Date of Approval: **May 14, 2020**

PIA ID Number: **4242**

SYSTEM DESCRIPTION

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

Refund Inquiry, REF, Refund Inquiry, REF

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?

Where is My Refund (WMR) 3215

What is the approval date of the most recent PCLIA?

2/13/2018

Changes that occurred to require this update:

Were there other system changes not listed above?

Yes

What were those changes?

The addition of The Refund Trace (RTR) and Internet Refund Trace (IRTRC) application.

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

Small Business/Self-Employed (SB/SE) Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

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 Where is My Refund (WMR) application allows taxpayers receiving a refund to determine when it will be received. After entering their Social Security Number (SSN), Filing Status and Refund Amount from the tax return for authentication, the system will provide the status of the refund and or the date of delivery. The WMR application will request refund information from Integrated Data Retrieval System (IDRS), or, if no data is found, the Modernized e-File (MeF)/Modernized Tax Return Data Base (M-TRDB) since WMR does not store any taxpayer information. The WMR application checks the Client ID and 3rd Party Personal Identification Number (PIN), then uses the SSN, Filing Status and Refund Amount to provide the WMR response, which is then sent back to the company employee. The 3rd Party PIN is generated when the taxfiler participant selects a pin which is sent with the tax return through the Modernized eFile application in the electronic filing process. The WMR and Refund Inquiry (REF) application allows the taxpayer access to trace their refund and request a replacement check if the refund date is greater than 28 days of the date the check was mailed. The Refund Trace (RTR) and Internet Refund Trace (IRTRC) application allows the taxpayer to trace their refunds if lost, stolen, destroyed or never received. Each of the application's information is provided in both English and Spanish. The REF applications offer 2 medias, touchtone and voice recognition.

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:

Legal/statutory basis (e.g. where collection is expressly required by statute)

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

The Refund Inquiry system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax.

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

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. Refund Inquiry requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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

No

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

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

No

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

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.

The SSN is collected from the taxpayer to assist in the authentication, prior to providing them with tax refund information.

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

The validation process will verify the accuracy and completeness of the information in accordance with the business rules. The Where's My Refund Suite, Refund Inquiry and refund Trace does not store the PII information. It just uses what the taxpayer enters to retrieve their tax refund status information, and to authenticate against what is stored on IRS legacy databases. The Where's My Refund Suite, Refund Inquiry and Refund Trace system does not make adverse determinations but instead supplies the taxpayer with their requested information as a service to the taxpayer.

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 00.001   Correspondence Files and Correspondence Control 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: Modernized Tax Return Data Base (M-TRD)
Current PCLIA: Yes
Approval Date: 10/30/2018
SA&A: No

System Name: Integrated Data Retrieval System (IDRS)
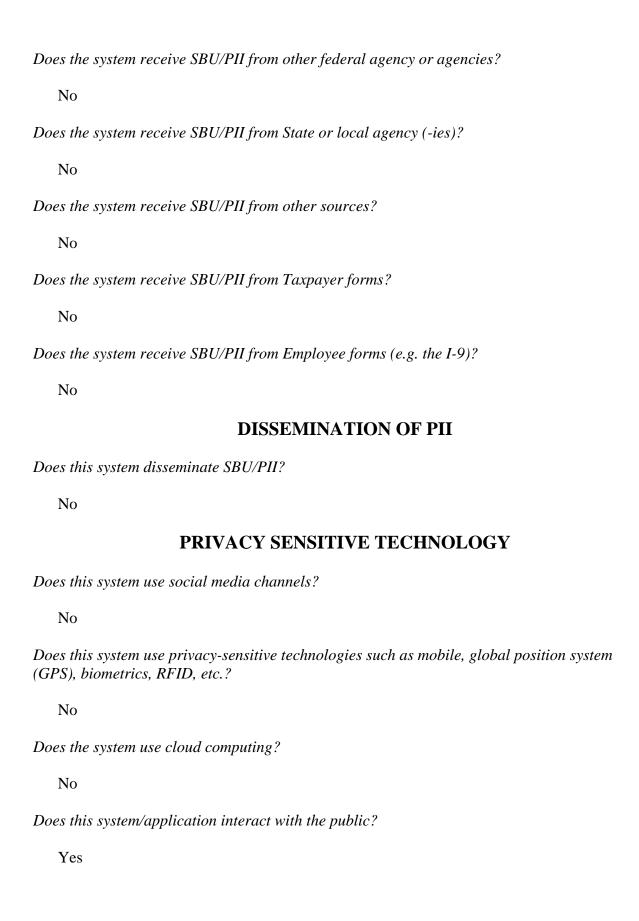Current PCLIA: Yes
Approval Date: 8/3/2017
SA&A: Yes
ATO/IATO Date: 1/2/2020

