FEDERAL RETIREMENT THRIFT INVESTMENT BOARD

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 investigate and prevent potential intrusions into FRTIB network boundaries, to investigate and prevent misuse of information within FRTIB's network boundaries, and to investigate and prevent the compromise or misuse of FRTIB information.

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 *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 *FEDERAL REGISTER*]**.

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

- *Federal eRulemaking Portal: https://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: Megan Grumbine, 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 system 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-22, Cybersecurity Investigation Records." The Agency employs a variety of network monitoring tools and security tools to protect the Agency's networks, systems, and data. The records contained in this system are used to investigate and prevent potential intrusions into FRTIB network boundaries, to investigate and prevent misuse of information within FRTIB's network boundaries, and to investigate and prevent the compromise or misuse of FRTIB information. This system of records is required to protect FRTIB information from unauthorized access, use, modification, disclosure, or destruction and to comply with the requirements of the Federal Information Security Modernization Act (FISMA).

FRTIB proposes to apply thirteen routine uses to FRTIB-22.

Megan Grumbine,

General Counsel and Senior Agency Official for Privacy.

SYSTEM NAME AND NUMBER:

FRTIB-22, Cybersecurity Investigation 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 kept at an additional location for Business Continuity purposes.

SYSTEM MANAGER:

Chief Technology Officer, 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; and 44 U.S.C. 3101.

PURPOSES OF THE SYSTEM:

The records in this system of records are used to investigate and prevent potential intrusions into FRTIB network boundaries, to investigate and prevent misuse of information within FRTIB's network boundaries, and to investigate and prevent the compromise or misuse of FRTIB information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system of records contains information on Thrift Savings Plan (TSP) participants and beneficiaries, FRTIB employees, FRTIB contractors, and any third party individuals with access to FRTIB systems, networks, computers, or data, or those have been alleged to have accessed or attempted to access FRTIB systems, networks, computers, or data without authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system include: first and last name, telephone number, username, e-mail address, media access control (MAC) address, internet protocol (IP) address, and network traffic data, and logs. Because network monitoring tools and security tools are used to analyze email and network traffic and to monitor user activity on FRTIB's network, these tools can capture a variety of data types including but not limited to: name; social security number; TSP account number; date of birth; address; email address; and financial information.

RECORD SOURCE CATEGORIES:

Records are provided by the Agency's network monitoring tools and the Agency's security tools. The network monitoring tools inspect incoming and outgoing network traffic and include the Agency's data loss prevention (DLP) capabilities. The security tools analyze user activity within the FRTIB network and include the Agency's security information and event management tool.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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, 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 – Investigations, Third Parties: A record from this system of records may be disclosed to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the third party officer making the disclosure.
7. Routine Use – Investigations, Other Agencies: A record from this system of records may be disclosed to appropriate Federal, state, local, tribal, or foreign government agencies or multilateral governmental organizations for the purpose of investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where FRTIB determines that the information would assist in the enforcement of civil or criminal laws.
8. Routine Use – Law Enforcement Intelligence: A record from this system of records may be disclosed to a Federal, state, tribal, local, or foreign government agency or organization, or international organization, lawfully engaged in

collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

9. Routine Use – Law Enforcement Referrals: A record from this system of records may be disclosed to an appropriate Federal, state, tribal, local, international, or foreign agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.
10. 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.

11. 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.
12. 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.
13. Routine Use – Security Threat: A record from this system of records may be disclosed to Federal and foreign government intelligence or counterterrorism agencies when FRTIB reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when FRTIB reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in 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, e-mail address, log identification number, internet protocol (IP) address, media access control (MAC) address, or FRTIB username.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

These records are maintained in accordance with General Records Schedule 3.1 (General Technology Management Records), items 11 or 20 or GRS 3.2 (Information System Security Records) item 10, 30, and 31 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. Electronic records are stored on computer systems and protected by role-based access to users with passwords set by authorized users that must be changed periodically.

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 Power of Attorney, in order for the representative to act on their behalf.

CONTESTING RECORDS PROCEDURES:

See Record Access Procedures above.

NOTIFICATION PROCEDURES:

See Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2020-18271 Filed: 8/21/2020 8:45 am; Publication Date: 8/24/2020]