FED

Privacy Act of 1974; System of Records

AGENCY: Federal Retirement Thrift Investment Board (FRTIB).

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Federal Retirement Thrift Investment Board (FRTIB) proposes to establish a new system of records. Records contained in this system will be used to implement FRTIB's Insider Threat Program.

DATES: This system will become effective upon its publication in today's *Federal Register*, with the exception of the routine uses which will be effective on **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. FRTIB invites written comments on the routine uses and other aspects of this system of records. Submit any comments by **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**.

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

- *Federal eRulemaking Portal: http://www.regulations.gov*. Follow the website instructions for submitting comments.
- *Fax:* 202-942-1676.
- *Mail or Hand Delivery:* Office of General Counsel, Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002.

FOR FURTHER INFORMATION CONTACT: Dharmesh Vashee, General Counsel and Senior Agency Official for Privacy, Federal Retirement Thrift Investment Board, Office of General Counsel, 77 K Street NE, Suite 1000, Washington, DC 20002, (202) 942-1600. For access to any of the FRTIB's systems of records, contact Amanda Haas, FOIA Officer, Office of General Counsel, at the above address and phone number.

SUPPLEMENTARY INFORMATION: FRTIB proposes to establish a new system of records entitled, "FRTIB-23, Insider Threat Program Records." FRTIB is committed to protecting FRTIB facilities, information, and information systems. In order to better protect these resources, FRTIB has established an Insider Threat Program to prevent, detect, and mitigate the effects of insider threats. An insider threat is an individual who has or had authorized access to an organization's assets, and uses their access, either maliciously or unintentionally, to act in a way that could cause harm to FRTIB facilities, information systems, or data.

FRTIB is not legally required to have an insider threat program under Executive Order 13587, as the agency does not maintain classified information. However, FRTIB has implemented this program as a best practice in order to protect the information that it maintains, including controlled unclassified information. FRTIB's Insider Threat Program is based on standards developed by the National Institute of Standards and Technology and the National Insider Threat Task Force. The records compiled to administer the insider threat program may be from any program, record, or source, and may contain records pertaining to information security, personnel security, or physical security.

FRTIB will publish regulations to exempt such material in the new system of records from certain requirements under the Privacy Act of 1974 (5 U.S.C. 552a), based on subsection (k)(2) of the Act.

The collection and maintenance of these records is new. The implementation of this new system of records will be effective on **[INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].** FRTIB proposes to apply eleven routine uses to FRTIB-23.

Dharmesh Vashee,

General Counsel and Senior Agency Official for Privacy.

SYSTEM NAME AND NUMBER: FRTIB-23, Insider Threat Program Records.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are located at the Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002. Records may also be maintained at the business offices of third-party service providers. Records may also be maintained at additional locations for Business Continuity purposes.

SYSTEM MANAGER: Insider Threat Program Manager, Federal Retirement Thrift Investment Board, 77 K Street NE, Suite 1000, Washington, DC 20002, (202) 942-1600.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 8474; 44 U.S.C. Chapter 35; 44 U.S.C. 3101.

PURPOSE(S) OF THE SYSTEM: FRTIB's Insider Threat Program is being implemented to prevent, detect, and mitigate the effects of insider threats, defined as, "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."

The Insider Threat Program system of records is being established to manage insider threat matters; facilitate insider threat activities, inquiries, and investigations; identify insider threats to FRTIB facilities, information, and information systems; track referrals of potential insider threats from FRTIB's hotline; and to track referrals of potential insider threats to internal and external partners.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system collects information on current or former FRTIB employees, contractors, subcontractors,

or any other individuals who have or have previously had authorized access to FRTIB facilities, information, or information systems.

CATEGORIES OF RECORDS IN THE SYSTEM: The categories of records compiled for each insider threat report, inquiry, or investigation may vary significantly based on the nature of each actual or potential insider threat incident.

Categories of records in the Insider Threat Program system of records may include name; social security number; date of birth; place of birth; personal and business email address; personal and business phone number; work history; background investigation information (including any information derived from SF-85, SF-85P, and SF-86 forms and background investigation processes); user ID; user activity performed on FRTIB devices; correspondence sent or received on an FRTIB device or network; personnel records (including disciplinary records and performance records); records of access to FRTIB facilities; records of security violations; reports from FRTIB's hotline for fraud, waste, abuse, and other misconduct; and law enforcement referrals.