System Name: Modernized e-File (MEF)
Current PCLIA: Yes
Approval Date: 2/20/2019
SA&A: Yes
ATO/IATO Date: 4/3/2018

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?

No

Does the system receive SBU/PII from Taxpayer forms?

No

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Yes

When was the e-RA completed?

12/11/2019

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Knowledge Based Authentication (Out of Wallet)

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?

The irs.gov has several methods of informing the taxpayer about these issues. The irs.gov website has a Privacy Policy which states "Using these services is voluntary and may require that you provide additional personal information to us. Providing the requested information implies your consent for us to use this data in order to respond to your specific request." Prior to using the WMR application, WMR has the required notice that this is a US Government system for authorized use only. The application requires that the taxpayer acknowledge that Internal Revenue Code Section 6109 authorizes the collection of the social security number in order to provide the service requested by the taxpayer. The application also informs the taxpayer of use of the System of Records 24.030 Individual Master File. The taxpayer is also provided a link to all IRS Privacy Impact Assessments. The phone system plays a contact recording message, "To protect your privacy, you will need the social security number, filing status, and refund amount from your tax return. If you do not have this information, call us again when you have it available or you may visit our web site at www.IRS.gov and click on "Where's My Refund". Please be prepared to take note of important information and call back numbers".

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

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

Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, 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

System Administrators: Read Write

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

Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets for the purpose of authentication. Once they enter shared secrets and their data matches up with the IDRS and or MeF/M-TRDB information to ensure that the information is correct, they are eligible to use the system. IRS System Administrators are provided access to the servers thru the Online 5081 system. This requires the supervisor to authorize the access to the server or servers.

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.

RCS 17 Item 25-IRS.gov Website: (1) Web Management and Operations Records. Include records such as help desk reports and contact logs; meeting minutes, status reports change requests and other artifacts of the Requirements Traceability Matrix (RTM). AUTHORIZED DISPOSITION Destroy/Delete 6 years after processing year or when superseded, obsolete or no longer needed for the conduct of Agency business, whichever is later. (2) Web content records and records that can be used as evidence of content. (A) HTML-Encoded Pages, PDF files and code changes; Site "snapshots" and comprehensive URL listings; CMA guidelines, style guides, Interim guidance, web applications such as Installment Agreement Calculator and Excise Tax including their requirements and design documents. AUTHORIZED DISPOSITION Destroy/Delete 20 years after processing year or when superseded, obsolete or no longer needed for the conduct of Agency business, whichever is later. (B) Copyrighted web content and agreements; Web Design documents and application development records; Web metrics data including web trends and other web traffic reports. AUTHORIZED DISPOSITION Destroy/Delete 6 after processing year or when superseded, obsolete or no longer needed for the conduct of Agency business, whichever is later.

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?

5/27/2019

Describe the system's audit trail.

Refund Inquiry is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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)?

An End of Test Report is produced after each testing cycle and is stored in the Integrated Customer Communications Environment's DocIT repository.

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?

Applications goes through the Annual Security Controls Assessment (ASCA) along with other testing activities during the development life cycle.

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: Not Applicable

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