NOTE: The following reflects the information entered in the PIAMS website.

## 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 Approval: November 20, 2014 PIA ID Number: **1044**

1. What type of system is this? New

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

Lead Management – Offset Reversal Leads, OSRL

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: | 100,000 - 1,000,000 |

**4. Responsible Parties:**

NA

**5. General Business Purpose of System**

The Lead Management - Offset Reversal Leads (OSRL) Program is part of the Return Integrity & Correspondence Services (RICS) under the purview of the Director of the Refund Integrity Correspondence, Wage and Investment (W&I). The OSRL program manages questionable federal tax refunds or offsets from the Office of Child Support Enforcement. Leads involve individual federal tax refunds. The OSRL database is primarily responsible for storing leads received from the Office of Child Support Enforcement. This allows standard users to monitor the inventory assigned to each tax examiner in order mitigate inventory receipts and closures. The following functionalities can be accessed through the OSRL database: storing lead records, searching records and editing existing lead information, managing department logistics and analyzing report statistics. RICS work is part of an overall revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. Due process is provided pursuant to 26 USC.

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*) No

6a. If **Yes**, please indicate the date the latest PIA was approved:

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)
- System is undergoing Security Assessment and Authorization

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

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'. None

## 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

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 | Yes | *Other Source:* Office of Child Support Enforcement |

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 | Yes |
| Social Security Number (SSN) | Yes | Yes | No |
| Tax Payer ID Number (TIN) | No | No | No |
| Address | No | No | No |
| Date of Birth | No | No | No |

**Additional Types of PII:** Yes

| PII Name | On Public? | On Employee? |
|---|---|---|
| Employee SEID | No | Yes |
| Employee IDRS ID Number | No | Yes |
| Last Updated by Field (Contains Employee SEIDs) | No | Yes |
| Taxpayer's State of Child Support | Yes | No |
| Taxpayer's DLN for STARS | Yes | No |
| Notes Field (May Contain Additional Taxpayer Info | Yes | No |

10a. What is the business purpose for collecting and using the SSN?

SSN required for research into leads involving questionable federal tax refunds or offsets from the Office of Child Support Enforcement. Leads involve individual federal tax refunds.

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.)

SSNs are permissible from Internal Revenue Code (IRC) 6109, “Identifying Numbers”, which requires individual taxpayers to include their SSNs on their income tax returns.

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

None.

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

None.

Describe the PII available in the system referred to in question 10 above.

PUBLIC PII INFORMATION: The database maintains lead data received from the Office of Child Support Enforcement. Each lead contains taxpayer's state, full name, SSN, DLN for STARS, and notes field. Notes field if a free form field that may contain additional information on the taxpayer. IRS PII INFORMATION: The database maintains for each employee: SEID, first name, last name, IDRS ID, and a last updated by field. The last updated by field will contain additional IRS SEIDS of employees associated with that lead as it goes through the research process.

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 <u>not</u> needed.

There is currently no audit trail for this database. The OSRL inventory is distributed to the Tax Examiners to work. The data maintained in the database is updated when assigned and closed. It is the intention to create an audit trail for these types of updates in the future.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? <u>No</u>

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

a. IRS files and databases: <u>No</u>

b. Other federal agency or agencies: <u>Yes</u>

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

Office of Child Support Enforcement.

c. State and local agency or agencies: <u>No</u>

d. Third party sources: <u>No</u>

e. Taxpayers (such as the 1040): <u>No</u>

f. Employees (such as the I-9): <u>No</u>

g. Other: <u>No</u> 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.

Return Integrity and Correspondence Service (RICS) work is part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The OSRL application is required to maintain PII in the database due to the types of lead cases it manages in order to have the ability to research the leads to detect improper activity by managing questionable federal tax refunds or offsets reported by the Office of Child Support Enforcement.

## 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 | No | |
| | | *If other, what is the use?* |
| Other: | Yes | Revenue Protection |

## 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

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 | | |
| | | *If other, specify:* |
| Other: | | |

## 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

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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 | No |
| Website Opt In or Out option | No |
| Published System of Records Notice in the Federal Register | Yes |
| Other: | No |

## 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: | Yes | |
| Users | | Read Write |
| Managers | | Read Write |
| System Administrators | | Read Write |
| Developers | | Read Write |
| Contractors: | No | |
| Contractor Users | | |
| Contractor System Administrators | | |
| Contractor Developers | | |
| Other: | No | |

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?

In order to obtain access to the OSRL database, all prospective users must adhere to the 5081 process. This procedure is used for controlling access, managing (create, modify, disable, delete) user accounts, and providing administrative rights to users. All requests are handled by the RICS Service Desk and stored for auditing purposes. All standard access requests must be authorized by the user's manager as well as an OSRL administrator. All approved database accounts will be logged in and authenticated through the Windows main frame. User level and access permissions are automatically configured to the database server.

