Date of Approval: 12/20/2024
Questionnaire Number: 1756

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Web Applications Platform Environments

Acronym:

WebApps Platform

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.

Web Apps Platform will develop and deliver the information technology systems via IRS.gov to provide taxpayers with a single conduit leveraging eAuthentication to access their tax account information as part of this strategy. Web Apps Platform being the single conduit provider of common services, utilities, and components, will allow all projects to utilize and leverage these services, supporting reusability across the enterprise. It will also support the integration with existing Internal Revenue Service (IRS) infrastructure services to address key non-functional requirements, including systems monitoring and security. All activities and data accessed because of that activity may be stored for usage statistics and analytics to improve the overall taxpayer experience when interaction with taxpayer applications. The information will be used to determine how to improve web applications, to track the response rate to notices, and to

track usage of website features related to tax application conditions. This data will also be used to determine how website usage correlates to tax and identity fraud. The IRS will benefit from the Web Apps Platform by having the ability to recover from errors quickly, reduce time, improve availability, and provide business continuity in production for all taxpayer facing applications. The IRS will not be collecting any new taxpayer information, only providing a new platform service for new taxpayer applications to interact with the IRS.

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 platform contains common functions usable by all projects and allows new products to quickly deploy their application on a taxpayer-facing platform with access to abstracted taxpayer information residing on IRS Core systems (e.g., Common Business Services (CBS), Returns Inventory and Classification System (RICS). Online activity is recorded to be used in the event of criminal online activity. Each application transaction is recorded as an audit event, extracted, and sent to Security Audit and Analysis System (SAAS) to prove audit trail for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and Cybersecurity.

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

Agency Sensitive Information
Criminal Investigation Information
Official Use Only (OUO) or Limited Office Use (LOU)
Physical Security Information
Protected Information

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

PII about individuals for Bank Secrecy Act compliance - 31 USC
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)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

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

System

1.35 Is there a data dictionary for this system?

No

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

For an IRS WebApp, the flow of Personally Identifiable Information (PII) and Sensitive but Unclassified (SBU) data requires a more detailed approach to address the highly sensitive nature of taxpayer information. Below is the detailed flow specific to the IRS WebApp environment, incorporating security, compliance, and operational safeguards.

1. Data Flow into the System (Input)

Sources of Input:

1. Taxpayer Submission:

• Individual or business taxpayers enter PII and SBU data, such as Social Security Numbers (SSN), Employer Identification Numbers (EIN), income details, and bank account numbers.

• Input methods:

• Online forms for tax filing, refunds, or status checks.

• File uploads, such as scanned forms or tax documents.

2. Third-Party Providers:

• Tax preparers, payroll companies, or financial institutions submit data on behalf of taxpayers.

• Examples include W-2 forms, 1099 filings, and financial reports via APIs or bulk uploads.

3. Internal IRS Systems:

• Legacy IRS systems may push data into the WebApp for user access, e.g., tax return history or account balances.

Security Measures:

• Authentication

• Use multi-factor authentication (MFA) to ensure secure access.

• Verify taxpayer identity using personal information (e.g., last year's AGI).

• Encryption in Transit:

• All incoming data must be encrypted using TLS (e.g., HTTPS).

• Input Validation:

• Sanitize all inputs to protect against injection attacks.
• Session Management:
• Enforce timeouts for user sessions to prevent unauthorized access.

2. Data Flow Through the System (Processing)
Handling PII and SBU:

1. Authentication and Authorization:
• Validate users against IRS databases for access to their specific records.
• Implement role-based access controls (RBAC) to restrict access by employees or contractors.
2. Data Transformation:
• Normalize and process raw taxpayer inputs into structured formats for:
• Calculating tax liabilities or refunds.
• Validating bank details for direct deposit.
3. Integration with IRS Backend Systems:
• API calls to backend systems (e.g., Integrated Data Retrieval System - IDRS) to retrieve or update taxpayer records.
• Synchronize processed data with internal databases.
4. Audit Logging:
• Log all access, changes, and data transmissions, tagging specific user IDs for compliance tracking.

Security Measures:

• Data Masking:
• Mask SSNs, bank account numbers, or other PII in non-critical workflows.
• Tokenization:
• Replace sensitive data with non-sensitive tokens during processing where feasible.
• Segmentation:
• Use separate environments for production, testing, and development to prevent unauthorized data exposure.
• Monitoring:
• Deploy intrusion detection systems (IDS) and automated alerts for abnormal activity.

