FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Reporting Data Mart Migration (RDMM)

August 2012

FDIC Internal System

Table of Contents

System Overview

The FDIC's Division of Information Technology (DIT) leads the Reporting Data Mart Migration (RDMM) project. The purpose of RDMM is to create a centralized reporting environment that improves data accuracy, analysis and reporting for authorized Corporate users.

RDMM is used to support the data analysis and reporting requirements of the FDIC's Office of Complex Financial Institutions (OCFI), Division of Depositor and Consumer Protection (DCP), Division of Risk Management Supervision (RMS), and Division of Resolutions and Receiverships (DRR). Other FDIC divisions will be able to utilize RDMM in the future.

RDMM contains personally identifiable information (PII) and non-PII about FDIC employees, as well as information about individuals who apply to FDIC job positions. This data is used by authorized Corporate users to conduct workload analysis and make staffing decisions and assignments. In addition, RDMM contains sensitive supervision information that may contain PII about bank employees, officials, and directors involved in supervision/enforcement actions.

The RDMM reporting environment extracts data from the Enterprise Data Warehouse (EDW). EDW contains data that has been pulled from authoritative data sources, such as the Corporate Human Resources Information System (CHRIS), CHRIS Time & Attendance (CHRISTA), FDICLearn Learning Management System (FDICLearn), Monster/Quickhire, and System of Uniform Reporting of Compliance and CRA Exams (SOURCE). Users are able to query, analyze, chart, and report on integrated data from these various data sources.

The RDMM reporting environment is segregated from the source data to eliminate reporting inconsistencies and prevent data exposure (by replacing the current need to download application data to the end user's machine for report processing). The configuration enables implementation of role-based access and data management techniques to further enhance data security, as well as aligning Corporate business functions with the FDIC target data architecture.

Personally Identifiable Information (PII) in RDMM

RDMM contains personally identifiable information (PII) and non-PII from current and prospective FDIC employees. Current active and inactive FDIC employee information include: Full Name, Employee ID, Status, Tour of Duty, other personnel data and technical evaluation information, such as test dates and test scores. Prospective applicant information include: Full Name, Home Address, Home Phone Number, Personal Email Address, Veterans Preference, Ethnicity, and Application Score. Additional information regarding the status of the individual's preliminary background investigation is stored in RDMM, but is limited to only the date that a particular action in the preliminary background investigation process occurred.

In addition, RDMM contains sensitive supervision/enforcement information, such as bank ratings, institution data, and comments about examinations. This data may contain PII about individuals who are involved in FDIC supervision and enforcement actions, such as bank employees, officials, and directors.

Purpose & Use of Information in RDMM

The purpose of RDMM is to create a centralized reporting environment that improves data accuracy, analysis and reporting for authorized Corporate users. Authorized Corporate users generate reports to support specific data analysis and reporting requirements of their respective divisions.

The data in RDMM is both relevant and necessary for the purpose for which the system was designed, namely to support critical business functions, 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, job applicants, or individuals involved in supervision/enforcement actions.

Sources of Information in RDMM

RDMM extracts data from the Enterprise Data Warehouse (EDW) to satisfy business reporting requirements and follows an Extract, Transform, and Load (ETL)[1] process. The information contained within EDW derives from the following internal and external sources:

- Corporate Human Resources Information System (CHRIS)
- CHRIS Time and Attendance (CHRISTA)
- Corporate University FDICLearn (FDICLearn)
- QuestionMark
- Background Investigation Result Tracking (BIRT)
- Virtual Supervisory Information On the Net (ViSION)[2]
- System of Uniform Reporting of Compliance and CRA Exams (SOURCE)
- Structure Information Management System (SIMS)
- Call Processing System (CALL)
- CALL/Savings & Loans (CALL/SL)
- Uniform Banking Performance Report Internet Application (UBPR)
- Corporate Business Information System – Federal Reserve Board (CBIS-FRB)
- Financial Industry Regulatory Authority (FINRA)
- Monster Analytics/Quickhire

Notice & Consent

Individuals do not have the opportunity to "opt out" of providing their information for inclusion in RDMM. PII is not collected directly from individuals and is obtained via a secure data feed from the Enterprise Data Warehouse (EDW) that contains data that has been pulled from authoritative data sources, such as CHRIS, CHRISTA, FDICLearn, Monster/Quickhire, and SOURCE. This information is necessary for supporting the Corporation's various data analysis and reporting requirements.

