Date of Approval: 01/26/2025
Questionnaire Number: 1910

Basic Information/Executive Summary

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

Web Applications Enterprise Service

Acronym:

WAES

Business Unit

Transformation and Strategy Office

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.

The Web Applications Enterprise Service (WAES) platform is comprised of the following components: Individual Online Account (IOLA), Taxpayer Protection Program Identity Verification (TPP-ID), Digital Notices and Letter (DNL), WAES Income Verification Express Service (IVES), Business Tax Account (BTA) (formerly known as Business Online account (BOLA)), Clean Energy Special Handling (CESH), and Tax Professional Account (TAXPRO). WebApps Enterprise Services (WAES), formerly known as Online Account (OLA), is a Web-based application, using the Integrated Enterprise Portal (IEP), that allows individual and business taxpayers access to their tax information and be able to take actions on their tax accounts using a single sign-on capability. It also provides the framework for additional online capabilities to expand the taxpayer online experience. WAES implements a single sign-on with a login and password

leveraging the Secure Access (eAuthentication/ Secure Access Digital Identity (SADI)) system and provides a landing page that includes the following capabilities across the platform: a) View balance due, b) View payment history/ Manage payments/Make a payment, c) Integrated Payments, d) View tax records, e) Apply and Modify installment agreement/payment plan, f) Authorizations, g) Digital Notices and Letters, h) Digital communications i) Language Preferences j) Profile & Preferences. Business Tax Account BTA (shares similar features to IOLA listed above) includes the following unique capabilities: a) Business Authorization, b) Business Profile c) Manage EIN online, d) Federal Contractor Tax Check System (FCTCS), e) Business Tax Compliance Check, Clean Energy Special handling (CESH): includes the following unique capabilities: a) Clean Energy Vehicle Manufacturers registration and reporting b) Clean Energy Vehicle Dealers and Sellers registration and transaction reporting c) Clean Energy and Semiconductor Elective Pay and Transferability Pre-Filing Registration Tool d) 8Energy Efficient Home Improvement Manufacturers (Going live 1/26/25) Individual Online Account (IOLA) includes the following unique capabilities: a) Taxpayer Protection Program (TPP) Identity Verification (ID Verify), b) Secure Messaging, c) Update my address, d) Offer in compromise (OIC) Self-service applications, e) Digital Mobile Adaptive Forms (DMAF), f) View My Audit (VMA). The IRS benefits from WAES by providing taxpayers increased availability to self-service applications, which decreases taxpayer's reliance on more expensive phone, correspondence, and walk-in channels. The IRS is not collecting any new taxpayer information, only providing a new online channel for taxpayers to interact with the IRS. The WAES application itself, and not the enterprise Secure Access (e-Authentication/SADI) application, focuses on the role and privileges of the taxpayer only. WAES uses the Web Apps Platform environments, which is the single conduit provider of common services, utilities, and components, which allows all the projects to utilize and leverage these services, supporting reusability across the enterprise. All activities and data accessed as a result of that activity may be stored for usage statistics and analytics on the Web Apps Platform. * Additionally, Google Analytics are running on each microservice, which log non-PII user activities such as clicks and view-page statistics. Currently each time a taxpayer requests their personal information, a service call is made from the WebApps platform to the database where this data resides. With this current implementation, there has been a history of service disruptions and excessive service calls between WAES platform and the database. To resolve these issues, the Software Architecture Refactoring (SAR) team is planning to implement a cache to temporarily hold taxpayer PII in ephemeral storage. This data will only be available as read-only by the WebApps platform and is completely held in RAM (non-persistent). Individuals (internal nor external) will not be able to access or read this cache. Security has been consulting during the design phase of this cache and validated that all necessary security controls are in place. The business case of this is to decrease the number of service calls and bandwidth requirements, decrease response times to taxpayer requests, and improve the taxpayer experience. The Centralized Online

Transactional Processing (COLTP) is a DB on the WAES Database server which is currently annotated in the System Security Plan.

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).