3. Data Storage
Storage Types:

1. Database Storage:
• PII and SBU data are stored in relational databases (e.g., Oracle, PostgreSQL) using strict access controls.
2. Cloud Infrastructure:
• If the WebApp uses cloud services, IRS guidelines (e.g., FedRAMP compliance) dictate data protection.
3. Backup Systems:

• Regular backups are encrypted and stored in secure locations for disaster recovery.

Security Measures:

•Encryption at Rest:

• Encrypt all stored data using FIPS 140-2 validated algorithms.

• Data Retention Policies:

• Retain data only as long as required by IRS regulations.

• Access Auditing:

• Maintain logs of database access and modifications for internal audits and external compliance reviews.

4. Data Flow Out of the System (Output)

Output Methods:

1. User-Facing Output:

• Taxpayers can view their account details, tax filings, and payment statuses on the WebApp.

• Export options include downloadable PDFs of tax returns or status reports.

2. External Reporting:

• PII and SBU data may be shared with authorized third parties (e.g., Treasury Department, financial institutions) via secure file transfer protocols (SFTP).

3. Notifications:

• Email or SMS alerts (with minimal PII) are sent to taxpayers, e.g.,

•Your refund has been processed.

Security Measures:

• Redaction:

• Ensure sensitive data (e.g., SSNs) is partially or fully redacted in user-facing outputs.

• Transmission Encryption:

• Use end-to-end encryptions for all external data sharing.

• Data Use Agreements:

• Establish agreements with third parties outlining strict use and handling of IRS data.

Additional Compliance Considerations

Regulatory Frameworks:

1. FISMA (Federal Information Security Modernization Act):

• The IRS WebApp must comply with federal guidelines for managing sensitive taxpayer data.

2. NIST 800-53:

• Implement security and privacy controls recommended by the National Institute of Standards and Technology.

3. Internal Revenue Code (IRC) Section 6103:

• Protect taxpayer data confidentiality and ensure limited access.

Incident Response:

• The WebApp must have a robust incident response plan to detect, report, and mitigate breaches involving taxpayer PII and SBU.

Periodic Audits:

• Perform regular audits to ensure adherence to IRS and federal security standards.

1.4 Is this a new system?

No

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.6 What is the PCLIA number?

6351

1.7 What are the changes and why?

Expiring PCLIA

1.8 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.

Currently there isn't an ABA Number for the PIA ID Number: 6351, Date of Approval: 01/14/2022.

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Readiness

2.1 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? Contact Disclosure to determine if an accounting is required. Enter "Yes" or "No". If Exempt, type "Exempt".

Exempt

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

Web Applications (WebApps) Governance Board and Strategic Development Executive Steering Committee

3.1 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?

No

3.3 Does this system use cloud computing?

No

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

The taxpayer has due process by writing, calling, faxing or visiting the IRS. They are also provided due process rights on the tax forms.

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

IRS Employees:
Users Read-Only
Managers Read-Only
System Administrators Read-Only
Developers No Access

Contractor Employees:
Users Contractor Users Read-Only Access, Background Invest. Level - Moderate
Contractor Managers Read-Only Access, Background Invest. Level - Moderate
Contractor System Administrators Administrator Access, Background Invest. Level - Moderate
Contractor Developers No Access

4.51 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

4.52 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

4.53 How many records in the system are attributable to members of the public? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not applicable".

More than 1,000,000

4.6 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 taxpayer enters 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. All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, access to WebApps Platform is obtained through the On-Line 5081 (OL5081) process. All access must be approved by the user's manager who reviews the OL5081 at the time of submission and on an annual timeframe. The system administrators/approvers will also verify group membership to ensure only the appropriate rights are granted based upon need-to-know. For non-production supporting environments users must complete the necessary Sensitive But Unclassified (live) data training, request access through the OL5081, and in some cases as outlined by the requirements set forth within the Internal Revenue Manual submit an elevated access letter that is approved by the Associate Chief Information Officer prior to granting access. The non-production environment will also routinely review access lists and verify accounts, removing ones that are no longer necessary. Every individual is reminded of their UNAX requirements where they are restricted to see certain taxpayer data and, in many instances, a third-party tool is implemented to restrict access to that data.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

No

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 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

Security Audit and Analysis System (SAAS)

Incoming/Outgoing
Both
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Online Account (OLA)
Incoming/Outgoing
Both
Transfer Method
Secured channel via HTTPS

Interface Type
IRS Systems, file, or database
Agency Name
Returns Inventory and Classification System (RICS)
Incoming/Outgoing
Both
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Common Business Services Release 1 (CBS)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secured channel via HTTPS
Other Transfer Method
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 Online Account application, Online Account has the required notice that this is a U.S. Government system for authorized use only. That notice is copied below. The application 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. THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY! Use of this system constitutes

consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including all penalties applicable to willful Unauthorized Access (UNAX) or inspection of taxpayer records (under 18 United States Code (U.S.C.) 1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431)

Interface Type

IRS Systems, file, or database

Agency Name

Cybersecurity Data Warehouse (CSDW)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Electronic File Transfer Utility (EFTU)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

This SORN covers records related to correspondence between taxpayers and the IRS. It is used to manage and control all correspondence generated or received by the IRS to ensure timely and accurate responses. These records are critical for maintaining accountability and transparency in taxpayer interactions. They support compliance with legal requirements and serve as reference material for resolving disputes or tracking communication history.

