

---

**A. SYSTEM DESCRIPTION**

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10-Privacy Accountability and #21-Privacy Risk Management

---

Date of Submission: Mar 28 2012

PIA ID Number: 155

---

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Specialist Referral System, SRS-2

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

---

4. Responsible Parties:

---

N/A

---

5. General Business Purpose of System

---

SRS-2 is a web-based, client server application that is accessed through the IRS intranet. It allows IRS employees to enter referrals to request the assistance of a specialist to assist with the examination of a tax return. Referrals are sent to a Specialist Manager who accepts or rejects the referral. If a referral is accepted it is assigned to a specialist to assist with the examination. The SRS-2 application automates the referral process for Large Business & International (LB&I), Small Business/Self-Employed (SB/SE), Wage & Investment (W&I), and Tax Exempt and Government Entities (TE/GE) examiners. SRS-2 users are authenticated through the IRS local area network (LAN) in order to access the SRS-2 application. There are approximately 35,000 users, IRS wide, who can access the application via the IRS Intranet. Using the SRS-2, a user can generate referrals for the following specialists: • Art Appraisers • Computer Audit Specialists (CAS) • Economists • Employee Plans (TE/GE) • Employment Taxes (LB&I, SB/SE and TE/GE) • Engineering • Estate & Gift • Excise Tax (Fuel) • Excise Tax (General) • Exempt Organizations • Federal, State and Local Governments • Financial Products Specialist • Indian Tribal Governments • International Business Compliance • Joint Committee • LB&I Actuary • Tax Computation Specialists • Tax Exempt Bonds • TEFRA Coordinators The privacy/taxpayer data stored within the SRS-2 application is: • Taxpayer Name • Taxpayer Identification Number (TIN) • Address • Years under audit • Activity code of taxpayer • Earliest statute date of taxpayer SRS-2 also contains information about users. Employee information that it contains includes: • Standard Employee Identifier (SEID) • Employee Business Unit • Manager/Requestor Name • Manager/Requestor Email address • Manager/Requestor Phone Number • Treasury Integrated Management Information System (TIMIS) Code In addition, an Application Administrator is assigned to maintain the routing tables, which contain the specialist manager geographic locations within each business unit.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 05/05/2009

---

6b. If Yes, please indicate which of the following changes occurred to require this update.

• System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No

• System is undergoing Security Assessment and Authorization Yes

---

6c. State any changes that have occurred to the system since the last PIA

New hardware and servers. Reports functionality has been removed

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-00-02--00-01-5201-00

**B. DATA CATEGORIZATION**

Authority: OMB M 03-22 & PVR #23-PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes  
Employees/Personnel/HR Systems Yes

Other Source:

Other No

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

| TYPE OF PII                  | Collected? | On Public? | On IRS Employees or Contractors? |
|------------------------------|------------|------------|----------------------------------|
| Name                         | Yes        | Yes        | No                               |
| Social Security Number (SSN) | Yes        | No         | No                               |
| Tax Payer ID Number (TIN)    | Yes        | No         | No                               |
| Address                      | Yes        | No         | No                               |
| Date of Birth                | No         | No         | No                               |

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

SRS-2 contains PII data from the following: Taxpayers, Employees, and Audit Trail Information. The privacy/taxpayer data stored within the SRS-2 application is: • Taxpayer Name • Taxpayer Identification Number (TIN) • Address • Years under audit • Activity code of taxpayer • Earliest statute date of taxpayer SRS-2 also contains information about users. Employee information that it contains includes: • Standard Employee Identifier (SEID) • Employee Business Unit • Manager/Requestor Name • Manager/Requestor Email address • Manager/Requestor Phone Number • TIMIS Code

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

Title 26 USC (United States Code) 6109. Section 7801 and 7803 of the Internal Revenue Code

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

IRS and Congress have not provided for an alternative means to identify taxpayers.

---

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

No strategy exists currently for the application.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

SEID, date/time stamp, type of event that occurred, sources of the event.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

| <u>System Name</u>   | <u>Current PIA?</u> | <u>PIA Approval Date</u> | <u>SA &amp; A?</u> | <u>Authorization Date</u> |
|--|---------------------|--------------------------|--------------------|---------------------------|
| Customer Authoritative Directory System (CADS – Part of MITS–17) | Yes                 | 02/19/2010               | Yes                | 09/24/2010                |

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: No If Yes, specify:

---

### C. PURPOSE OF COLLECTION

---

Authorities: OMB M 03–22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

Collection of PII data is required to automate the audit referral request process for LMSB, SBSE, W&I, and TEGE Field Specialists.

---

### D. PII USAGE

---

Authority: OMB M 03–22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration Yes

To provide taxpayer services No

To collect demographic data No

For employee purposes Yes

Other: No

If other, what is the use?

