



## Privacy Act of 1974; System of Records

**AGENCY:** Federal Deposit Insurance Corporation (FDIC).

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, as amended, the Federal Deposit Insurance Corporation (FDIC) is modifying an existing system of records, FDIC-035, Identity, Credential, and Access Management Records. This system of records is used by FDIC to manage the safety and security of FDIC resources, facilities, information technology systems, and other Federal government agency facilities and systems, as well as the occupants of those facilities. The FDIC is updating this system of records to rename it “Credentialing, Facility Access, and Visitor Management Records” and to modify numerous sections of the notice, including the Categories of Individuals; Categories of Records; Record Sources; Routine Uses; Policies and Practices for Storage, Retention and Disposition of Records; and Record Access, Contesting Records, and Notification Procedures. Additionally, this notice includes non-substantive changes to simplify the formatting, clarify the text of the previously published notice, and improve consistency across FDIC system of record notices.

**DATES:** This action will become effective on **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. The routine uses in this action will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**, unless the FDIC makes changes based on comments received. Written comments should be submitted on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

**ADDRESSES:** Interested parties are invited to submit written comments identified by Privacy Act Systems of Records (FDIC-035) by any of the following methods:

- *Agency Website:* <https://www.fdic.gov/resources/regulations/federal-register->

publications/. Follow the instructions for submitting comments on the FDIC website.

- *Email:* [comments@fdic.gov](mailto:comments@fdic.gov). Include “Comments-SORN (FDIC-035)” in the subject line of communication.
- *Mail:* Jennifer M. Jones, Deputy Executive Secretary, Attention: Comments SORN (FDIC-035), Legal Division, Office of the Executive Secretary, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.
- *Hand Delivery/Courier:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW building (located on F Street NW) on business days between 7:00 a.m. and 5:00 p.m.

*Public Inspection:* Comments received, including any personal information provided, may be posted without change to <https://www.fdic.gov/resources/regulations/federal-register-publications/>. Commenters should submit only information that the commenter wishes to make available publicly. The FDIC may review, redact, or refrain from posting all or any portion of any comment that it may deem to be inappropriate for publication, such as irrelevant or obscene material. The FDIC may post only a single representative example of identical or substantially identical comments and in such cases will generally identify the number of identical or substantially identical comments represented by the posted example. All comments that have been redacted, as well as those that have not been posted, that contain comments on the merits of this document will be retained in the public comment file and will be considered as required under all applicable laws. All comments may be accessible under the Freedom of Information Act (FOIA).

**FOR FURTHER INFORMATION CONTACT:** Shannon Dahn, Assistant Director, Privacy, 703-516-5500, [privacy@fdic.gov](mailto:privacy@fdic.gov).

**SUPPLEMENTARY INFORMATION:** Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, FDIC is modifying an existing system of records, FDIC-035, Identity, Credential

and Access Management Records. The FDIC uses the system to manage physical security operations and visitor access to FDIC facilities and implement Homeland Security Presidential Directive 12 (HSPD-12), which requires Federal agencies to use a common identification credential for access to Federally-controlled facilities and information systems. This system of records notice (SORN) is being updated to rename it “Credentialing, Facility Access, and Visitor Management Records” and to modify the Categories of Individuals, Categories of Records, Routine Uses, and various other sections of the notice to clarify and better reflect the FDIC’s facility access control and visitor management system.

This system of records contains records on FDIC employees, contractors, and other individuals who have applied for, been issued, and/or used a Personal Identity Verification (PIV) card or HSPD-12 compliant credentials for access to FDIC or other Federal facilities. It also contains records on FDIC visitors and guests who require infrequent access to FDIC facilities and/or have otherwise not been issued a PIV or HSPD-12 compliant credentials by FDIC or another Federal agency. The system consists of both electronic and paper records and is used to manage physical security and access to FDIC facilities, verify that all persons entering FDIC facilities are authorized, and ensure the safety and security of FDIC facilities and their occupants.

This update proposes to modify the Routine Uses section to align with the updated FDIC standard routine uses (Routine Uses 1 through 10). Routine Use 11, which permits disclosures to another Federal agency when, or to verify whether, a PIV card is no longer valid, is proposed to be modified to better support and facilitate access control and visitor management at FDIC facilities. Proposed Routine Use 13 is new and proposes to permit disclosures to the U.S. General Services Administration (GSA) or another agency, organization, or individual for the purpose of performing audit or oversight operations in accordance with interagency or contractual agreements or as authorized by

law. Other routine uses were not substantially modified but may have been renumbered.

