Date of Approval: May 26, 2015 PIA ID Number: **1192**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Remittance Transaction Research, RTR

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.

Remittance Transaction Research, RTR

Next, enter the **date** of the most recent PIA. 8/23/2012

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
Yes	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

Were there other system changes not listed above? No

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
Yes	System Development/Milestone 4B
Yes	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? Yes

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.

The Remittance Transaction Research (RTR) system is a minor application, which is owned and operated by the IRS Wage and Investment (W&I) Division and is designed to provide a central repository of taxpayer remittance information. RTR includes a database that contains remittance data and images of checks and vouchers captured during remittance processing for each remittance transaction performed through the Integrated Submission and Remittance Processing (ISRP) system, Remittance Strategy for Paper Check Conversion (RS-PCC) system, and Lockbox Banks. Lock Box securely delivers data to the IRS. That data is then transferred to RTR via Electronic File Transfer Utility (EFTU). There is no direct interface or exchange of data between RTR and the Lockbox Banks. The RTR data is made available to authorized users across the IRS, in several different functions, who need to research payments. Users cannot modify the data and images stored in the RTR system, but are permitted to add notes concerning transaction records. RTR is comprised of three distinct areas: the RTR Database, Remittance Processing, and the RTR Web Application. The RTR Database is where remittance transaction data is validated and loaded into tables in the staging schema and transferred to tables in the production schema. Remittance Processing performs validation on remittance information and images that are received from each input source and then loads the remittance data and images onto the image file system. The RTR Web Application provides an online interface, allowing IRS users Intranet access to the system through a web browser located on their standard workstation. Data The type of data that comprises the RTR system is categorized as Sensitive but Unclassified (SBU) Privacy Act data. It includes taxpayer name, taxpayer identification number (TIN), along with remittance data (check, money order) which includes banking and payment information. In addition, RTR data consists of transaction codes, deposit transaction date, and Master File Tax (MFT) information. RTR collects and processes the following privacy information: Taxpayer: Data gathered from the taxpayer's remittance payment (check, money order) and voucher. To include: Name control, Bank routing and account numbers, TIN, payment amount, Transaction Date, Deposit Date, Tax period, Transaction code and MFT account code . Employee: The RTR application captures the employees' Standard Employee Identifier (SEID), information queried from the application and validates authorization for access.

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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Preparer Taxpayer Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or variations of SSN s).

There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system. There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (i.e. Names, addresses, etc.) No

6c. Does this system contain SBU information that it uses, collects, receives, displays, stores, maintains, or disseminates? No.

6d. Are there other types of SBU/PII used in the system? No

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

Yes 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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

RTR collects the following PII data from the taxpayer’s remittance payment (check, money order) and voucher, to include: Name control, Bank routing , TIN, payment amount, Transaction Date, Deposit Date, Tax period, Transaction code and MFT account code Name Social Security Number (SSN) Tax Payer ID Number (TIN) Address , SEID.

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 RTR system receives data from the Integrated Submission and Remittance Processing (ISRP), Remittance Strategy for Paper Check Conversion (RS-PCC), and Lockbox Bank systems, which have their own verification process for data accuracy, timeliness, completeness and; therefore, RTR assumes that the data is accurate, timely, and complete when it is provided by these systems.

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**
Treasury/IRS System of Records Number 22.054	Subsidiary Accounting Files
Treasury/IRS System of Records Number 34.037	IRS Audit Trail and Security Records
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF

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. N/A

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.

System Name	**Current PIA?**	**PIA Approval Date**	**SA & A?**	**Authorization Date**
Remittance Strategy for Paper Check Conversion (RS-PCC):	Yes	09/05/2013	Yes	02/15/2013
Integrated Submission and Remittance Processing (ISRP):	Yes	04/12/2014	Yes	07/24/2014

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
LockBox Banks	Tumbleweed Secure Transport	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? 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, cloud, 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? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
The system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions.

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? 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.

19. How does the system or business process ensure due process regarding information access, correction and redress?
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.

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? Yes

IRS Employees?	**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-Only

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Employees request access to the application by submitting an OL5081 which must be approved by their manager.

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 ? Yes

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.

The data and images for RTR are located on electronic media (database/cartridge). Once the retention period (7 years) has expired, the data and images will be overwritten. This disposition instruction is in accordance with National Archives-approved Job No. N1-58-09-47. Reference for this requirement/information can be located in Records Control Schedule (RCS) Document 12990 under RCS 29 for Tax Administration – Wage and Investment Records, item 133; and in IRM 3.5.10.7.3.4.(3) Images.

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)? Yes

23a. If **yes**, what date was it completed? 11/28/2012

23.1 Describe in detail the system s audit trail. Application-level audit trails monitor and log user activities. At a minimum, an event record shall specify the following: Data files opened and closed; Specific actions, such as reading and printing reports. The requirements of the Security Audit Automatic Response section of this IRM shall also be implemented in application level audit trails. Taxpayer

Information Specific – In addition to the Security Audit Automatic Response and Auditable Events requirements applications which process any type of, or subset of, taxpayer data shall capture and record the following application transactional information in audit trails: Employee and contractor transactions that add, delete, modify, or research a tax filer's record. Employee and contractor transactions that add, delete, modify, or research an employee's record (personnel and financial). Employee and contractor transactions that add, delete, or modify an employee's access to Employee User Portal (EUP), including changes to EUP roles or sub-roles. Any system transactions that alter an employee's access to the EUP, or a system's or application's role or sub role. Any employee or contractor transactions identified by the system owner as requiring additional oversight. Any third party transactions identified by the system owner as requiring additional oversight. For database management systems, the following minimum set of operations is audited for successful and unsuccessful execution: The DBA ensures that the creation, alteration, or deletion (drop) of database accounts is audited The DBA ensures that the creation, alteration, or deletion (drop) of any database system storage structure is audited The DBA ensures that the creation, alteration, or deletion (drop) of database objects is audited The DBA ensures that the creation, alteration, or deletion (drop) of database tables is audited The DBA ensures that the creation, alteration, or deletion (drop) of database indexes is audited The DBA ensures that enabling and disabling of audit functionality is audited The DBA ensures that granting and revoking of database system level privileges is audited The DBA ensures that any action that returns an error message because the object referenced does not exist is audited The DBA ensures that any action that renames a database object is auditedThe DBA ensures that any action that grants or revokes object privileges from a database role or database account is audited The DBA ensures that all modifications to the data dictionary or database system configuration are audited The DBA ensures that all database connection failures are audited. Where possible, the DBA ensures that both successful and unsuccessful connection attempts are audited. All connections performed to maintain or administer the database are audited. All DBA operations are audited where possible. At a minimum, the DBA connection is audited, and the following list of DBA activities are reported □ Database startup Dat
Database archiving Database performance statistics collection

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 9/30/2015

24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
Prior to being placed on the RTR production servers, a process is in place to develop, test and document the results of the proposed changes. This includes using a formal test plan to document the testing process, its scope, expected results, final results, and summary. Developers create test and evaluation plans, and use test plans to ensure changes to the application work properly without introducing new problems. The results of test plans are stored on DocIT and test results are used to correct identified flaws. If a security-related change required, the developers will incorporate additional security test cases into the RTR Test Plan. In the event that changes will be made to the security posture of RTR, the developers will conduct self-testing on the proposed changes, and the results, along with the date, will be subsequently documented and stored in DocIT. Additionally user testing, as well as tests to determine the impact to security, are also performed, all of which are then presented to the CCB overseeing the RTR application for final disposition. RTR is in compliance with IRM Section 10.8.6 for Secure Application Development.

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: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other: No

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