RECORD SOURCE CATEGORIES: To monitor, identify, and respond to potential insider threats, information in the system will be received on an as-needed basis depending on the nature of the inquiry or investigation from: FRTIB employees, contractors, vendors, or other individuals with access to FRTIB facilities, information, or information systems; FRTIB's hotline for reporting fraud, waste, abuse, and other misconduct; information collected through user activity monitoring; officials from other foreign, federal, tribal, state, and local government agencies and organizations; non-government, commercial, public, and private agencies and organizations; and from relevant records, including information security databases and files; personnel security databases and files; FRTIB human resources databases and files; access records for FRTIB facilities; FRTIB contractor files; FRTIB's Office of Technology Services; FRTIB telephone usage records; federal, state, tribal, territorial, and local law

enforcement and investigatory records; other Federal agencies; and publicly available information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(b); and:

1. Routine Use – Audit: A record from this system of records may be disclosed to an agency, organization, or individual for the purpose of performing an audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FRTIB officers and employees.
2. Routine Use – Breach Mitigation and Notification: Response to Breach of FRTIB Records: A record from this system of records may be disclosed to appropriate agencies, entities, and persons when (1) FRTIB suspects or has confirmed that there has been a breach of the system of records; (2) FRTIB has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, FRTIB (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FRTIB's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
3. Routine Use – Response to Breach of Other Records: A record from this system of records may be disclosed to another Federal agency or Federal entity, when

FRTIB determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) 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.

4. Routine Use – Congressional Inquiries: A record from this system of records may be disclosed to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.
5. Routine Use – Contractors, et al.: A record from this system of records may be disclosed to contractors, grantees, experts, consultants, the agents thereof, and others performing or working on a contract, service, grant, cooperative agreement, interagency agreement, or other assignment for FRTIB, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FRTIB officers and employees.
6. Routine Use – Third-Party Service Providers: A record from this system of records may be disclosed to third-party service providers, including other government agencies, such as the Department of Justice, that provide support for FRTIB's Insider Threat Program under a contract or interagency agreement.
7. Routine Use – Disclosure to Law Enforcement: Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature – the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law

enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

8. Routine Use – Litigation, DOJ or Outside Counsel: A record from this system of records may be disclosed to the Department of Justice, FRTIB's outside counsel, other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (1) FRTIB, or (2) any employee of FRTIB in his or her official capacity, or (3) any employee of FRTIB in his or her individual capacity where DOJ or FRTIB has agreed to represent the employee, or (4) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and FRTIB determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which FRTIB collected the records.
9. Routine Use – Litigation, Opposing Counsel: A record from this system of records may be disclosed to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena.
10. Routine Use – NARA/Records Management: A record from this system of records may be disclosed to the National Archives and Records Administration (NARA) or other Federal Government agencies pursuant to the Federal Records Act.
11. Routine Use – Insider Threat Community of Practice: A record from this system of records may be disclosed to any Federal agency or group of agencies with responsibilities for activities related to counterintelligence or the detection of insider threats.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in paper and electronic form, including on computer databases and cloud-based services, all of which are securely stored.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name, phone number, case number, or internal FRTIB identification (including FRTIB email, username, etc.).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records are maintained in accordance with General Records Schedule 5.6 (Security Records), Items 210 through 240, issued by the National Archives and Records Administration (NARA).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: FRTIB has adopted appropriate administrative, technical, and physical controls in accordance with FRTIB's security program to protect the security, confidentiality, availability, and integrity of the information and to ensure that records are not disclosed to or accessed by unauthorized individuals. Access to the records in this system is limited to individuals who have the appropriate permissions and who have a need to know the information in order to perform their official duties.

RECORD ACCESS PROCEDURES: Individuals seeking to access records within this system must submit a request pursuant to 5 CFR part 1630. Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual, such as a Power of Attorney, in order for the representative to act on their behalf.

CONTESTING RECORD PROCEDURES: See Record Access Procedures above.

NOTIFICATION PROCEDURES: See Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Records in this system will be exempt, based on 5 U.S.C. 552a(k)(2), from the requirements in subsections (c)(3),

(d)(1)-(4), (e)(1), (e)(4)(G)-(I), and (f) of the Privacy Act. The Agency has promulgated regulations implementing the Privacy Act at 5 CFR 1632.15 that establish this exemption.

HISTORY: None.

[FR Doc. 2021-16016 Filed: 7/27/2021 8:45 am; Publication Date: 7/28/2021]