The System Location section was updated to reflect that the records may be maintained at various FDIC locations, including authorized cloud environments. The System Manager section was updated to align with FDIC organizational changes. The Purpose section was modified to clarify that the system supports (a) FDIC's issuance of PIV cards or other forms of credentials or badges to FDIC personnel and individuals who are visitors or guests at FDIC facilities or events, and (b) the maintenance of entry and exit records from FDIC facilities as well as FDIC-sponsored parking. The Purpose section was also amended to clarify that FDIC may use the data during the development or use of information technologies. The Categories of Individuals and Categories of Records sections were updated to improve clarity and public understanding of the individuals, including short-term FDIC visitors and guests, who are covered by this system of records and the data maintained about them. The Sources of Records section was modified to add FDIC's identity and access management systems, GSA's USAccess system, and other Federal agencies as sources and otherwise edited for clarity. The Storage of Records section was updated to clarify that electronic records may be stored locally on digital media or in FDIC-owned or authorized vendor cloud environments. The Retrieval of Records section was amended to expand and clarify how records are indexed and retrieved from this system of records. The Retention and Disposal of Records section was modified to add retention and disposition procedures for visitor management records. It was also modified to clarify the retention and disposition procedures for facility access control records related to FDIC employees, contractors, and other individuals who have applied for, been issued, and/or used a PIV card or HSPD-12 compliant credentials. The Record Access, Contesting Records, and Notification Procedures sections were all updated to include the website address for the FDIC FOIA Service Center.

This system includes only records maintained by FDIC. Certain PIV card

information not included in this system is covered under a GSA government-wide SORN, GSA/GOVT-7, HSPD-12 USAccess, which applies to participating Federal agency employees, consultants, and volunteers who require long-term access to Federal facilities, systems and networks, as well as individuals who are authorized to perform or use services in agency facilities. FDIC-035 covers additional categories of individuals and records to include occasional and short-term visitors and guests with temporary credentials, paper-based security logs, and other information necessary to support access and visitor management at FDIC facilities. This system of records is separate from FDIC-009, Safety and Security Incident Records, which supports the administration and maintenance of FDIC safety and security incident investigations involving FDIC facilities, property, personnel, contractors, volunteers, or visitors. Further, this system is separate from FDIC-041, Personal Information Allowing Network Operation, which supports the approval, monitoring, and disabling of access by individuals that interact with FDIC information technology resources.

This modified system will be included in FDIC's inventory of record systems.

**SYSTEM NAME AND NUMBER:** Credentialing, Facility Access, and Visitor Management Records, FDIC-035.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** The Federal Deposit Insurance Corporation (FDIC) located at 550 17th Street NW, Washington, DC 20429, and other FDIC office locations.

Information may also be stored within an appropriately authorized cloud environment or in other secure locations.

**SYSTEM MANAGER(S):** Chief, Physical Security and Intelligence Unit, Security Enterprise Programs Section, Corporate Services Branch, Division of Administration, 3501 Fairfax Dr. Arlington, VA 22226.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819); Executive Order 9397, as amended; and Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

**PURPOSE(S) OF THE SYSTEM:** The primary purpose of the system is to manage the safety and security of FDIC resources, facilities, information technology systems, and other Federal government agency facilities and systems, as well as the occupants of those facilities. The system supports FDIC's issuance of Personal Identity Verification (PIV) cards or other forms of credentials or badges to FDIC personnel and individuals who are visitors or guests at FDIC facilities or events. It also supports the maintenance of entry and exit records from FDIC facilities as well as FDIC-sponsored parking. Information in the system of records may also be used to support the development and operation of current and future information technology to support the objectives of the FDIC's physical security operations program.

**Note:** This system does not cover records described in FDIC-041, Personal Information Allowing Network Operation, which supports the approval, monitoring, and disabling of access by individuals that interact with FDIC information technology resources. It also does not cover records described in FDIC-009, Safety and Security Incident Records, which supports the administration and maintenance of FDIC safety and security incident investigations involving FDIC facilities, property, personnel, contractors, volunteers, or visitors.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** This system covers (1) all FDIC employees, contractors, and other individuals who have applied for and/or been issued a PIV card or HSPD-12 compliant credentials by FDIC; (2) Federal government employees, contractors, and other individuals who require access to FDIC facilities and have been issued a PIV card or HSPD-12 compliant credentials by another

(non-FDIC) Federal agency; and (3) FDIC visitors, guests, or other individuals who require infrequent access to FDIC facilities and/or have otherwise not been issued a PIV card or HSPD-12 compliant credentials.

