FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Personnel, Recruiting, and Reporting (PRR)

January 2013

FDIC Internal System

Table of Contents

System Overview

Within FDIC, the Division of Resolutions and Receiverships (DRR) is charged with, among other important responsibilities, providing customer support to depositors and customers of failed banks and coordinating the overall closing process. The employees hired to fulfill the FDIC/DRR mission are supported through the Planning and Resource Management (RM) Section within DRR. RM developed the Personnel, Recruiting, and Reporting (PRR) application to improve the hiring process and is used by DRR RM staff to log and monitor the new hire and position management processes across all offices nationwide.

PRR contains personally identifiable information (PII) about current and prospective FDIC/DRR employees, such as their names, dates of birth, personal contact information, and education and employment records. PII is obtained via a secure data feed from FDIC's Reporting Data Mart Modernization (RDMM), which receives personnel employee data from FDIC's Corporate Human Resources Information System (CHRIS) and new hire data from Monster.com. In addition, authorized RM staff manually collect and enter potential hire information into PRR based on data they obtain directly from Monster.com, and hardcopy and electronic documents (i.e. resumes, cover letters, etc.) they receive from job applicants.

Personally Identifiable Information (PII) in PRR

PRR contains personally identifiable information (PII) and non-PII from current and prospective FDIC/DRR employees such as: name, date of birth, employee identification number (only applicable for employees), home address, non-work phone numbers (e.g. home, cell, fax), personal email address, education records and employment status and/or records of employment.

Purpose & Use of Information in PRR

The data in PRR is both relevant and necessary for the purpose for which the system was designed, namely to support critical business functions to monitor the new hire and position management processes. Personal information is necessary for identification of potential candidates and tracking each applicant through the hiring process.

PRR provides a variety of reports that include PII and non-PII data. PRR has the ability to be routinely queried based on an individual's unique identifier, such as first and last name. These reports are used for a variety of purposes, including determining the number of authorized positions within DRR, the number of vacancies, and which of the departments have vacancies. These reports are run by authorized DRR Planning and Resource Management Staff. Reports containing PII are provided to authorized FDIC personnel on a "need to know" basis.

Sources of Information in PRR

Information in PRR is derived from a wide range of sources, including:

- **FDIC Reporting Data Mart Modernization (RDMM) data:** RDDM is a centralized reporting environment that obtains data from authoritative FDIC data sources, such as the Corporate Human Resources Information System (CHRIS-HR) and Monster.com (Quickhire). RDDM provides a data feed containing applicant/employee and job vacancy information to PRR via a secure interconnection. The data is transmitted server to server within a closed access environment.
- **Monster.com / Quickhire data:** Using a secure login, authorized DRR RM staff logs directly into the Monster.com Website to capture new application data and manually enters this data into the PRR application.
- **Electronic / Hard copy applicant-supplied source data:** (i.e. resume, cover letter, etc.) is manually obtained and entered by authorized DRR RM staff into the PRR application.

After the data is loaded into PRR, the DRR RM staff reconciles the information, correcting any discrepancies, and proceeds with the onboarding process with the applicant information.

Notice & Consent

Individuals do not have the opportunity to "opt out" of providing their information for inclusion in PRR. PII is obtained via a secure data feed from FDIC's Reporting Data Mart Modernization (RDDM), and is not collected directly from individuals. In some instances, DRR RM may request information directly from a potential new hire in order to resolve an application question. The requested data is necessary to process new hire job applications for individuals wishing to apply and be considered for FDIC employment.

In addition, through the currently used online application process, the individual/applicant agrees for their information to be collected by FDIC/DRR.

Access to Data in PRR

Authorized FDIC employees and contractors from the DRR Planning and Resource Management Section have access to the PRR data.

In order to access PRR, users must obtain the approval of their Manager/Supervisor and the DRR PRR Program Manager. Only authorized users with a "need to know" are granted access to PRR. Authorized FDIC employee users and contractors employed by DRR Planning and Resource Management Section must complete the DRR Security and Privacy Awareness Course and the Corporation's mandatory Information Security and Privacy Awareness Training, annually, which includes the Corporate Rules of Behavior. Contractors must sign an annual Contractor Confidentiality Agreement to be granted access to this system for the purpose of maintenance support and development for new requirements in the PRR system.

PRR uses a role-based access control system to restrict user edit access to the minimum necessary to perform their duties. The authority granted to a user's access role governs the user's ability to access or manipulate information. PRR's functional security classifies each user in one of the established business roles (User role or Administrator role). User's access is tracked in the Corporation's access control tracking system.

Data Sharing

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

System Name	System Description	Type of Information Processed
FDIC Reporting Data Mart Modernization (RDDM)	A centralized reporting environment that obtains data from authoritative FDIC data sources, such as CHRIS. The data is transmitted server to server within a closed access environment.	Customer-provided data (contains PII and non-PII)

Data Accuracy in PRR

The DRR PRR Program Manager is responsible for assuring proper use and integrity of the data. The DRR PRR Program Manager and DRR Information Security Manager serve as the sources of information for data definition and data protection requirements.

Data received from Monster.com/Quickhire is the result of applicant data entry. Data entry screens and load modules managed by the DRR RM staff include edit checks to ensure that business rules and data relationships are maintained. Data validation is incorporated in a required format within the application and the database. In some instances, DRR RM may request information directly from a potential new hire in order to resolve an application question. The DRR Program Manager runs daily audit logs following a documented reconciliation process.

Data Security for PRR

The DRR PRR Program Manager has overall responsibility for protecting the privacy rights of individuals by developing data access guidelines and standards that must be followed.

Data received from Monster.com/Quickhire is the result of applicant data entry. Both Monster.com and FDIC have controls in place to ensure the data is free from viruses and malicious code that could introduce harm in both the Monster.com and FDIC operating environments.

Most of the data is personally identifiable information, which is needed to monitor the new hire and position management processes. The system employs security controls that protect the PRR system/application from unauthorized access. Access to PRR is only granted to those persons within the FDIC specifically authorized by the

Corporation. Access levels and permission levels have been established and access provided only to those persons who have a "need to know" the information contained in the system in order to carry out their duties.

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, all users must log in with active FDIC Network IDs and passwords. 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.

In accordance with OMB Circulars A- 123, and A-l30, Appendix III, PRR has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of: firewalls and IP addresses, passwords, user identification, database permissions and software controls.

System of Records Notice (SORN)

PRR operates under the following FDIC Privacy Act SORN 30-64-0015, *Personnel Records* and FDIC Privacy Act SORN 30-64-0011, *Corporate Applicant Recruiting, Evaluating and Electronic Referral 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.