SORN Number & Name

IRS 26.020 - Taxpayer Delinquency Investigation Files

Describe the IRS use and relevance of this SORN.

This SORN includes records used in investigations of taxpayers who have failed to file required tax returns or pay taxes owed. These records support the IRS's enforcement activities by providing detailed information on delinquent accounts, including identifying information, income data, and payment history. The relevance lies in enabling the IRS to prioritize delinquent cases, initiate collection efforts, and ensure compliance with federal tax laws. The records are also critical for maintaining the integrity of the tax system by addressing noncompliance and deterring future delinquency.

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

This SORN contains records for business taxpayer accounts. Like the Individual Master File, it tracks tax filings, payments, and account statuses for businesses. The system supports accurate tax administration, compliance efforts, and resolution of business-related tax issues. It ensures businesses are properly credited for payments and compliant with tax obligations.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

This SORN pertains to records that document access to IRS systems and data. It is critical for ensuring the security and privacy of taxpayer information. These records are used to detect and respond to unauthorized access, support investigations, and maintain accountability for system users. The audit trail promotes compliance with federal privacy and security requirements.

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

This SORN encompasses records related to electronically filed tax returns and associated data. It ensures the efficient processing of electronic submissions, maintains the integrity of tax return data, and provides a secure record of electronic transactions. The records are relevant for error resolution, fraud detection, and compliance monitoring. Additionally, they support taxpayer convenience by enabling faster processing and quicker refunds.

SORN Number & Name

IRS 22.061 - Information Return Master File

Describe the IRS use and relevance of this SORN.

This SORN includes records related to information returns (e.g., Forms 1099 and W-2) submitted by third parties. These records are vital for verifying taxpayer-reported income and ensuring compliance with tax laws. The Information Return Master File supports fraud detection, audits, and enforcement activities by providing accurate data on income and payments reported by employers, financial institutions, and other entities.

SORN Number & Name

IRS 37.111 - Preparer Tax Identification Number Records

Describe the IRS use and relevance of this SORN.

This SORN covers records related to the issuance and management of Preparer Tax Identification Numbers (PTINs), which are required for paid tax return preparers. These records are used to track and monitor the activities of tax preparers, ensuring accountability and compliance with tax laws and regulations. The PTIN records help identify preparers, prevent fraud, and enhance oversight of preparer conduct. They also provide a framework for addressing complaints and enforcing penalties for noncompliance, contributing to the protection of taxpayers and the integrity of the tax preparation process.

SORN Number & Name

IRS 26.019 - Taxpayer Delinquent Account Files

Describe the IRS use and relevance of this SORN.

This SORN relates to records of investigations into delinquent taxpayers. It is used to track and manage cases of noncompliance, including failure to file returns or pay taxes owed. The records assist the IRS in prioritizing and resolving delinquency cases, ensuring equitable enforcement of tax laws and maintaining the integrity of the tax system.

SORN Number & Name

IRS 37.006 - Correspondence, Miscellaneous Records, and Information Management Records

Describe the IRS use and relevance of this SORN.

This SORN includes miscellaneous records related to correspondence and information management. It supports the IRS's internal operations by documenting communications and other administrative activities. The records are relevant for maintaining institutional knowledge, tracking responses, and ensuring efficient management of information resources.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

This SORN includes records on individual taxpayer accounts. It is a core system that contains critical taxpayer information, such as filing history, payments, refunds, and account balances. The relevance lies in its use for managing individual accounts, resolving taxpayer issues, and ensuring accurate tax administration. It is integral to customer service and enforcement activities.

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Information System Security Records
What is the GRS/RCS Item Number?
GRS 3.2, item 031
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
System access records. These records are created as part of the user identification and authorization process to gain access to systems.
What is the disposition schedule?
Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Information System Security Records
What is the GRS/RCS Item Number?
GRS 3.2 item 030
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
System access records. These records are created as part of the user identification and authorization process to gain access to systems.
What is the disposition schedule?
Temporary. Destroy when business use ceases.