FEDERAL DEPOSIT INSURANCE CORPORATION

Privacy Act of 1974; System of Records

AGENCY: Federal Deposit Insurance Corporation (FDIC).

ACTION: Notice of new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the FDIC proposes to establish a new FDIC system of records titled FDIC-042, "Insider Risk Program Records." This system of records enables FDIC to implement the requirements of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. The system supports the operation of the FDIC Insider Risk Program, which seeks to deter, detect, and mitigate risk to FDIC personnel, facilities, assets, resources and information from insiders.

DATES: Written comments should be submitted on or before September 30, 2024. The routine uses in this action will become effective on September 30, 2024.

ADDRESSES: Written comments may be submitted via 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*. Include "Comments-SORN (FDIC-042)" in the subject line of communication.
- *Mail*: James P. Sheesley, Assistant Executive Secretary, Attention: Comments SORN (FDIC-042), Legal Division, Office of the Executive Secretary, Federal

Deposit Insurance Corporation, 550 17th Street NW, Washington, D.C. 20429.

- *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, Chief, Privacy Program, 703-516-5500, *privacy@fdic.gov*.

SUPPLEMENTARY INFORMATION:

Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, as amended, FDIC is establishing a new system of records titled FDIC-042, Insider Risk Program Records, to support the operation of the FDIC Insider Risk (InR) Program. The FDIC InR Program seeks to deter, detect, prevent and mitigate risk to FDIC personnel, facilities, assets, resources and information by insiders. This risk can include damage to the FDIC through

espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of FDIC information, resources, and capabilities. The risk also includes the effects of workplace-related violence on FDIC personnel.

The FDIC InR Program will use records maintained in this system of records to deter, detect, prevent, and mitigate risks or threats from insiders, including the analysis, monitoring, and auditing of information of such records. The InR Program was established to provide an integrated framework for personnel to affirmatively protect the FDIC with a defensive program to address risks posed to its personnel, facilities, assets, resources, and information by insiders as mandated by Executive Order (E.O.) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, issued on October 7, 2011. E.O. 13587 requires Federal agencies to establish an insider threat detection and prevention program, and ensure the security of networks and the responsible sharing and safeguarding of information consistent with the appropriate protections for privacy and civil liberties.

This newly established system will be included in FDIC's inventory of record systems. FDIC is also proposing to exempt this system of records from certain requirements of the Privacy Act to protect against harm to law enforcement and national security interests.

SYSTEM NAME AND NUMBER: Insider Risk Program Records, FDIC-042.

SECURITY CLASSIFICATION: Unclassified and Classified.

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

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

SYSTEM MANAGER(S): Program Manager, Insider Risk (InR) Program, Division of Administration, FDIC, 550 17th Street NW, Washington, DC 20429.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Order (E.O.) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* dated October 7, 2011, and *National Insider Threat Policy and the Minimum Standards*, dated November 21, 2012.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to support the operation of the FDIC InR Program in deterring, detecting and mitigating risk to FDIC personnel, facilities, assets, resources and information by insiders. By identifying and managing insider risks, the InR Program and this system of records help FDIC execute its mission to insure deposits; examine and supervise financial institutions for safety, soundness, and consumer protection; make large and complex financial institutions resolvable; and manage receiverships.

FDIC will use the system of records to manage InR matters; identify and track potential and verified risks to FDIC; manage referrals of potential risks to and from internal and external partners; provide authorized assistance to lawful administrative, civil, and criminal investigations; generate statistical reports; and meet InR reporting requirements. 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 InR Program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The subjects of InR reporting and individuals who exhibit or demonstrate insider risk or threat behaviors or activities, which may include FDIC employees, contractors, detailees, assignees, interns, and authorized FDIC visitors or guests.

In addition, information about other individuals who are not covered by this system of records may be collected, such as individuals who report concerns about insider risk or threat behaviors or activities, witnesses, and relatives.

CATEGORIES OF RECORDS IN THE SYSTEM: The particular information collected for any InR matter may vary widely depending on the facts and nature of the potential risk or threat being assessed and/or mitigated. The system of records may maintain information about covered individuals that is relevant to the assessment and mitigation of the InR matter, including but not limited to the following:

Biographic, descriptive, and contact information, such as name, aliases, physical description / photograph, physical addresses, email addresses and phone numbers (personal and work), date and place of birth, Social Security Number, immigration identifier numbers, citizenship and immigration status, driver's license and vehicle registration information.

