

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: February 12, 2015

PIA ID Number: **1195**

1. What type of system is this? Where's My Refund, WMR

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, and milestone of the most recent PIA.

Where's My Refund - Planned Maintenance path, WMR, ms4b

Next, enter the **date** of the most recent PIA. 1/8/2013 12:00:00 AM

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

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>Yes</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

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

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>Yes</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>No</u>	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 Where's My Refund application allows taxpayers receiving a refund to determine when it will be received? After entering their 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), since WMR does not store any taxpayer information. New this year is that employees of 8 tax preparation companies can access a link on IRS.gov to get the refund status for their customers. The WMR application checks the Client ID and 3rd Party Pin, and 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, 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 Yes On Spouse No On Dependent

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

<u>Yes</u>	Social Security Number (SSN)
<u>No</u>	Employer Identification Number (EIN)
<u>No</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	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).

This application does truncate the Social Security Number (last four digits are masked). The application cannot mitigate the use of Social Security numbers until an alternate identifier has been adopted by the IRS to identify taxpayers.

- 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

No PII Elements found.

- 6c. Does this system contain SBU information the system 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)

<u>No</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	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.

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

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 validation process will verify the accuracy and completeness of the information in accordance with the business rules. The WMR system 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 WMR system does not make adverse determinations but instead supplies the taxpayer with their requested information as a service to the taxpayer.

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

IRS 00.001

Correspondence Files and Correspondence Control Fi

IRS 34.018 IDRS Security Files
 IRS 34.037 Audit Trail and Security Records System
 IRS 24.030 IMF
 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

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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Integrated Data Retrieval System	Yes	08/03/2014	Yes	12/05/2014

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

No Organization Records found.

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

No Organization Records found.

11d. Does the system receive SBU/PII from other sources? No

No Organization Records found.

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

No Tax Form Records found.

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

12a. Does this system disseminate SBU/PII to other IRS Systems?

No System Records found.

12b. Does this system disseminate SBU/PII to other Federal agencies?

No Organization Records found.

12c. Does this system disseminate SBU/PII to State and local agencies?

No Organization Records found.

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors?

No Organization Records found.

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

12e. Does this system disseminate SBU/PII to other Sources?

No Organization Records found.

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? Yes

16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

Single Factor Identity Validation

If **no**, when will the e-RA be conducted?

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 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.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
The taxpayer's use of the web application is voluntary. Authentication using Shared Secrets is required in order to have confidence in the identity of the web application user.

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

The taxpayer has due process by calling or visiting the IRS.

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 Contractor Operated

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

IRS Employees? Yes

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

Contractor Employees? No

21a. 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 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 OL5081 system. This requires the supervisor to authorize the access to the server or servers.

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? No

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.

WMR is non-recordkeeping and does not require a NARA-approved records control schedule to affect data disposition. WMR is a web-based lookup application used for convenience of reference by taxpayers. It is not a data repository system. Recordkeeping copies of data accessed by this tool are disposed of in accordance with IRS Records Control Schedules. The WMR interface retains logs of all access of taxpayer records and passes this data and audit information to the SAAS application where it will be maintained for seven years (in accordance with NARA Job No. N1-58-10-22, approved 4/5/2011). SAAS disposition instructions are published in IRS Document 12990, Records Control Schedule 19 for Enterprise Computing Center - Martinsburg, item 88.

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? 9/5/2013 12:00:00 AM

23.1 Describe in detail the system's audit trail. The audit trail being sent to SAAS identifies the WMR application, the taxfiler type, the SSN, and the date time stamp. The Auditable events are Authenticating (successful or unsuccessful) and whether the taxpayer has too many invalid attempts at authentication and is locked out.

I.2 SA&A OR ECM-R

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

If **yes**, Is the test plan in process or completed: Completed

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?

Only the PII that is needed to authenticate is requested from the taxpayer. The validation process will verify the accuracy and completeness of the information in accordance with the business rules. Authentication is tested thoroughly to ensure security and confidentiality. An audit trail ensures that all users' activities are being monitored. The results of the test cases are documented and analyzed for defects.

24b.1. If **completed**, 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 ICCE's DocIT repository.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? No
25a. If **yes**, was permission granted per the requirements of Form 13471 Live Data Request? Yes
If **yes**, provide the date the permission was granted. 8/12/2013 12:00:00 AM
25b. If **yes**, was testing performed in conformance with IRM 10.8.8 IT Security, Live Data Protection Policy? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:
- 26a. IRS Employees: Not Applicable
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 or IRS contractors 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
