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: Sep 29 2014 11:36AM PIA ID Number: **1110**

1. What type of system is this? Non-Major System

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

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

Refund Hold Report, RHR

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:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The Delinquent Return Refund Hold Program (RHP) was created for taxpayers that file a return expecting a refund and have an existing tax delinquency. The RHP holds the taxpayers' refunds for up to 6 months, until the filing delinquency is settled. The Refund Hold Report generates weekly, identifying accounts that meet the refund hold criteria. Tax examiners resolve the issues faster, release refunds sooner, and generally reduce process time to 2 weeks or less. The report provides the Operation with the data necessary to administer the program. It is used to release refunds where delinquencies have been resolved, and to move taxpayer accounts to the appropriate treatment stream within the required 6 month time frame. The Operational users would have no way to identify the inventory without the report. 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*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 03/24/2006

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

Minimal updates to accommodate annual processes.

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'. NA

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

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Name Control, Tax Period	Yes	No
Name Control, Tax Period	Yes	No

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

The SSN is necessary to identify taxpayers who have been selected as Refund Hold Program inventory. The report provides IRS campus Operations with the means (the SSN) to identify and update the appropriate cases for the Refund Hold process or obtaining a return and releasing the refund when appropriate.

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.)

26 USC 6109 is the authority for SSNs in IRS systems. 26 USC 6109 requires inclusion of identifying numbers in returns, statements, or other documents for securing proper identification of persons required to make such returns, statements, or documents.

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

No alternative solution to the use of the SSN will be applied to this report. It is an internal list of TINs used to administer the Delinquent Return Refund Hold program at IRS.

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

There is no mitigations strategy or implementation date to mitigate or eliminate Social Security Numbers on this report.

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

Taxpayer: The Return Received Date, Taxpayer Identification Number (TIN), Name Control, Tax Period, IDRS control Action Date, IDRS control Status, IDRS control Category Code, IDRS control Activity, Freeze Codes, AIMS Status/Organization Code, Business Operating Division (BOD), Refund Hold Module Balance, Universal Location Code, Area Office Code, Collection Location Code, MFT, Plan Num, CAF (Centralized Authorization File) Indicator, Delinquent Year, Selection Code, Return Cycle, Namelines, Address, ACS (Automated Collection System) Indicator, Reason Code Cycle, Collection Service Center Code. Employee: The Collection Assignment (TSIGN) number and the IDRS control Assignee Number. Other: The Refund Hold Report does not contain information not collected from the taxpayer or the employee.

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.

Audit Trail Information: The system the application resides on collects the audit trail information. The data elements are obtained from the IMF Master File. The TIN and Return Received Date and Namelines and Addresses are collected from the return filed by the Taxpayer. The TSIGN and IDRS controls are collected from the employee. No Other Federal Agencies provide data for the application. No State or Local Agencies provide data for the application. No Other third party sources provide data for the application.

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

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:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
IMF	Yes	05/02/2014	Yes	11/15/2012

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): No

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.

The Delinquent Return Refund Hold Program (RHP) was created for taxpayers that file a return expecting a refund and have an existing tax delinquency. The RHP holds the taxpayers' refunds for up to 6 months, until the filing delinquency is settled. The Refund Hold Report generates weekly, identifying accounts that meet the refund hold criteria. Tax examiners resolve the issues faster, release refunds sooner, and generally reduce process time to 2 weeks or less. The report provides the Operation with the data necessary to administer the program. It is used to release refunds where delinquencies have been resolved, and to move taxpayer accounts to the appropriate treatment stream within the required 6 month time frame. The Operational users would have no way to identify the inventory without the report.

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:	No	

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		
		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

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:	Yes	
Users		Read Only
Managers		Read Only
System Administrators		Read Only
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?

Users, Managers, System Administrators, and the Programmer will have access to the data in the system. The developer has access to handle problems with missing tapes, problems during run, cleanup of log files, etc. Access to the data is determined by the manager based on a user’s position and need-to-know. The manager will request a user be added. They must fill out Form 5081, Information System User Registration/Change Request, to request access to the Control-D System where the data is displayed. The System Administrator determines to which group and menu the user will have access. A user’s access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

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

The IMF Master File is updated weekly. The data is generated weekly from the IMF Master File. This ensures the data is timely. Tax Examiners review the data for completeness and accuracy.

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.

Refund Hold Reports are scheduled under General Records Schedule (GRS) 20, item 5 as Extracted Information from IRS Master Files data scheduled as temporary under other approved, recordkeeping disposition authorities. Under GRS 20, item 5 Refund Hold Reports may be destroyed/deleted when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. The Refund Hold Reports are generated weekly and overlay/supersede the previous week's output.

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.

This is not a system. The report is generated weekly and overlays the previous week's output.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
The data is sorted by received date and placed in report format. The report is downloaded to Control-D. Data is retrievable by the Return Received Date, Taxpayer Identification Number (TIN), Name Control, Tax Period, IDRS control Action Date, IDRS control Status, IDRS control Category Code, IDRS control Activity, Freeze Codes, AIMS Status/Organization Code, Business Operating Division (BOD), Refund Hold Module Balance, Collection Assignment (TSIGN) number or the IDRS control Assignee Number. Users, Managers, System Administrators, and the Programmer will have access to the data in the system. The developer has access to handle problems with missing tapes, problems during run, cleanup of log files, etc. Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user be added. They must fill out Form 5081, Information System User Registration/Change Request, to request access to the Control-D System where the data is displayed. The System Administrator determines to which group and menu the user will have access. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

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

No user interface, security covered by Unisys GSS-23

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.

N/A, not FISMA reportable. Batch process with no user interface. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

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.

No SORN Records found.

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