.1 **How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

Users will only have access to tables/views based on the approved IAMS requests, and only authorized users will be able to query PII. If a user is authorized to access PII data, the user will be able to query data about an individual using name, social security number, home phone number, or any other attribute describing the individuals.

6.2 **What kind of reports can be produced on individuals? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?**

Authorized Corporate users will be able to generate reports to support specific data analysis and reporting requirements of their respective divisions. These reports will only be used for authorized business needs, such as to support staffing decisions and assignments, personnel recruiting, and supervision/enforcement actions. Depending on the business need, the nature of these reports will vary and may include PII about FDIC employees and contractors.

**6.3 What are the retention periods of data in this system? 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 period for the data in EDW has not been established at this time. When decided, the retention period for data in the EDW will vary based on several factors, including the criticality of the data relative to reporting and analysis, and the guidance provided in the Records Retention and Disposition Schedule published by the FDIC Division of Administration. Future discussions are planned to address data migration/retention issues with representatives from the Division of Information Technology (DIT), Corporate Program Managers/Data Stewards, the EDW Steering Committee, and other key stakeholders.

Procedures for disposition of the data at the end of the retention period will be based on the disposition procedures for the sources systems. The sources systems' disposition procedures were established in accordance with FDIC Records Schedules in conjunction with National Archives and Records Administration (NARA) guidance.

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

EDW will not operate as a Privacy Act Systems of Record.

**6.5 If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.**

Not applicable.

## Section 7.0: Business Processes and Technology

*The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.*

**7.1 Will the system aggregate or consolidate data in order to make privacy 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?**

Aggregated, consolidated, and/or derived data will be created and maintained within EDW itself. As such, the same controls that protect replicated source data from unauthorized access or use (described above in Section 5.1), would be applied to consolidated, aggregated, and/or derived data.

**7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.**

EDW does not employ any of the new technologies mentioned above nor any similar technologies to collect, maintain, or track information about individuals.

**7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.**

EDW itself does not provide the ability to monitor individuals or users.

**7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?**

Any exposure of privacy-related data could adversely affect the reputation of the Corporation and is deemed to be a moderate risk. Since the system is used to maintain data about FDIC employees and contractors, it is necessary to maintain safeguards to protect against the potential fraud or theft from either an FDIC employee or FDIC contractor personnel. Disclosure of this data could be harmful to both individuals and employees of the Corporation. Therefore, FDIC takes all security measures necessary to prevent an unauthorized disclosure of data.

**7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.**

No.