**CATEGORIES OF RECORDS IN THE SYSTEM:** This system contains the following categories of records:

*(1) Records maintained on FDIC employees, contractors, and other individuals who have applied for and/or been issued a PIV card or HSPD-12 compliant credentials by FDIC* include all information submitted during application for the PIV card required to establish and verify the identity of each individual issued a PIV card. These records include, but are not limited to, the individual's name, Social Security number (SSN), date and place of birth, hair and eye color, height, weight, ethnicity, status as Federal or contractor employee, employee ID number, email address, home and work address, telephone numbers, biometric identifiers including fingerprints, digital color photograph, physical and/or logical access rights, and data from source documents used to positively identify the applicant, including passport and Form I-9 (Employment Eligibility Verification) documents. Records also include entry and egress details (e.g., date, time, location of entry) and, as applicable, purpose of entry, agency point of contact/sponsor, and vehicle information, such as vehicle identification, license plate number, and state of issuance.

**Note:** This system includes only records maintained by the FDIC. FDIC participates in the General Services Administration (GSA) USAccess shared service that provides PIV credentialing services for Federal agencies. FDIC's USAccess records are covered by GSA's government-wide system of records, GSA/GOVT-7, HSPD-12 USAccess.

*(2) Records maintained on Federal government employees, contractors and other individuals who access FDIC facilities using PIV cards or HSPD-12 compliant credentials issued by other (non-FDIC) Federal agencies* include the following information: the individual's full name; date of birth; digital image (photograph); hair

color; eye color; height; weight; physical/mailling address; email address; employer/agency name and affiliation (e.g., employee, contractor, volunteer, etc.); telephone number; PIV card/HSPD-12 compliant credentials issue and expiration dates; copies of documents used to verify identification (e.g., driver's license, passport, etc.); vehicle information (if parking in FDIC facilities), including vehicle make, model and color; license plate number; state of issuance; date, time, and location of entry and exit; purpose for entry; and agency point of contact/sponsor. Additionally, the system will access the Public Key Infrastructure (PKI) certificate for the individual's PIV/HSPD-12 compliant credentials in order to grant/provision access to FDIC facilities but will not store or maintain the certificate.

*(3) Records maintained on FDIC visitors, guests, and other individuals who require infrequent access to FDIC facilities and/or have not been issued a PIV card or HSPD-12 compliant credentials include the following information: full name; date and place of birth; physical/mailling address; email address; telephone numbers; employment information (e.g., employer/company name, position title, etc.); organization/office of assignment; digital photograph; identification number, such as driver's license number or passport number; images of and information from relevant identification documents (e.g., driver's license, passport, etc.); U.S. citizenship status; vehicle information (if parking in FDIC facilities), including vehicle make, model and color; license plate number; state of issuance; date, time, and location of entry and exit; purpose for entry; and agency point of contact/sponsor.*

**RECORD SOURCE CATEGORIES:** Information in this system is obtained from the individual to whom the record pertains; supervisors, designated approving officials, sponsors or FDIC visitors or guests, and/or those authorized by the subject individuals to furnish information; FDIC's identity and access management and personnel systems and records; GSA's USAccess system; and other Federal agencies issuing PIV or HSPD-12

compliant cards/credentials. Information regarding entry and egress from FDIC facilities or access to information technology systems is obtained from use of the PIV card or HSPD-12 compliant credentials.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING**

**CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, 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, local, tribal, territorial, and foreign agencies responsible for investigating or prosecuting a violation of, or for enforcing or implementing a statute, rule, regulation, or order issued, when the information, either alone or in conjunction with other 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 or adjudicative body before which the FDIC is authorized to appear when, (a) the FDIC or any component thereof; or (b) any employee of the FDIC in his or her official capacity; or (c) any employee of the FDIC in his or her individual capacity where the FDIC has agreed to represent the employee; or (d) the United States, where the FDIC determines that litigation is likely to affect the FDIC or any of its components, is a party to litigation or has an interest in such litigation, and the FDIC determines that use of such records is relevant and necessary to the litigation, provided, however, that in each case, the FDIC determines that disclosure of the records is a use of the information contained in the records which is compatible with the purpose for which the records were collected.

- (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 agencies, entities, and persons when (a) the FDIC suspects or has confirmed that there has been a breach of the system of records; (b) the FDIC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the FDIC (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the FDIC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- (5) To another Federal agency or Federal entity when the FDIC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach; or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
- (6) To appropriate Federal, State, local, tribal, and territorial agencies 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, to the extent that the information shared is relevant and necessary to the requesting agency's decision on the matter.
- (7) To contractors, grantees, experts, consultants, students, volunteers, and others performing or working on a contract, service, grant, cooperative agreement, or project for the FDIC or the Office of Inspector General for use in carrying out their obligations under such contract, grant, agreement or project.

