FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Personnel Security Records (PERSEREC)

July 2014

FDIC Internal System

Table of Contents

System Overview

In support of the Federal Deposit Insurance Corporation's (FDIC's) Strategic Plan Objective of acquiring and retaining only trustworthy employees and contractors, and as required by Federal and FDIC employment suitability requirements, the FDIC Division of Administration (DOA) Security & Emergency Preparedness Section (SEPS) performs on-boarding processes that include fingerprinting, receipt of preliminary background investigation (BI) applications, and preliminary suitability reviews (background checks) on prospective employees and contractors ("applicants"). In addition to performing a preliminary check, DOA/SEPS also initiates Office of Personnel Management (OPM) background investigations (BIs) of FDIC employees and contractors, the results of which are used by SEPS to make a final determination about each individual's suitability for employment. Previously, these records were maintained in case files in a locked storage room. The Personnel Security Records (PERSEREC) solution is being used to upload DOA/SEPS scanned case files (active and inactive) into FDIC's Enterprise Secured Document Repository/Documentum. Documentum is a unified Content Management System that provides tools for working with many types of content (i.e., documents, drawings, scanned images, and hard copies) in a single repository that can span multiple departments and functional areas within an organization.

Personally Identifiable Information (PII) in PERSEREC

PERSEREC maintains background investigation (BI) case files about prospective and existing FDIC employees and contractors. Each BI case may contain a wide variety of PII, including but not limited to the following: Full Name; Date of Birth; Social Security Number (or other number originated by a government that specifically identifies an individual); Photographic Identifiers (e.g., photograph image); Driver's license/state identification number; Biometric Identifiers (e.g., fingerprint and voiceprint); Employee Identification Number; Mother's Maiden Name; Home Address; Phone Numbers (e.g., phone, fax, and cell) (non-work); Medical Information (Medical Records Numbers, Medical Notes, or X-rays); Financial Information and/or Numbers; Certificates (e.g., birth, naturalization, marriage); Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, or other); Investigation Report or Database; Email Address (non-work); Education Records; Military Status and/or Records; Employment Status and/or Records; and Foreign Activities and/or Interests.

Purpose & Use of Information in PERSEREC

FDIC/DOA SEPS uses the PII specified above to make an informed decision to recommend or deny potential new hires and retain trustworthy employees and contractors.

Sources of Information in PERSEREC

DOA SEPS employee/contractor employment background investigation (BI) case files are manually scanned by authorized FDIC/DOA SEPS personnel via the PERSEREC solution.

BI case files consist of the various background investigation forms[1] submitted by applicants during the preliminary suitability review, and by FDIC employees/contractors as part of the full BI conducted by OPM. In addition, case files consist of BI-related information from external (non-FDIC) entities, such as the Federal Bureau of Investigation (FBI), OPM, and three major credit bureaus (Experian, Equifax, and TransUnion). Specifically, this data includes information collected via the preliminary suitability review process that SEPS completes to ensure prospective FDIC employee and contractor personnel meet minimum Integrity and Fitness standards as set forth by the FDIC. This process includes checks of FBI fingerprint criminal records, review of personnel security questionnaires, credit reports provided by the three major credit reporting agencies, and other internal FDIC resources such as digital and manual fingerprinting of applicants at FDIC facilities, local police stations, and authorized commercial vendors. Also, during the case adjudication process (which is the process that SEPS completes once the cleared applicant has been on-boarded/hired by the Corporation after rending a favorable determination of the initial review), source information comes from a cleared applicant's OPM BI corresponding to the designated risk level associated with the duties of each position.

Notice & Consent

Individuals cannot "opt out" of providing their personal information or consent to only particular uses. All PII collected is necessary to complete BIs as a condition of employment with the FDIC.

Access to Data in PERSEREC

Only internal FDIC/DOA SEPS staff will have access to the data in the PERSEREC solution. A limited number of authorized DOA SEPS users are granted access to the system to allow BIs to be completed. PERSEREC also has controls in place to prevent the misuse of data by those having access to the data, such as: passwords, user identification, database permissions, and software controls.

[1] BI forms includes: the following: Forms FDIC 1600/10 – Notice and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Act of 1970, 15 U.S.C & 1681, et. Seq, FDIC 1600/11 – Position Designation Record, OF-306 – Declaration for Federal employment, FDIC, FDIC 2120/16 Applications Certification Statement, FD 258 – Fingerprint Card. FDIC 1600/13 – Personnel Security Action Request, FDIC 1600/18 Tax Check Waiver forms, SF – 85 (original) – Question for Non-Sensitive position for all positions designated as low risk, SF-85P – Questionnaire for Public Trust and Personnel Investigation Summary Data are available on the FDIC net under Standardized Forms.

Data Sharing

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

No other systems currently have access to the content stored in the PERSEREC solution.

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy in PERSEREC

BI information is received from a number of external non-FDIC sources. Since the DOA PERSEREC solution does not communicate directly with any internal or external sources, the supporting BI information received is verified for accuracy by the DOA SEPS staff prior to placing the information into the BI case file. All case files (active or inactive) contain an activity log. The activity log is used by DOA SEPS to track the status and completeness of each BI case.

Data Security for PERSEREC

The DOA PERSEREC solution has security controls in place in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. These security controls include, but are not limited to, FDIC Windows General Support System (GSS) access controls, firewalls, network (NT) login credentials, data permissions, and intrusion-detection systems to prevent unauthorized monitoring. All employees including contractors must meet the requirement for security Privacy Act protection information. An access matrix is in place to prevent inadvertent not authorized to use the system or those who do not have direct need to know certain information contained in the system.

Authorized access is limited to FDIC DOA SEPS staff. Access is controlled by NT login credentials and Active Directory (AD). All PERSEC users have user ID and password that is issued by the Corporation. The DOA PERSEREC solution further controls access with user-defined roles. DOA Management approval is required to allow user access to the DOA PERSEREC solution.

The Corporate Program Manager/Data Owner and DOA SEPS Manager share overall responsibility for protecting the data in the DOA PERSEREC solution. In addition, all individual users of the DOA PERSEREC solution are responsible for ensuring and protecting the information contained in the DOA PERSEREC system. The policy and procedures for responsibility and accountability are included in the FDIC's Information Security and Privacy Awareness Training, which includes the Corporate Rules of Behavior, and all users of the system are required to complete this training on an annual basis. All users of FDIC systems must annually certify that they agree to abide by the Rules of Behavior to retain access to FDIC systems.

System of Records Notice (SORN)

PERSEREC operates under the FDIC Privacy Act SORN 30-64-0015: *Personnel 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.