

FEDERAL DEPOSIT INSURANCE CORPORATION

Privacy Act of 1974, as Amended; System of Records

AGENCY: Federal Deposit Insurance Corporation

ACTION: Notice of New System of Records

SUMMARY: The Federal Deposit Insurance Corporation (FDIC) proposes to add one new system of records to its existing inventory of systems subject to the Privacy Act of 1974, as amended. This new system of records is entitled FDIC 30-64-0035, Identity, Credential and Access Management Records. We hereby publish this notice for comment on the proposed system of records..

DATES: Comments on the proposed system of records must be received on or before _____ . The proposed system of records will become effective 45 days following publication in the *Federal Register*, unless a superseding notice to the contrary is published before that date.

ADDRESSES: You may submit written comments by any of the following methods:

- Agency web site: Located at www.fdic.gov/regulations/laws/federal/propose.html. Follow instructions for submitting comments on this web site.
- Email: Send to comments@fdic.gov. Include “Notice of New FDIC System of Records” in the subject line.
- Mail: Send to Gary Jackson, Counsel, Attention: Comments, FDIC System of Records, 550 17th Street, NW, Washington, DC 20429.

All submissions should refer to “Notice of New FDIC System of Records.” By prior appointment, comments may also be inspected and photocopied in the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1005, Arlington, Virginia 22226, between 9:00 a.m. and 4:00 p.m. (EST), Monday to Friday.

FOR FURTHER INFORMATION CONTACT: Gary Jackson, Counsel, FDIC, 550 17th Street, NW, Washington, DC 20429, (703) 562-2677.

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, as amended, the FDIC has conducted a review of its Privacy Act systems of records and has determined that it needs to add one new system of records. The FDIC’s system notices were last published in the *Federal Register* on December 13, 2011, Volume 76, Number 239 (76 FR 77626); this last publication may be viewed at <http://www.fdic.gov/about/privacy/> on the FDIC’s Privacy web page.

The Identity, Credential and Access Management Records system will contain records collected or generated in the process of producing Personal Identity Verification (PIV) cards issued by the FDIC. PIV cards are required for granting and controlling access to FDIC and other federal facilities.

A Report of New Systems of Records has been submitted to the Committee on Oversight and Government Reform of the House of Representative, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget pursuant to Appendix I to OMB Circular A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated November 30, 2000, and the Privacy Act, 5 U.S.C. 552a(r).

More detailed information on the proposed new system of records may be viewed in the complete text below.

FDIC-30-64-0035

SYSTEM NAME: Identity, Credential and Access Management Records.

SECURITY CLASSIFICATION: Unclassified but sensitive.

SYSTEM LOCATION: The Division of Administration, FDIC, 550 17th Street, NW, Washington, DC 20429, and the FDIC regional or area offices. (See Appendix A for a list of the FDIC regional offices and their addresses.) Duplicate systems may exist, in whole or in part, at secure sites and on secure servers maintained by third-party service providers for the FDIC.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system covers all FDIC employees, contractors, and other individuals who have applied for, been issued, and/or used a Personal Identity Verification (PIV) card for access to FDIC or other federal facilities.

CATEGORIES OF RECORDS IN THE SYSTEM: This system includes all information submitted during application for the PIV card and any resulting investigative and adjudicative documentation required to establish and verify the identity and background of each individual issued a PIV card. The system includes, but is not limited to, the applicant's name, social security number, date and place of birth, hair and eye color, height, weight, ethnicity, status as Federal or contractor employee, organization and office of assignment, company name, employee ID number, telephone number(s), email, biometric identifiers including fingerprints, digital color photograph, signature, data from source documents used to positively identify the applicant, including Form I-9 documents and OPM Forms SF-85 or SF-86, network user name, user access rights, and PIV cardholder history and transaction reports.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819); Executive Order 9397; Section 5113 of the Federal Information Security Act (Pub. L. 104-106, sec. 5113); Section 203 of the Electronic Government Act (Pub. L. 104-347, sec. 203); and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

PURPOSE: The primary purpose of the system is to manage the safety and security of FDIC and other federal facilities, as well as the occupants of those facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under the Privacy Act, 5 U.S.C. 552a(b), all or a portion of the

records or information contained in this system may be disclosed outside the FDIC as a routine use as follows:

