Department of the Treasury

Internal Revenue Service

Privacy Act of 1974

AGENCY: Internal Revenue Service, Treasury

ACTION: IRS notice of its intent to match computerized data to detect sensitive but unclassified (SBU) information that is being transmitted in violation of IRS security policy that requires an adequate level of encryption.

SUMMARY: The IRS will review detections of potential violations to determine whether there has been an actual violation of security policy. This review may include matching data from existing IRS systems of records such as:

I. Treasury Payroll and Personnel System [Treasury/DO.001]

II. Subsidiary Accounting Files [Treasury/IRS 22.054]

III. Automated Non-Master File (ANMF) [Treasury/IRS 22.060]

IV. Information Return Master File (IRMF) [Treasury/IRS 22.061]

V. CADE Individual Master File (IMF) [Treasury/IRS 24.030]

VI. CADE Business Master File (BMF) [Treasury/IRS 24.046]

VII. Audit Trail and Security Records [Treasury/IRS 34.037]

VIII. General Personnel and Payroll Records [Treasury/IRS 36.003]

This review may include using date elements such as:

I. Employee Name, Social Security Number (SSN), Employee Identification Number (SEID), Address, Email Addresses

II. Employee Spouse's Name, SSN, Address

III. Taxpayer Entity Information, including prior and current name, Taxpayer Identification Number (TIN), Address, Tax Return/Account Information

IV. Electronic transmission specifics such as sender's email address, recipient's email address, recipient's internet service provider, transmission date and time, "IP Address", computer machine name, terminal identification

REPORTING: A report describing this proposed matching agreement has been provided to the Office of Management and Budget (OMB) and the Congressional committees responsible for oversight of the Privacy Act in accordance with the Privacy Act of 1974, OMB Guidelines on the Conduct of Matching Programs (54 FR 25818, June 19, 1989), OMB Bulletin 89-22, "Instructions on Reporting Computer Matching Programs to the Office of Management and Budget (OMB), Congress and the Public," and OMB Circular No. A-130, (rev. Nov. 28, 2000), "Management of Federal Information Resources."

NOTICE PROCEDURES: IRS employees, contractors, and other individuals who have been granted access to IRS information, or to IRS equipment and resources, are notified regularly that their computer activity is monitored. A notice describing Treasury/IRS 34.037 was most recently published at volume 77, number 155 (Friday, August 10, 2012).

SECURITY: All information obtained and/or generated as part of the IRS computer matching program will be safeguarded in accordance with the provisions of: 5 U.S.C. § 552a, 26 U.S.C. § 6103, as well as IRS record safeguarding requirements which conform with Treasury Directive (TD) 80-05, Records and Information Management, and TD P 71-10, Department of the Treasury Security Manual, and are no less restrictive than the standards prescribed in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. Matches under this agreement will comply with the standards of OMB Policy M-06-16,

Protection of Sensitive Agency Information, requiring that sensitive information, including all Personally Identifiable Information be protected at all times.

RECORDS USAGE, DUPLICATION AND DISCLOSURE: The information generated and/or obtained during these computer matches will be used by IRS employees in the performance of their official responsibilities. Access to this information is limited to those individuals who have a need to know the information in the performance of their official duties and to those who are authorized access by disclosure provisions in applicable law. These individuals are subject to criminal and civil penalties for the unauthorized inspection and/or disclosure of this information. During the execution of this program of computer matches and the resultant analyses or investigations, the records used may be duplicated by IRS employees only for use in performing their official duties. The information collected or generated as part of this program of computer matches may only be disclosed in accordance with the provisions of 5 U.S.C. § 552a, 26 U.S.C. § 6103, and any other applicable Federal privacy provisions.

LEGAL AND REGULATORY AUTHORITY: The Internal Revenue Service has responsibilities to follow safeguarding requirements to ensure that information is kept confidential 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 Management Act (FISMA), and other applicable laws that require safeguarding of information. Confidential information that is sent without sufficient protection is in violation of IRS security policy. This matching program will assist the IRS in ensuring that sensitive information is properly protected from unauthorized use or disclosure.

DATES: Comments must be received no later than [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. The proposed matching program will

become effective [INSERT DATE 40 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER], unless the IRS receives comments which cause reconsideration of this action.

ADDRESSES: Comments should be sent to the Office of Privacy, Governmental Liaison and Disclosure, Internal Revenue Service, 1111 Constitution Avenue, NW, Washington, DC 20224. Comments will be available for inspection and copying in the IRS Freedom of Information Reading Room (Room 1621) at the above address. The Telephone number for the Reading Room is (202) 622-5164 (not a toll-free number).

FOR FURTHER INFORMATION CONTACT: David Silverman, Management and Program Analyst, IRS Office of Privacy, Governmental Liaison and Disclosure, (202) 622-5625 (not a toll-free number).

Dated: March 15, 2013

_____

Veronica Marco,

Acting Deputy Assistant Secretary for Privacy, Transparency, and Records

Billing Code: 4830-01-P

[FR Doc. 2013-06448 Filed 03/20/2013 at 8:45 am; Publication Date: 03/21/2013]