Date of Approval: 05/30/2025
Questionnaire Number: 1929

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?
> Where's My Amended Return

Acronym:
> WMAR

Business Unit
> Information Technology

Preparer
> # For Official Use Only

Subject Matter Expert
> # For Official Use Only

Program Manager
> # For Official Use Only

Designated Executive Representative
> # For Official Use Only

Executive Sponsor
> # For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.
> Where's My Amended Return (WMAR) is designed to track the status of amended returns as they are processed through the Submission Processing (SP) pipeline. Integrated Data Retrieval System (IDRS) will update the tax account with the transaction codes (TC) to indicate which WAGE group is handling the amended return. The application will provide the taxpayer the ability to track the status of up to 4 prior years Amended Returns. They can view the last filing season and 3 previous years. The status will be presented visually with three bars showing status, submitted, adjusted, and completed along with dates for each.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

    Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

    The Where's My Amended Return application requires the use of Social Security Numbers (SSNs) because no other identifier can uniquely verify a taxpayer at this time. The use of SSNs is permissible under Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on income tax returns. WMAR truncates the SSN (only the last four digits are displayed). The application cannot mitigate the use of SSNs until an alternate identifier is adopted by the IRS. While WMAR does not collect or display additional PII such as name, mailing address, e-mail, or phone number directly from the user, the backend systems it accesses, such as form 1040 which contains that information. As a result, name, Mailing address, Phone Number, Email address, Date of Birth, Protection Personal Identification Number (IP PIN), financial Account Numbers, Employment Information, Tax Account Information and related PII are a part of the data retrieved during the return status inquiry. Taxpayer Forms Accessed: Form 1040 - U.S. Individual Income Tax Return and Form 1040X - Amended U.S. Individual Income Tax Return. IRS Systems Accessed: Integrated Data Retrieval System (IDRS), Modernized E-File (MeF), and Security and Communications System (SACS). PII is not disclosed to third parties outside of the IRS. The Integrated Online Account (IOLA) provides access to WMAR. In alignment with OMB Circular A0130, the IRS continues to develop strategies to mitigate or eliminate the use of SSNs in systems where feasible. However, in this case, the SSN remains uniquely necessary to identify and retrieve a taxpayer's amended return record.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

    Address
    Email Address
    Employer Identification Number
    Employment Information
    Federal Tax Information (FTI)
    Individual Taxpayer Identification Number (ITIN)
    Name
    Other
    Preparer Taxpayer Identification Number (PTIN)
    Social Security Number (including masked or last four digits)
    Tax ID Number

Telephone Numbers

Please explain the other type(s) of PII that this project uses.
Date of Birth (DOB)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?
No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
Application

3 What Tier designation has been applied to your system?
2

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
Yes

4.11 What is the previous PCLIA number?
6703

4.12 What is the previous PCLIA title (system name)?
Where's My Amended Return

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)
Expiring PCLIA

5 Is this system considered a child system/application to another (parent) system?
Yes

5.1 Identify the parent system's approved PCLIA number.
Integrated Customer Communications Environment (ICCE)

5.2 Identify the parent system's name as previously approved.

     Integrated Customer Communications Environment (ICCE)

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

     Execution

7 Is this a change resulting from the OneSDLC process?

     No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

     Small Business/Self Employed (SBSE) Governance Board

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

     211160

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

     No

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

     The application does not currently have an Accounting of Disclosures process in place. Coordination will take place to develop and implement the required process. A project completion date will be provided upon initial consultation.

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

     No

11.1 Describe the business process and purpose of your Artificial Intelligence (AI) and identify what system(s) or business process(es) this AI supports.

      The application does not utilize AI. No business process and purposes are required.

11.2 What is the algorithm or learning method used and what database is training your AI?

      This application does not utilize AI. Therefore, no algorithm, learning method, or training database is used.

11.3 How is this AI system tested and validated to ensure that the decisions or outputs are reliable (relevant to the input) and performs without biases and drifting? Note: Outputs include, User information, transfer to assistor, reports on dashboard depicting activities.

      The application does not utilize AI. No testing and validation are required.

12 Does this system use cloud computing?

      No

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

      The application does not utilize a CSP.

12.2 Does the CSP allow auditing?

      No

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

      This system does not utilize a CSP. Therefore, there is no CSP audit data to access.

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

      This application does not utilize a CSP, therefore no background check is required.

13 Does this system/application interact with the public?

      Yes

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

      Yes

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

      Yes

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

Taxpayer initiates use of application implying consent.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

The taxpayer voluntarily initiates use of the application. Information about the purpose, use and authority to collet is provided during the process via system prompts or linked notices.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

Not applicable. The system only collects information directly from the taxpayer.