- (1) To appropriate Federal, State, and local authorities responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto;
- (2) To a court, magistrate, or other administrative body in the course of presenting evidence, including disclosures to counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal proceedings, when the FDIC is a party to the proceeding or has a significant interest in the proceeding, to the extent that the information is determined to be relevant and necessary;
- (3) To a congressional office in response to an inquiry made by the congressional office at the request of the individual who is the subject of the record;
- (4) To appropriate Federal, State, and local authorities, and other entities when (a) it is suspected or confirmed that the security or confidentiality of information in the system has been compromised; (b) there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs that rely upon the compromised information; and (c) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;
- (5) To appropriate Federal, State, and local authorities in connection with hiring or retaining an individual, conducting a background security or suitability investigation, adjudication of liability, or eligibility for a license, contract, grant, or other benefit;
- (6) To appropriate Federal, State, and local authorities, agencies, arbitrators, and other parties responsible for processing any personnel actions or conducting administrative hearings or corrective actions or grievances or appeals, or if needed in the performance of other authorized duties;
- (7) To appropriate Federal agencies and other public authorities for use in records management inspections;
- (8) To officials of a labor organization when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions;
- (9) To contractors, grantees, volunteers, and others performing or working on a contract, service, grant, cooperative agreement, or project for the Federal Government;
- (10) To notify another Federal agency when, or verify whether, a PIV card is no longer valid.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

Storage: Records are stored in electronic media or in paper format within individual file folders.

Retrievability: Records are indexed and retrieved by name, social security number, other ID number, PIV card serial number, and/or by any other unique individual identifier.

Safeguards: Electronic records are password protected and accessible only by authorized personnel. Paper format records maintained in individual file folders are stored in lockable file cabinets and/or in secured vaults or warehouses and are accessible only by authorized personnel.

Retention and Disposal: Records are retained in accordance with National Archives and Records Administration and FDIC Records Retention and Disposition Schedules. Disposal is by shredding or other appropriate disposal systems. PIV cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. PIV cards are destroyed by shredding no later than 90 days after deactivation.

SYSTEM MANAGER(S) AND ADDRESS: Deputy Director, Corporate Services Branch, Division of Administration, FDIC, 3501 North Fairfax Drive, Arlington, VA 22226

NOTIFICATION PROCEDURE: Individuals wishing to determine if they are named in this system of records or who are seeking access or amendment to records maintained in this system of records must submit their request in writing to the Legal Division, FOIA & Privacy Act Group, FDIC, 550 17th Street, NW, Washington, DC 20429, in accordance with FDIC regulations at 12 CFR Part 310. Individuals requesting their records must provide their name, address and a notarized statement attesting to their identity.

RECORD ACCESS PROCEDURES: See "Notification Procedure" above.

CONTESTING RECORD PROCEDURES: See "Notification Procedure" above. Individuals wishing to contest or amend information maintained in this system of records should specify the information being contested, their reasons for contesting it, and the proposed amendment to such information in accordance with FDIC regulations at 12 CFR Part 310.

RECORD SOURCE CATEGORIES: Information is provided by the individual to whom the record pertains, those authorized by the subject individuals to furnish information, and the FDIC's personnel records. Information regarding entry and egress from FDIC facilities or access to information technology systems is obtained from use of the PIV card.

EXEMPTIONS CLAIMED FOR THE SYSTEM: None.

Appendix A

FDIC Atlanta Regional Office
10 Tenth Street, NE, Suite 800
Atlanta, GA 30309-3906

FDIC Boston Area Office
15 Braintree Hill Office Park, Suite 100
Braintree, MA 02184-8701

FDIC Chicago Regional Office
420 W. VanBuren, Suite 1700
Chicago, IL 60606

FDIC Dallas Regional Office
1601 Bryan Street,
Dallas, TX 75201

FDIC Kansas City Regional Office
1100 Walnut Street, Suite 2100
Kansas City, MO 64106

FDIC Memphis Area Office
6060 Primacy Parkway, Suite 300
Memphis, TN 38139

FDIC New York Regional Office
350 Fifth Avenue, Suite 1200
New York, NY 10118-0110

FDIC San Francisco Regional Office
25 Jessie Street at Ecker Square, Suite 2300
San Francisco, CA 94105-2780

By order of the Board of Directors
Dated at Washington, DC, this ___ day of _____, 2013.

Robert E. Feldman
Executive Secretary