FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Identity, Credential and Access Management (ICAM)

March 2012

FDIC Internal System

Table of Contents

System Overview

The Federal Deposit Insurance Corporation (FDIC) Identity, Credential and Access Management (ICAM) program provides access control that is aligned with Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 requires the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 directs the use of a common identification credential (ID Badge) for both logical and physical access to federally controlled facilities and information systems. Compliance with HSPD-12 is intended to enhance security, increase efficiency, reduce identity fraud and protect privacy.

HSPD-12 requires that the credential be secure and reliable. Under the Directive, the National Institute of Standards and Technology (NIST) published technical standards for secure and reliable forms of Personal Identity Verification (PIV), which are defined in Federal Information Processing Standard Publication 201 (FIPS 201).

FIPS 201 has two parts: PIV-I and PIV-II. The requirements in PIV-I support the control objectives and security requirements pertaining to the standard background investigation required for all federal employees and long term contractors. The standards in PIV-II support the technical interoperability requirements described in HSPD 12. PIV-II specifies standards for implementing identity credentials on integrated circuit cards (i.e. smart cards) for use in a federal system. FIPS 201 requires agencies to:

- Establish roles to facilitate identity proofing, information capture and storage, and card issuance and maintenance;
- Develop and implement a physical security and information security infrastructure to support these new credentials;
- Establish processes to support the implementation of a PIV program.

FDIC is neither an executive department nor an executive agency and is not required to comply with HSPD-12. However, the FDIC has elected to phase-in components of HSPD-12 through the implementation of the Identity, Credential, and Access Management (ICAM) program. The ICAM program includes Enrollment and Issuance Stations, a centralized card management system, a card production facility, and card activation, finalization, and issuance.

Personally Identifiable Information (PII) in ICAM

ICAM contains personally identifiable information (PII) and non-PII from prospective and current FDIC employees and contractors such as: full name, other used names, date of birth, place of birth, home address, email address, telephone number, employee identification number, SSN, gender, citizenship, identifying information (e.g. weight, height, hair color, eye color, ethnicity, organization affiliation, employee affiliation, fingerprints, digital color photograph, spouse and relative associations, marital status, employment history, address history, educational history, personal references, military records, criminal history, illegal drug history, foreign countries visited, background investigations history, and financial history.

Purpose & Use of Information in ICAM

The data maintained in ICAM is both relevant and necessary for the purpose for which the system was designed, namely to meet the requirements mandated by HSPD-12, FIPS 201, and OMB M-05-24 by conducting background investigations, completing the identity proofing and registration process, and issuing a PIV card for FDIC employees and contractors to acquire physical access to federal facilities, enhance security, reduce identity fraud and protect personal privacy and information.

Sources of Information in ICAM

ICAM obtains data directly from the individual applicant through background investigation forms and questionnaires required by FIPS 201. This information is compared to the Federal Bureau of Investigation (FBI) criminal history repository to prevent hiring of applicants with a criminal record or possible ties to terrorism. The results of the suitability and criminal check are provided to the adjudicator at the FDIC and a list of pre-approved and adjudicated applicants are maintained in ICAM.

The biographic information collected as part of this process is necessary to establish the PIV applicant's identity. During the registration process, the applicant appears at FDIC in which the Enrollment Official verifies two approved forms identification documents, uses the fingerprint scanner to collect the applicant's fingerprints, and takes a photograph of the applicant.

Notice & Consent

Individuals do have the opportunity to "opt out" of providing their information for inclusion in ICAM. The Privacy Act Statement provided by FDIC notifies the employee/contractor that the completion of the FDIC PIV enrollment is voluntary. The notice also informs the employee that failure to provide the requested information may delay or prevent the receipt of an FDIC PIV Identification card.

Access to Data in ICAM

Access to the data is limited to those with an operational need to access the information and specifically limited to authorized FDIC Division of Administration (DOA) Security and Emergency Preparedness Section (SEPS) staff members and ICFI contractors. This includes designated adjudicators, enrolment personnel, and management personnel that have been authorized to use the system in accordance with their roles and responsibilities. Additionally, access to the data requires management approval.

The FDIC MyID CMS Security Officer has access to all information contained within MyID CMS, and the appointed FDIC Enroller, FDIC Registrar, and FDIC Issuer have access to the data associated with individuals they process during the ICAM enrollment and issuance process. A Sponsor (federal manager or project officer) typically initiates the request for an applicant's FDIC card. Subsequently, an Enroller meets with the applicant to collect the information required for an FDIC badge. A

Registrar then administers the identity proofing and registration process and ensures successful completion of the background investigation (BI). After receiving final approval from the Registrar, an FDIC Issuer delivers the identity credential to the applicant.

Contractors are involved in the design, implementation, and maintenance of ICAM and MyID CMS. As contractually required, non-disclosure agreements are completed and in place for all contractors associated with the design, implementation, and maintenance. Audit logs are maintained and used throughout the process to ensure that access and operations are appropriate and necessary. A "least-privilege" role-based access system restricts access to data on a "need to know" basis.

Data Sharing

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

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

Data Accuracy in ICAM

The FDIC Registrar is responsible for ensuring the submission of the FDIC background investigation form and for initiating the printing of the PIV card, which is then issued to the applicant. The FDIC Enrollment Official manually enters the applicant's necessary information from the Applicant's ID Card Request Form into MyID CMS to generate a data record. The FDIC Registrar ensures the Applicant's data has been entered into MyID CMS correctly and completely. If the required information is not entered or is incomplete, the PIV Card is not issued to the Applicant.

Data Security for ICAM

The FDIC ICAM Program Manager is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual application users are responsible and accountable for assuring the proper collection and use of the data. The FDIC Program Manager has overall responsibility for the ICAM Program and is accountable for establishing the criteria, procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected. Unauthorized monitoring is prevented by restricting access to the system to only those FDIC employees/contractors that have a business need and that have been appropriately authorized.

Encryption technologies, firewalls and intrusion-detection systems are used to ensure that Internet "eavesdropping" does not take place and that data is sent only to its intended destination and to an authorized user, by an authorized user. Audit logs are maintained and used to ensure that access and operations are appropriate and

necessary. Authorized employees must complete training specific to their roles within the system to ensure they are knowledgeable about how to protect personally identifiable information.

The FDIC ICAM Program Manager also has overall responsibility for protecting the privacy rights of individuals by developing data access guidelines and standards which must be followed by authorized employees and contractors as part of the ICAM Program. Furthermore, the ICAM system is fully compliant with FIPS 201, Part I (PIV-I), which describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12.

System of Records Notice (SORN)

ICAM 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.