DEPARTM

Internal Revenue Service

Privacy Act of 1974; Matching Program

AGENCY: Department of the Treasury, Internal Revenue Service.

ACTION: Notice of a new matching program.

SUMMARY: Pursuant to section 552a(e)(12) of the Privacy Act of 1974, as amended, and the Office of Management and Budget (OMB) *Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, notice is hereby given of the conduct of the Internal Revenue Service (IRS) Insider Risk Management (InRM) Computer Matching Program.

DATES: Comments on this matching notice must be received no later than 30 days after date of publication in the Federal Register. If no public comments are received during the period allowed for comment, the agreement will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], provided it is a minimum of 30 days after the publication date.

Beginning and completion dates: The matches will be conducted on an ongoing basis in accordance with the terms of the computer matching agreement in effect with the IRS as approved by the applicable Data Integrity Board. The term of this agreement is expected to cover the 18-month period, September 30, 2025, through March 31, 2027. Ninety days prior to expiration of the agreement, the parties to the agreement may request a 12-month extension in accordance with 5 U.S.C. 552a(o).

ADDRESSES: Comments may be sent by email to FOIA@treasury.gov, or by mail to the Office of Privacy, Governmental Liaison and Disclosure, Internal Revenue Service, 1111 Constitution Avenue, N.W. Washington, DC 20224.

FOR FURTHER INFORMATION CONTACT: John Davis, Management and Program Analyst, IRS Privacy, Governmental Liaison and Disclosure, 303-603-4733 (not a toll-free number)

SUPPLEMENTARY INFORMATION: The InRM program involves a computer matching program, including a computer matching agreement (CMA), established to assist the IRS in furthering the purposes of the InRM program.

PARTICIPATING AGENCIES: Department of the Treasury, IRS, and The Treasury Inspector General for Tax Administration.

AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM:

Executive Order 13587, "Structural Reforms to Improve the Security of Classified 2 Networks and the Responsible Sharing and Safeguarding of Classified Information, and its implementing policies and standards such as National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" requires agencies to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties as required by the Internal Revenue Code, the Privacy Act of 1974, the Bank Secrecy Act, Title 18 of the United States Code, the Federal Information Security Modernization Act (FISMA), and other applicable laws that require safeguarding of information.

PURPOSE(S): This matching program will assist the IRS in deterring, detecting, and mitigating insider threats to the IRS's information, resources, and personnel.

The purpose of this program is to detect, deter and mitigate breaches of security policy by IRS employees, contractors, or other individuals who wittingly or unwittingly engage in activities that threaten harm to the security of the United States. These threats can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

CATEGORIES OF INDIVIDUALS: Current and former employees, contractors, interns, visitors. 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, 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 inquiry.

CATEGORIES OF RECORDS: Information relevant, or potentially relevant, to identifying, preventing, or mitigating insider risk to IRS resources, including potential risk indicators (PRIs) about or related to individuals reported to exhibit behaviors requiring analysis and consideration by Holistic Insider Risk Management's Hub Operations Team as a result of exceeding risk tolerance, including records of the results of the analysis and explanations of any responsive actions; IRS security investigations, including authorized IT Security, Physical Security, and Personnel Security risk scoring; information systems security analysis and logs; and determinations derived from information obtained in other systems. Data used in this match from the listed systems of records includes, but is not limited to, employee name, Social Security Number (SSN), employee number, address, email addresses; employee spouse's name, SSN, address; taxpayer name, Taxpayer Identification Number (TIN), address, tax return/account information, credit card or bank account information, taxpayer entity information, including prior and current name; electronic transmission specifics, including sender’s email address, recipients’ email addresses, recipients’ internet service providers, transmission date and time, internet protocol (IP) address, computer machine name, and terminal identification.

SYSTEM(S) OF RECORDS: The following systems of records maintained by the IRS and the Department of the Treasury Offices may be utilized:

01. Treasury/IRS 22.054 Subsidiary Accounting Files
02. Treasury/IRS 22.060 Automated Non-Master File
03. Treasury/IRS 22.061 Information Return Master File (IRMF)

04. Treasury/IRS 24.030 Customer Account Data Engine Individual Master File

05. Treasury/IRS 24.046 Customer Account Data Engine Business Master File

06. Treasury/IRS 26.019 Taxpayer Delinquent Account Files

07. Treasury/IRS 34.016 Security Clearance Files

08. Treasury/IRS 34.018 Insider Risk Management Records

09. Treasury/IRS 34.021 Personnel Security Investigations

10. Treasury/IRS 34.022 Automated Background Investigations System (ABIS)

11. Treasury/IRS 34.037 Audit Trail and Security Records

12. Treasury/IRS 35.001 Reasonable Accommodation Request Records

13. Treasury/IRS 36.001 Appeals, Grievances and Complaints Records

14. Treasury/IRS 36.003 General Personnel and Payroll Records

15. Treasury/IRS 42.001 Examination Administrative Files

16. Treasury/IRS 48.001 Disclosure Records

17. Treasury/DO .311 Treasury Inspector General for Tax Administration (TIGTA) Office of Investigation Files

18. Treasury/DO .411 Intelligence Enterprise Files

19. Treasury .015 General Information Technology Access Account Records

20. Treasury .020 Health Screening and Contact Tracing Records

Ryan Law,

Deputy Assistant Secretary for Privacy, Transparency, and Records.

[FR Doc. 2025-18880 Filed: 9/26/2025 8:45 am; Publication Date: 9/29/2025]