---

[1] Extract, transform and load (ETL) is a process in database usage and in data warehousing that involves: extracting data from authoritative sources; transforming it to fit operational needs (which can include quality levels); and loading it into the end target (database or data warehouse).

[2] ViSION consolidates data from up to thirteen authoritative sources.

Access to Data in RDMM

The primary internal FDIC users of the RDMM data mart are authorized Corporate employees for the purposes of generating specialized reports to assist with activities that include conducting workload analysis, recruiting/hiring new employees, making staffing decisions and assignments, and satisfying supervision/enforcement-related duties. All authorized users have a "read-only" access to the data. Only select FDIC users have access to the data in RDMM that is deemed confidential/sensitive. Additionally, DIT contractors have access to RDMM for purposes of system maintenance.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
Enterprise Data Warehouse (EDW)	EDW is a warehouse of stored data that has been pulled from other data sources, such as CHRIS, CHRISTA, FDICLearn, Monster/Quickhire, and SOURCE.	Full Name, home address, home phone number, personal email address, military status, and ethnicity
Personnel, Recruiting, and Reporting (PRR)	PRR is used to log and monitor new hire and position management processes across all FDIC offices and provide real time reporting capabilities. RDMM provides a data feed containing applicant/employee and job vacancy information to PRR.	Full Name, home address, home phone number, personal email address, military status, and ethnicity
Corporate Human Resources Information System (CHRIS)	CHRIS is a Commercial Off-The-Shelf (COTS) Human Resource Management System for U.S. Federal Government agencies. CHRIS supports all human resource functions.	Full name, date of birth, SSN, home address, home telephone number, personal email address, employee ID, ethnicity/race, handicap information, employment history, gender and BI results.

Data Accuracy in RDMM

The RDMM project collects data via an Extract, Transform, and Load process. This function is implemented to ensure data completeness and accuracy of data. If required data is missing, the ETL process is terminated. The ETL process triggers an email notification and an exception report back to the source system/system representative when the data is incomplete.

Data Security for RDMM

In order to access RDMM, users must obtain the approval of their Manager/Supervisor and the approval of data steward/data owner of the authoritative application system sources. Only authorized users with a "need to know" are granted access to RDMM. FDIC uses the Identity Access Management System (IAMS) security application to support access requests. IAMS requests must be submitted by users and approved by managers in order to gain access to RDMM. Further, access to RDMM is controlled through role-based filtering.

Access to data in RDMM 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 Resources

Contractors must sign an annual Contractor Confidentiality Agreement to be granted access to this system for the purpose of maintenance support and development of new requirements in the RDMM system.

The Business Intelligence Unit stakeholders, in collaboration with the Corporate Program Managers/Data Stewards and DIT Project Manager have overall responsibility for protecting the privacy rights of those individuals and employees whose information is contained in RDMM. In addition, all individual users of RDMM are responsible for ensuring the protection of privacy rights of the public and employees affected by the RDMM interface

Users must take the mandatory FDIC Information Security and Privacy Awareness Training, which includes specific policies and procedures for responsibility and accountability of information regarding compromise and the prevention of misuse of data. All users are responsible for protecting personal information covered by the Privacy Act and must certify that they agree to abide by the system's Rules of Behavior to retain access to the system. Additionally, existing security policies and procedures are leveraged for database role definitions and grants, via the IAMS software solution.

The RDMM 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. Consistent data access and use controls will be applied, in accordance with FDIC policies and procedures. Additionally, RDMM segregates the sensitive data and does not consolidate personal identifiable information with non-sensitive data.

For external data received from FINRA, FDICLearn, QuestionMark, and the Monster Analytics system, this data enters the FDIC environment (either physically or logically) through a variety of secure transmission methods, such as Secure File Transfer Protocol, or is made available to the FDIC through other secure channels.

System of Records Notice (SORN)

RDMM operates under the following FDIC Privacy Act SORNs:

- FDIC 30–64–0002 *Financial Institutions Investigative and Enforcement Records.*
- FDIC 30–64–0004 *Changes in Bank Control Ownership Records.*
- FDIC 30-64-0005 *Consumer Complaint and Inquiry Records.*
- FDIC 30–64–0008 *Chain Banking Organizations Identification Records.*
- FDIC 30–64–0016 *Professional Qualification Records for Municipal Securities Dealers, Municipal Securities Representatives, and U.S. Government Securities Brokers/Dealers.*
- FDIC 30–64–0007 *Employee Training Information Records.*
- FDIC 30–64–0015 *Personnel Records.*
- FDIC 30–64–0011 *Corporate Recruitment Tracking Records.*

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.