---

---

**E. INFORMATION DISSEMINATION**

---

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

|                               | Yes/No | Who? | ISA OR MOU**? |
|-------------------------------|--------|------|---------------|
| Other federal agency (-ies)   |        |      |               |
| State and local agency (-ies) |        |      |               |
| Third party sources           |        |      |               |
| Other:                        |        |      |               |

\*\* Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

|                    | YES/NO | AUTHORITY                          |
|--------------------|--------|------------------------------------|
| Persistent Cookies | _____  | _____                              |
| Web Beacons        | _____  | _____                              |
| Session Cookies    | _____  | _____                              |
| Other:             | _____  | <i>If other, specify:</i><br>_____ |

---

**F. INDIVIDUAL CONSENT**

---

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent \_\_\_\_\_  
Website Opt In or Out option \_\_\_\_\_  
Published System of Records Notice in the Federal Register \_\_\_\_\_  
Other: \_\_\_\_\_

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9–Privacy as Part of the Development Life Cycle, #11–Privacy Assurance, #12–Privacy Education and Training, #17–PII Data Quality, #20- Safeguards and #22–Security Measures

---

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

---

22. The following people have use of the system with the level of access specified:

|                                  | Yes/No     | Access Level |
|----------------------------------|------------|--------------|
| IRS Employees:                   | <u>Yes</u> |              |
| Users                            |            | _____        |
| Managers                         |            | _____        |
| System Administrators            |            | _____        |
| Developers                       |            | _____        |
| Contractors:                     | <u>No</u>  |              |
| Contractor Users                 |            | _____        |
| Contractor System Administrators |            | _____        |
| Contractor Developers            |            | _____        |
| Other:                           | <u>No</u>  | _____        |

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

---

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

On–Line 5081 (OL5081) is required for any person, with the exception of the Requester Group, requiring access to the data retrieval section of the application (Reports, Request approvals/routing/assignments) and administrative interface. The OL5081 is used to document access requests, modifications, and terminations for all types of users, including Application Administrators.

---

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

As the auditor enters the Specialist Referral Form, the TIN will be validated for length and format. Requestor and Manager information are derived from the Discovery Directory (mentioned in response to question 2) in real time. Specialist and Approving Manager Information are verified for accuracy and completeness by the SRS–2 Application Administrator.

---

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

---

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

SRS–2 recordkeeping copies of referred cases are approved for destruction 10 years after the close of the referred case (Job No. N1–58–09–73, approved 2–2–2010). This disposition authority also provides for the retention of system inputs, outputs and documentation. These disposition instructions will be published under IRM 1.15.23 Records Control Schedule for Tax Administration - Examination, Item 82 when next updated.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

---

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

SRS-2 utilizes Secured Socket Layer (SSL) for to protect the integrity of all transmitted information from the webpage. No information is transferred between SRS-2 and other applications.

**26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.**

SRS-2 relies upon MITS-30 GSS for the implementation of this control. The MITS-30 GSS protects SRS-2 data at rest as follows: Back Up Tapes: MITS-30 uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140-2 validated encryption. Application Servers: IRM 10.8.1.5.6 (12) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. The MITS-30 environment, in accordance with the IRM, has employed the following due diligence methods for protecting the SRS-2 PII data that resides on the servers:

- SRS-2 does not utilize any shares or shared drives.
- SRS-2 enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties.
- SRS-2 does not routinely print any documents. If required, printing is limited to the specific reason for printing any document.
- SRS-2 has had a risk assessment conducted. Security Assessment Services has previously completed a Security Impact Analysis and will conduct a new SIA as part of the current SA&A cycle.
- The SRS-2 SSP is being updated as part of the current SA&A to reflect the encryption utilized by MITS-30 environment to protect PII data.
- Physical security is an inherited control by SRS-2 at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

---

**27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII?** Yes

---

**28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.**

Continuous Monitoring (eCM) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

---

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy?** Not Applicable

---

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?**

---

**H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

---

**30. Are 10 or more records containing PII maintained/stored/transmitted through this system?** Yes

---

**31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address)** Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

**SORNS Number**

**SORNS Name**

- Treas/IRS 24.030 CADE Individual Master File
- Treas/IRS 24.046 CADE Business Master File
- Treas/IRS 26.019 Taxpayer Delinquent Accounts Files
- Treas/IRS 42.001 Examination Administrative File
- Treas/IRS 34.037 IRS Audit Trail and Security Records System

**Comments**

---

**I. ANALYSIS**

---

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

---

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

|   |           |
|---|-----------|
| Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated) | <u>No</u> |
| Provided viable alternatives to the use of PII within the system                  | <u>No</u> |
| New privacy measures have been considered/implemented                             | <u>No</u> |
| Other:  | <u>No</u> |

32a. If Yes to any of the above, please describe:

NA

[View other PIAs on IRS.gov](#)