
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Refund Hold Report, RHR

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Refund Hold Report, RHR #946

Next, enter the **date** of the most recent PIA. 10/17/2014

Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of PII

No Conversions

No Anonymous to Non-Anonymous

No Significant System Management Changes

No Significant Merging with Another System

No New Access by IRS employees or Members of the Public

No Addition of Commercial Data / Sources

No New Interagency Use

No Internal Flow or Collection

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

- No Vision & Strategy/Milestone 0
- No Project Initiation/Milestone 1
- No Domain Architecture/Milestone 2
- No Preliminary Design/Milestone 3
- No Detailed Design/Milestone 4A
- No System Development/Milestone 4B
- No System Deployment/Milestone 5
- Yes Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used. This is a data extract of taxpayer information for the Delinquent Return Refund Hold Program (RHP), and should not be confused with a system or application that is accessible by users with a login. It is not accessible by any individual. The extract results in a report that is made available on the Control-D WebAccess system. The 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. Headquarters (HQ) Collection uses the report to validate existing Master File programming, and make processing decisions on future inventory. The report provides HQ Collection with the data necessary to administer the program. The HQ Collection analyst users would have no way to identify the inventory without the report. Due process is provided pursuant to 26 USC.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)

No Employer Identification Number (EIN)

Yes Individual Taxpayer Identification Number (ITIN)

No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)

No Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers). There is no mitigation strategy to eliminate the use of SSN's for this data extract. The purpose of the data extract is to provide the PII necessary for Collection to administer the Delinquent Return RHP. The information is required for the research that is performed by HQ Collection analysts.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
No	Name	No	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
Yes	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system.

Taxpayer's name control IDRS Control Assignee Number

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)

Yes SSN for tax returns and return information is Internal Revenue Code Section 6109

No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

No PII for personnel administration is 5 USC

No PII about individuals for Bank Secrecy Act compliance 31 USC

No Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets these criteria. Be specific. The Delinquent Return RHP is systemically processed at the Individual Master File (IMF) level. The extract, and resulting report, stored on the Control-D WebAccess system is the tool used by Collection HQ to affect processing changes, validate programming, project inventory levels, and make future predictive work planning decisions. In times of low resources, and high inventory volumes, the report has been used to change the IMF tolerance level for case selection, resulting in lower inventory volumes. In 2017, the report was used to implement an executive processing decision to release refunds to taxpayers that were below a set tolerance level. SSNs, and tax years provided by the report were essential in achieving the necessary processing change.
8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. The data is pulled directly from IMF processing, which is the purpose of the extract. It is not a system or application. No determinations are made by this data extract. The extract is the reported data that results from IMF processing decisions that were made for Refund Hold processing. The extract is used to validate the IMF process for accuracy and timeliness, and completeness. The IMF is updated weekly. The data is generated weekly from the IMF. This ensures the data is timely.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 24.030 IMF

Treas/IRS 26.019 Taxpayer Delinquent Account (TDA) Files

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Individual Master File (IMF)	Yes	03/06/2017	Yes	11/14/2016

11b. Does the system receive SBU/PII from other federal agency or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No
14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No
- 17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources. Taxpayers are identified and selected by Master File because they have not filed past year returns. The Master File programming identifies and selects non-filers for tax administration purposes. Information is collected via a data extract of the taxpayer's account information on IMF. The taxpayer does not have access to the information source. It is not appropriate in this application and administration of the RHP to collect the IMF data directly from the individual.
18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No
- 18b. If no, why not? Individuals provided the information to IRS via their signed tax returns. The information is used solely by IRS for administration of a filing compliance program. It is not shared with other agencies.
19. How does the system or business process ensure due process regarding information access, correction and redress? Since this is not a system or application, there is no direct information access. Users access the reported data extract information using the Control-D WebAccess system. No actions are taken as a result of this data extract. All actions are taken by the Master File RHP process. The Control-D WebAccess system provides the necessary user access and security. The RHP, a Master File process, provides redress separately. Due process by the RHP is provided pursuant to 26 USC.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated). IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees?	<u>Yes</u>	
<u>IRS Employees?</u>	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read And Write

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Users, Managers, System Administrators, and the Programmer will have access to the extract data. The developer has access to handle problems with missing tapes, problems during run, cleanup of log files, etc. Reference to the system indicates the Developer has Read/Write access to the programs, but not the data or report. Users have access to the data or reports (PII) via the Control-D WebAccess system and its access and security requirements, but no access to the programs. 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 WebAccess 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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. RHRs are scheduled under General Records Schedule (GRS) 4.3, item 031 as Extracted Information from IRS Master Files data scheduled as temporary under other approved, recordkeeping disposition authorities. Under GRS 4.3, item 031 RHRs may be destroyed/deleted when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. The RHRs are generated weekly and overlay/supersede the previous week's output.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the systems audit trail. This is a 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. 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, Name Control, Tax Period, Integrated Data Retrieval System (IDRS) control Action Date, IDRS control Status, IDRS control Category Code, IDRS control Activity, Freeze Codes, Audit Information Management System Status/Organization Code, Business Operating Division, Refund Hold Module Balance, Collection Assignment (TSIGN) number or the IDRS control Assignee Number.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees:	<u>Not Applicable</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>100,000 to 1,000,000</u>
26d. Other:	<u>No</u>

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report