- (8) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.
- (9) To a Federal, State, local, tribal, or territorial agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act of 1978, as amended.
- (10) To Federal agencies, and to those Federal employees designated by the President or Agency Heads pursuant to Executive Order 14243, for the purposes of identifying and eliminating waste, fraud, and abuse, including the elimination of bureaucratic duplication and inefficiency and the enhancement of the Government's ability to detect overpayments and fraud.
- (11) To notify another Federal agency when, or to verify whether, a PIV card or HSPD-12 compliant credential is no longer valid, or to otherwise facilitate access control and visitor management at FDIC and other Federal facilities.
- (12) 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.
- (13) To the U.S. General Services Administration or another agency, organization, or individual for the purpose of performing audit or oversight operations in accordance with interagency or contractual agreements or as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Records are stored electronically or in paper format in secure facilities. Electronic records may be stored locally on digital media, in FDIC-operated cloud environments, or in vendor cloud

service offerings that are appropriately authorized and/or certified.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records are indexed and retrieved by name, SSN, date of birth, driver's license number, passport number, PIV card serial number, mailing address and/or email address.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF**

**RECORDS:** Records relating to FDIC employees, contractors or other individuals who applied for, been issued, and/or used a PIV card or HSPD-12 compliant credentials are maintained for six (6) years after separation from the FDIC and then dispositioned in accordance with approved records retention schedules. PIV cards are destroyed or deactivated after expiration, confiscation, or return. Visitor access records are maintained for five (5) years after the requested access date and then dispositioned in accordance with approved records retention schedules. Visitor passes are destroyed or deactivated after expiration, confiscation, or return.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures. Administrative safeguards include written guidelines on handling personal information including agency-wide procedures for safeguarding personally identifiable information. In addition, all FDIC staff are required to take annual privacy and security training. Technical security measures within FDIC include restrictions on computer access to authorized individuals who have a legitimate need to know the information; multi-factor authentication for remote access and access to many FDIC systems; strong passwords when multi-factor authentication is not available; use of encryption for certain data types and transfers; firewalls and intrusion detection applications; and regular review of security procedures and best practices to enhance security. Physical safeguards include restrictions on building access to authorized individuals, security guard service, and maintenance of records in lockable offices and

filing cabinets.

**RECORD ACCESS PROCEDURES:** Individuals requesting access to records about them in this system of records should submit their request online through the FDIC FOIA Service Center at [fdic.gov/foia](http://fdic.gov/foia). Alternatively, individuals can send a request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street NW, Washington, DC 20429, or email [efoia@fdic.gov](mailto:efoia@fdic.gov). Individuals will be required to provide a detailed description of the records they seek including time period when the records were created and other supporting information where possible. Individuals will be required to provide proof of identity in accordance with FDIC regulations at 12 CFR part 310.

**CONTESTING RECORD PROCEDURES:** Individuals contesting the content of or requesting an amendment to their records in this system of records should submit their request online through the FDIC FOIA Service Center at [fdic.gov/foia](http://fdic.gov/foia). Alternatively, individuals can send a request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street NW, Washington, DC 20429, or email [efoia@fdic.gov](mailto:efoia@fdic.gov). The request should contain the individual's reason for requesting the amendment and a description of the record (including the name of the appropriate designated system and category thereof) sufficient to enable the FDIC to identify the particular record or portion thereof with respect to which amendment is sought. Requests must specify which information is being contested, the reasons for contesting it, and the proposed amendment to such information in accordance with FDIC regulations at 12 CFR part 310. Individuals will be required to provide proof of identity in accordance with FDIC regulations at 12 CFR part 310.

**NOTIFICATION PROCEDURES:** Individuals seeking to know whether this system contains information about them should submit their request online through the FDIC FOIA Service Center at [fdic.gov/foia](http://fdic.gov/foia). Alternatively, individuals can send a request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street NW, Washington, DC 20429, or email [efoia@fdic.gov](mailto:efoia@fdic.gov). Individuals will be required to provide proof of identity

in accordance with FDIC regulations at 12 CFR part 310.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** 80 FR 66982 (Oct. 30, 2015); 84 FR 35184 (Jul. 22, 2019); 90 FR 51316

(Nov. 17, 2025).

Federal Deposit Insurance Corporation.

Dated at Washington, DC, on February 18, 2026.

**Jennifer M. Jones,**

*Deputy Executive Secretary.*

**BILLING CODE 6714-01-P**

[FR Doc. 2026-03432 Filed: 2/19/2026 8:45 am; Publication Date: 2/20/2026]