Personnel and employment-related information, such as employer name and location, office location, telework location, current and past titles, government-held travel records, nature of affiliation with the FDIC (e.g., works for FDIC contractor, visitor to FDIC facilities), FDIC contract information, work and education history, FDIC or other government access card / credential information, facility and data access privileges,

personnel history (e.g., disciplinary or performance records), reports of investigations or inquiries regarding security violations or misconduct.

Security-related information, such as data and forms gathered and compiled for personnel security, security incidents, visitor security screening, or security clearance purposes, including background investigative reports and supporting documentation; current and former security clearance status(es); raw reporting and finished intelligence products pertaining to adversarial risks or threats; other information related to an individual's eligibility for access to classified information; non-disclosure agreements; document control registries; courier authorization requests; records reflecting personal and official foreign travel; facility access records; visitor access records; records of contacts with foreign persons; and briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations.

Activity information, such as logs of an individual's access to and use of FDIC information systems and facilities, or those of other facilities and systems (e.g., other agency classified or unclassified facilities and systems to which the individual has access) if pertinent to the insider risk being assessed and/or mitigated.

Other information, such as medical information relevant to the insider risk (e.g., an individual's hospitalization status); images, recordings, transcripts, or other media (e.g., CCTV footage, voicemails, news reports, social media postings) relevant to the insider risk being assessed or mitigated; police reports and other law enforcement records; publicly available information; information on family members, dependents, relatives and other personal associations, to the extent relevant to the particular harm or

risk at issue; and other information provided to the InR Program by law enforcement, employers, witnesses, other government agencies, or FDIC employees and contractors.

RECORD SOURCE CATEGORIES: Information in the system is received from: individuals, to include FDIC personnel and contractors; FDIC recordkeeping systems, information assurance databases, and other files; other U.S. Government agencies, to include User Activity Monitoring (UAM) repositories; law enforcement agencies; the Office of the Inspector General; and publicly available information.

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, 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.

(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, treaty, or other international agreement.

(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 appropriate Federal, State, local, territorial, and tribal authorities, agencies, arbitrators, and other parties responsible for hearing, deciding, or processing any personnel actions, controversies, corrective actions, grievances or appeals, or if needed in the performance of other authorized personnel-related duties, but only to the extent the disclosure directly relates to or results from the insider risk matter.

(11) To a Federal, State, local, territorial, or tribal agency in order to obtain information that may be relevant to the FDIC's handling of an insider risk matter.

(12) To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational,

or professional qualifications of an individual who is licensed or who is seeking to become licensed.

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-owned cloud environments, or in vendor cloud service offerings that are appropriately authorized and/or certified.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by: name of the covered individual, email address, computer assigned identification number, business affiliation, and/or event name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records of FDIC Insider Risk Program matters initiated from referrals that meet approved insider risk reporting thresholds are maintained for 25 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are protected from unauthorized access and improper use through administrative, technical, and physical security measures. Access to these records within the FDIC is strictly limited to those with a need to know. External disclosure of information from this system of records may only occur with the approval of the InR Program Office. 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, security and InR training. Technical security measures within FDIC include restrictions on computer access to authorized individuals who have a legitimate need to know the information; required use of strong passwords that are frequently changed; multi-factor authentication for remote

access and access to many FDIC network components; 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. 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. Individuals will be required to provide a detailed description of the records you seek including time period when the records were created and other supporting information where possible, and the reason for amendment or correction. 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*. 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*. Individuals will be required to provide proof of identity and 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*. Alternatively, individuals can send a request in writing to the FDIC FOIA & Privacy Act Group, 550 17th Street, NW, Washington, D.C. 20429, or email *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: This system of records has been exempted from the requirements of subsections (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Records maintained in this system that originated in another system of records shall be governed by both the exemptions claimed for this system as well as any additional exemptions claimed in the originating system of records.

HISTORY: None.

Federal Deposit Insurance Corporation.

Dated at Washington, D.C., on August 30, 2024

James P. Sheesley,

Assistant Executive Secretary.

BILLING CODE 6714-01-P