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

The PII information maintained in the OSRL database is provided by external entities and RICS relies on the accuracy of the lead information from those sources. OSRL tax examiners research the lead information using existing IRS systems and approved programs to determine improper activity. Input of the data received is manually entered into the OSRL database. Assignment of OSRL inventory to tax examiners is also manually entered by managers/administrators. Accuracy and completeness of the data used to research the lead is inherited from the existing IRS systems.

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? No

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.

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.

The Offset Reversal Lead (OSRL) database is unscheduled. W&I will work with the IRS Records Office to draft a request for records disposition authority for approval by the National Archives and Records Administration (NARA). When approved, disposition instructions for OSRL inputs, outputs, master files data, and system documentation will be published in Records Control Schedule (RCS) Document 12990, likely under RCS 29 for Tax Administration - Wage and Investment. OSRL is a W&I inventory tracking database for external leads identified as questionable federal tax refunds or offsets from the Office of Child Support Enforcement involving individual federal tax refunds. W&I proposes OSRL data disposition instructions to destroy 3 years after case is closed. The data in the OSRL database will be backed up daily and weekly for purposes of restoration.

---

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

The system follows FIPS PUB 200 minimum security requirements for the appropriate security controls and requirements as described in NIST SP 800-53 Revision 3. The appropriate policy checkers, network checkers, security scans, and critical updates are maintained. The technical controls that the reporting database has in place are mainly inherited from the GS. The system administrator role includes: 1) Controlling remote access to the system; 2) Installing OS updates and patches; 3) Running system policy checker; 4) Ensuring the system configuration remains in compliance with the SQL server policy checker. The database administrator role includes: 1) Adding/Removing users to/from SQL server; 2) Assigning access levels to SQL server users; 3) Creating and maintaining database instances; 4) Running the SQL Server policy checker; 5) Ensuring the SQL Server configuration remains in compliance with the SQL server policy checker; 6) Backing up the data. All other administrative and technical controls are inherited by the GS. All RICS applications will be using databases housed on a SQL server using Windows authentication only. SQL Server authentication will be disabled on the SQL server to comply with IRM requirements. Database roles will be created for each database, and proper “least privilege” permissions will be assigned on all pertinent database objects (tables, stored procedures, views, etc…) to these roles. Rather than adding each application user as a login to the SQL server, we will create Local windows groups on the SQL server with appropriate names describing the application and access level within in the name (i.e., Contacts_Admin and Contacts_StdUser). These local windows groups will then be added as SQL logins and given only the permission to the database needed for the application. In addition, the local windows groups will then be placed in the corresponding database role. The security administrator, based on the 5081, will place the IRS user into the appropriate local windows groups, which has already been mapped to the appropriate access level on the SQL server.

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

Data At Rest: The database has been archived on a separate drive and a separate server in the event it needs refreshed. The server is maintained under the IRS GS and controls for "Protection of Information At Rest" which outlines the configurations for firewalls, gateways, intrusion detection/prevention systems, and filtering routers are inherited. Data In Flight or In Transition: The OSRL inventory database does not maintain any data in flight or in transition. SQL Server is setup to protect data. From a database level, we have enabled TDE (Transparent Data Encryption) will encrypt the entire database’s file contents. This means that if someone were to access the MDF, LDF or BAK files associated with that database, they would not be able to read the contents by restoring or attaching those files to their own SQL server. The majority of the protection for the data will be in the permission setup. The goal is to deny most permission to the actual tables in the database, and create stored procedures to perform the bulk of the data manipulation. For example, if I deny the DELETE permission on a table to a user, they will not be able to delete a record in that table, through an application or through SSMS. However, we can create a stored procedure that contains the code to DELETE a record, and then give EXECUTE permission on that stored procedure to that user. This provide the best level of security so that users MUST go through pre-defined methods of manipulating data.

---

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? No

---

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

GS Level: System/Intrusion Detection System (IPS/IDS) and Host Intrusion Detection System (HIDS). Monitoring Roles: SAs and DBAs assign initial identifications and passwords, security profiles, and other security characteristics of new users. Other tasks include changing security profiles for existing users, ensuring that user’s access or type of access is restricted to the minimum necessary to perform his/her job, and monitoring system integrity, protection levels, and security-related events. Additionally monitoring activities include running policy and network checkers and scans. System logs are maintained.

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)*? No

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.

| SORN Number | SORN Name |
|---|---|
| Treasury/IRS 34.037 | Audit Trail and Security Record System |
| Treasury/IRS 42.021 | Compliance Programs and Projects Files--Treasury/I |

## 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) | No |
| Provided viable alternatives to the use of PII within the system | No |
| New privacy measures have been considered/implemented | No |
| Other: | No |

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

NA