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Access to data by taxpayers is determined through authentication using valid shared secrets. Once the taxpayer provides this information and it matches the IDRS records, they are granted access to the system. IRS system administrators are granted access though the BEARS process, which requires supervisor approval to authorize access to servers.

15 Is this system owned and/or operated by a contractor?

No

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

Systems administrators - read/write access. Contractors are only used for development and not tax administration. Contractor do not have access to PII in this system.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

    A Privacy Act Statement is presented to the taxpayer before any PII is collected. The statement outlines the authority for collection, purpose of use, and the consequences of non-provision. Consent is implied through voluntary use of the application.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

    Not Applicable

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

    Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

    More than 1,000,000

22 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 or if the taxpayer has an IOLA account. 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 BEARS system. This requires the supervisor to authorize the access to the server or servers.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

    No

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

    No

26 Describe this system's audit trail in detail. Provide supporting documents.

    WMAR uses the (ICCE) capability to capture audit data and forward the data to an Enterprise Logging System - Security Audit and Analysis System (SAAS). ICCE does not store audit data. Instead, audit records are created in memory and sent to SAAS as "forward and forget". There is no ability to access the audit information from the application or from the server on which the application runs.

27 Does this system use or plan to use SBU data in a non-production environment?
No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
ICCE Management Information System
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
ICCE Telephone Applications IVR
Incoming/Outgoing
Both
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Individual Master File online (IMFOL)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
Forms
Agency Name
Form 1040X (Amended U.S. Individual Tax Return)
Incoming/Outgoing
Both
Transfer Method
Secured channel via HTTPS

Interface Type
    IRS Systems, file, or database
Agency Name
    Taxpayer Information File Data Store (TIF DS)
Incoming/Outgoing
    Incoming (Receiving)
Transfer Method
    Electronic File Transfer Utility (EFTU)

Interface Type
    IRS Systems, file, or database
Agency Name
    Taxpayers
Incoming/Outgoing
    Incoming (Receiving)
Transfer Method
    Electronic File Transfer Utility (EFTU)

Interface Type
    IRS Systems, file, or database
Agency Name
    National Account Profile (NAP)
Incoming/Outgoing
    Incoming (Receiving)
Transfer Method
    Electronic File Transfer Utility (EFTU)

Interface Type
    Forms
Agency Name
    Form 1040 (U.S. Individual Income Tax Return)
Incoming/Outgoing
    Both
Transfer Method
    Secured channel via HTTPS

Systems of Records Notices (SORNs)

SORN Number & Name
    IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
    This SORN is identified for the use of tax administration,
    specifically for refund information.

SORN Number & Name
>IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.
>To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites.

SORN Number & Name
>IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.
>The SORNs are identified for tax administration.

Records Retention

What is the Record Schedule System?
>General Record Schedule (GRS)

What is the retention series title?
>Information System Access Records

What is the GRS/RCS Item Number?
>3.2, item 030

What type of Records is this for?
>Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
>System access logs that document user login activity, authentications, and access to IRS systems. These records support system security, user monitoring, and audit trail verification. Access logs are transmitted to the WebApps Audit Service and integrated into IRS Cybersecurity's enterprise monitoring systems, including the Security Audit and Analysis System (SAAS) and Splunk.

What is the disposition schedule?
>Temporary. Destroy 6 years after the password is changed or the user separates from access per RS 3.2, item 030.

What is the Record Schedule System?
>General Record Schedule (GRS)

What is the retention series title?
>System Audit Logs

What is the GRS/RCS Item Number?
>3.2, item 031

What type of Records is this for?
>Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
> System audit logs record internal system activity such as data access, changes and administrative actions. These logs support system diagnostics, audit forensics, and monitoring. Audit records are passed through WebApps Audit Service and integrated into IRS-wide monitoring systems including the Security Audit and Analysis System (SAAS) and Splunk.

What is the disposition schedule?
> Temporary. Destroy 3 years after the audit or event, in accordance with GRS 3.2, item 031.

Data Locations

What type of site is this?
> System

What is the name of the System?
> Where's My Amended Return

What is the sensitivity of the System?
> Federal Tax Information (FTI)

What is the URL of the item, if applicable?
> https://sa.www4.irs.gov/wmar/

Please provide a brief description of the System.
> Where's My Amended Return (WMAR) provides taxpayers with the status of their amended federal tax return using shared secret information for identity verification.

What are the incoming connections to this System?
> WMAR received data from the Integrated Data Retrieval System (IDRS), which pulls amended return status updates processed though the submission processing pipeline. This included the transaction code indicating which WAGE group is handling the return.

What are the outgoing connections from this System?
> WMAR does not transmit data to any external or internal systems. It displays return status information to the taxpayer only.