Date of Approval: **April 30, 2021**

PIA ID Number: **5892**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Remittance Transaction Research, RTR

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Remittance Transaction Research, (3411) RTR

What is the approval date of the most recent PCLIA?

5/3/2018

Changes that occurred to require this update:

Internal Flow or Collection

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Wage and Investment (W&I) Risk Committee

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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) application consolidates all Integrated Submission Remittance Processing (ISRP), Lockbox Bank (LB), and Remittance Strategy for Paper Check Conversion (RS-PCC) remittance transaction data and images and makes them available to authorized internal users who need to research remittance transactions. The data and Images are on a Tier II platform with the production environment. The end users of the RTR system access the payment data and images through the web browser on internal standard workstations. The business requirements specify the ability to support 1,300 concurrent users. Information is used by Wage and Investment employees.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements.

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

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.

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 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. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Standard Employee Identifier (SEID)
Financial Account Numbers
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

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.

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.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Name control, Bank routing, Taxpayer Identification Number (TIN), payment amount, Transaction Date, Deposit Date, Tax period, Transaction code and MFT account code.

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

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

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

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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 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, Taxpayer Identification Number (TIN), payment amount, Transaction Date, Deposit Date, Tax period, Transaction code and MFT account code, Name, Social Security Number (SSN), Taxpayer Identification Number (TIN), Address, Employer Identification Number (EIN), Standard Employee Identification (SEID). RTR is a repository of digital images of paper remittance checks submitted by taxpayers who don't pay electronically. The paper checks usually come with Name, Address, SSN/EIN, so the payment can be associated with the taxpayer's IRS account. RTR does not receive the actual paper checks, just the digitized images.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 22.054 Subsidiary Accounting Files

IRS 34.037 Audit Trail and Security Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Remittance Strategy for Paper Check Conversion (RS-PCC)
Current PCLIA: Yes
Approval Date: 9/16/2019
SA&A: Yes
ATO/IATO Date: 12/10/2020

System Name: Integrated Submission and Remittance Processing (ISRP)
Current PCLIA: Yes
Approval Date: 1/23/2019
SA&A: Yes
ATO/IATO Date: 11/17/2020

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

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: LockBox Bank
Transmission Method: Tumbleweed Secure Transport
ISA/MOU: Yes

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040V
Form Name: Payment Voucher

Form Number: 1040 Family
Form Name: FM1040

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Security Audit and Analysis System
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

Identify the authority.

The authority for processing taxpayer information is 5 U.S.C. 301 and 26 U.S.C. 7801. IRC 6103(d) Tax Administration.

For what purpose?

Tax Administration.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

They are notified of such collection by the Privacy Act Notice in the tax return instructions. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Read Only

Developers: Read Only

How is access to SBU/PII determined and by whom?

Employees request access to the application by submitting an (Online) OL5081 which must be approved by their manager. A potential user will request access via the OL5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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 Internal Revenue Manual (IRM) 3.5.10.7.3.4.(3) Images.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

10/1/2020

Describe 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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

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 is 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 Change Control Board (CCB) overseeing the RTR application for final disposition. RTR is in compliance with IRM Section 10.8.6 for Secure Application Development.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

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 Change Control Board (CCB) overseeing the RTR application for final disposition. RTR is in compliance with IRM Section 10.8.6 for Secure Application Development.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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