4810-AK-P

DEPARTMENT OF THE TREASURY

Privacy Act of 1974; System of Records

AGENCY: Internal Revenue Service, Department of the Treasury.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended (Privacy Act), the Department of the Treasury, Internal Revenue Service (IRS), proposes to establish a new system of records entitled, "Treasury/IRS 34.018, Insider Risk Management Records," within its inventory of records systems subject to the Privacy Act. The IRS will use this system to identify potential threats to IRS resources and information assets and facilitate management of insider threat investigations, complaints, inquiries, and counterintelligence threat detection activities. An "insider" is defined to include current and former employees, contractors, interns, visitors, and any other individuals who have or who had persistent authorized access to IRS assets including any IRS facility, information, equipment, network, or system. An "insider threat" is the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the IRS mission, resources, personnel, facilities, information, equipment, networks, or systems.

DATES: Comments must be received no later than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system of records will be effective upon publication in the Federal Register unless the IRS receives comments which would result in a contrary determination. The routine uses will be effective on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE REGSTER]. The IRS invites written comments on the routine uses and other aspects of this system of records prior to the proposed effective date.

ADDRESSES: Comments may be submitted to the Federal eRulemaking Portal electronically at *http://www.regulations.gov* identified by docket number TREAS-DO-2024-0003. Comments can also be sent to the Deputy Assistant Secretary for Privacy, Transparency, and Records, Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington, DC 20220, Attention:

New Privacy Act Systems of Records. All comments received, including attachments and other supporting documents, are part of the public record and subject to public disclosure. All comments received will be posted without change to *www.regulations.gov*, including any personal information provided. You should submit only information that you wish to make publicly available.

FOR FURTHER INFORMATION CONTACT: Kathleen Walters, Chief Risk Officer, Internal Revenue Service, Office of the Chief Risk Officer, Enterprise Risk Management, 1111 Constitution Ave NW, Washington, DC 20224-0002; enterprise.risk.mgt@irs.gov, telephone: (801) 612-4815.

SUPPLEMENTARY INFORMATION: The IRS has long-standing processes, controls, and systems in place to meet legal and regulatory guidance to protect agency assets including personnel, facilities, information systems, equipment, and data. To better protect these resources, the Department of Treasury established an Insider Risk Management Office, under Treasury Directive 15-70, to implement and maintain a holistic, proactive, and risk-based program to effectively deter, detect, and mitigate the risks associated with insider actions or behaviors, while protecting the privacy and civil liberties of insiders through supporting policies, procedures, and standards. The IRS established a subordinate Insider Risk Management Program, which consists of a Program Management Office, Executive Steering Committee and Working Group governance boards, and coordinated Insider Risk Management incident response operations. The Insider Risk Management program collaborates with business unit representatives to perform a comprehensive risk assessment, aiding business units in their risk prioritization efforts.

This established system will be included in Treasury's inventory of record systems. Below is the description of the Treasury/IRS 34.018, Insider Risk Management Records System of Records.

Treasury has provided a report of this system of records to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget (OMB), pursuant to 5 U.S.C. 552a(r) and OMB Circular A-108, "Federal Agency Responsibilities for Review,

Reporting, and Publication under the Privacy Act," dated December 23, 2016.

The system of records entitled "Treasury/IRS 34.018, Insider Risk Management Records" is published in its entirety below.

Dated: February 13, 2024.

Ryan Law,

Deputy Assistant Secretary for Privacy, Transparency, and Records.

SYSTEM NAME AND NUMBER:

Insider Risk Management Records. Treasury/IRS 34.018.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Enterprise Risk Management, Internal Revenue Service, 1111 Constitution Ave NW, Washington, DC 20224-0002.

SYSTEM MANAGER(S):

Chief Risk Officer, Internal Revenue Service, 1111 Constitution Ave NW, Washington, DC 20224-0002.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulations; 26 U.S.C. 7801, Authority of Department of the Treasury; 26 U.S.C 7803, Commissioner of Internal Revenue, other officials; 18 U.S.C. 1030(a)(2)(B), Fraud and Related Activity in Connection with Computers; 44 U.S.C. 3101, Records Management by Agency Heads; General Duties; 44 U.S.C. 3551 to 3558, Federal Information Security Modernization Act of 2014; 28 U.S.C 535, Investigation of Crimes Involving Government Officers and Employees; Limitations; Treasury Order 105-20: Insider Threat Program; Treasury

Order 105-22: Delegation of Authorities Concerning the Treasury Operations Security Program; Treasury Directive 15-70: Delegation of Treasury Counterintelligence and Insider Threat Functions and Programs.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to maintain, analyze, and process records about insider risks to support holistic security analysis, case management, and incident response activities in the administration of the IRS Insider Risk Management Program.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Current and former employees, contractors, interns, visitors, and any other individuals who have or who had persistent authorized access to IRS assets including any IRS facility, information, equipment, network, or system.

(2) Individuals who are, or have been, temporarily authorized to perform, provide, or use services in IRS facilities (either on an ongoing or occasional basis), including, but not limited to, visitors, security personnel, custodial staff, maintenance workers, food service workers, employee assistance program staff, and other non-IRS employees with access to IRS assets; witnesses and other individuals who provide statements or information to the IRS related to an insider threat inquiry.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records about individuals reported to exhibit behaviors requiring analysis and consideration by Holistic Insider Risk Management's Hub Operations team as a result of exceeded risk tolerance; IRS security investigations, including authorized IT Security, Physical Security, and Personnel Security risk scoring; information systems security analysis and logs; determinations derived from information obtained in other systems; information potentially relevant to conducting insider risk management. These records include the results of the analysis and explanations of any responsive actions.

RECORDS SOURCE CATEGORIES:

IRS internal personnel and security records, external law enforcement agencies, Federal Counterintelligence and Security agencies, third party witnesses, public and social media, complainants, and informants.

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

Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. Material covered by rule 6(e) of the Federal Rules of Criminal Procedure may be disclosed only as permitted by that rule. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which the IRS collected the records, and no privilege is asserted.

(1) Disclose information to the Department of Justice (DOJ) when seeking legal advice or for use in any proceeding, or in preparation for any proceeding, when: (a) The IRS or any component thereof; (b) any IRS employee in their official capacity; (c) any IRS employee in their individual capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS determines that the records are relevant and necessary to the proceeding or advice sought.

(2) Disclose information in a proceeding (including discovery) before a court, administrative tribunal, or other adjudicative body when: (a) the IRS or any component thereof; (b) any IRS employee in their official capacity; (c) any IRS employee in their personal capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS or DOJ determines that the information is relevant and necessary to the proceeding. Information may be disclosed to the adjudicative body to resolve issues of relevancy, necessity, or privilege pertaining to the information.

(3) Disclose information to an appropriate Federal, state, local, tribal, or foreign agency, or other public authority, responsible for implementing or enforcing, or for investigating or

prosecuting the violation of, a statute, rule, regulation, order, or license, when a record on its face, or in conjunction with other records, indicates a potential violation of law or regulation and the information disclosed is relevant to any regulatory, enforcement, investigative, or prosecutorial responsibility of the receiving authority.

(4) Disclose information to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation.

(5) Disclose information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

(6) Disclose information to a contractor or service provider, including an expert witness or a consultant, hired by the IRS, to the extent necessary for the performance of a contract.

(7) Disclose information to the news media as described in the IRS Policy Statement 11-94 (formerly P–1–183), News Coverage to Advance Deterrent Value of Enforcement Activities Encouraged, IRM 1.2.1.11.9.

(8) Disclose information to professional organizations or associations with which individuals covered by this system of records may be affiliated, such as state bar disciplinary authorities, to meet their responsibilities in connection with the administration and maintenance of standards of conduct and discipline.

(9) Disclose information to a Federal, state, local, or tribal agency, or other public authority, which has requested information relevant or necessary to hiring or retaining an employee, or issuing or continuing a security clearance, license, contract, grant or other benefit.

(10) To appropriate agencies, entities, and persons when (1) the Department of the Treasury or IRS suspects or has confirmed that there has been a breach of the system of records; (2) the Department of the Treasury or IRS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of the Treasury and/or Treasury bureau(s) (including 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 the Department of the Treasury's or IRS efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm;

(11) To another Federal agency or Federal entity, when the Department of the Treasury or IRS 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 information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper records and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By name, Social Security Number (SSN), access/security badge number, obfuscated system-generated identifier and other electronic identification numbers, date of birth, phone number, and other unique individual identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained in accordance with IRM 1.15, Records and Information Management (also see Documents 12829 and 12990).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Role based access controls are not less than those published in IRM 10.8, Information Technology (IT) Security, IRM 10.2, Physical Security Program, and IRM 10.5, Privacy and Information Protection.

RECORDS ACCESS PROCEDURES:

See “Notification Procedures” below.

CONTESTING RECORDS PROCEDURES:

See “Notification Procedures” below.

NOTIFICATION PROCEDURES:

This system may not be accessed for purposes of determining whether the system contains a record pertaining to a particular individual; the records are exempt under 5 U.S.C. 552a(k)(2) and (k)(5).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Records maintained in this system haves been designated exempt from sections (c)(3), (d), (e)(1), (e)(4)(G)–(I), and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(2) and (k)(5) (See 31 CFR 1.36).

HISTORY:

None.

[FR Doc. 2024-09698 Filed: 5/2/2024 8:45 am; Publication Date: 5/3/2024]