WAES establishes a single WebApps Enterprise Services enabling taxpayers to view, update, and retrieve their tax information. Social Security Number (SSN) is used as an access key to retrieve and update information in other IRS systems. Web Apps Platform services include usage statistics. Web and business analytics are critical components for Web Apps and target platform, providing IRS the ability to improve the website's usability and make business decisions to improve business processes and user experiences. SSNs are required to uniquely identify individuals impacted by or associated with website activity. Online Audit Trail-Online activity is recorded to be used in the event of criminal online activity (e.g., return fraud) for court cases. Universal User Identifiers (UUIDs) do not cover all cases: spouses, dependents, and clients of tax professionals that do not have UUIDs or other suitable identifiers. For these cases, there is no other alternative identifier, SSNs must be used to cross correlate any fraudulent activity. Each application transaction is recorded as an audit event, extracted, and sent to SPLUNK to prove audit trail for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigations (CI), and Cyber. Cybersecurity-Online activity is tracked for use in identifying and mitigating cybersecurity threats. Web Apps Platform collects web service requests and responses and copied to the Cybersecurity Data Warehouse (CSDW) that stores historical audit data and provides an offline analytic resource for Cybersecurity. Diagnostics-The Custom Diagnostics solution allows internal IRS users the ability to view health of the Web Application Servers and the actual applications running on them, including user access patterns and errors, typically during production support. Custom Diagnostics could include any functionality where log data is monitored and cleansed for viewing by any internal IRS user.

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

Address
Centralized Authorization File (CAF)
Email Address
Employer Identification Number

Financial Account Number
Internet Protocol Address (IP Address)
Social Security Number (including masked or last four digits)
Vehicle Identification Number (VIN)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
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)?
Yes

1.1 What is the IRA Initiative Number?
IRA objectives 1 and 2

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

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

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?
1672

4.12 What is the previous PCLIA title (system name)?
WebApps Enterprise Services

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.)

Updating PCLIA to include PII needed for IRA/CE Optical Character Recognition (OCR) Functions, Clean Energy Vehicle Manufacturers, Clean Energy Vehicle Dealers and Sellers, Clean Energy and Semiconductor Elective Pay and Transferability Pre-Filing Registration Tool, and Energy Efficient Home Improvement Manufacturers

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

No

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.

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

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.

Account (BTA) 211489 Online Account (IOLA) 210830 Tax Professional (TAXPRO) 211043 Clean Energy (CE) 211496

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?

Yes

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

12 Does this system use cloud computing?

Yes

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

AWS GovCloud: package ID:F1603047866. Date: 06/21/2016

12.2 Does the CSP allow auditing?

Yes

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

IRS

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

Moderate

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?

Yes. By accessing the site, consent is given.

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 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 Individual Online Account application, Individual Online Account has the required notice that this is a U.S. Government system for authorized use only. That notice is copied below: WARNING! By accessing and using this government computer system, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized use of, or access to, this computer system may subject you to

criminal prosecution and penalties. The taxpayer is also provided a link to all IRS Privacy Impact Assessments.

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

N/A

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

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

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

Yes

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?

Yes

15.2 What PII/SBU data does the subcontractor(s) have access to?

Technical system information and vulnerability data

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.)

IRS Employees:	Access Level
Users	Read-Only
Managers	Read-Only
Sys. Administrators	Administrator
Developers	Read-Only

Contractor Employees:	Access Level	Background Invest. Level
Contractor Users	Read-Only	Moderate
Contractor Managers	Read-Only	Moderate
Contractor Sys. Admin.	Administrator	Moderate
Contractor Developers	Read-Only	Moderate

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.

The IRS is committed to protecting the privacy rights of America's taxpayers. These rights are protected by the Internal Revenue Code, the Privacy Act of 1974, the Freedom of Information Act, and IRS policies and practices. Visit the IRS

Electronic Freedom of Information Act Reading Room for more information about these laws. We document much of our internal policy on these laws in IRM 10.5.1, Privacy Policy. The Senior Agency Official for Privacy (SAOP), as mandated by OMB M-16-24 PDF, has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy. The SAOP for the IRS is positioned at the Department of Treasury.

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".

N/A

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".

N/A

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

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

N/A

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 (ID.Me) for the purpose of authentication. Once taxpayer enters shared secrets and their data matches up with the Integrated Data Retrieval System (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 these requests go through Business Entitlement Access Request System (BEARS). All access must be approved by the user's manager who reviews the BEARS request 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 BEARS, 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 Unauthorized Access (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.

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

No

24 Explain any privacy and civil liberties risks related to privacy controls.

N/A

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

An Audit Plan has been created for this system by the project team with the support of Enterprise Security Audit Trail (ESAT)/SPLUNK. The system collects legal events for TIGTA, CI, and the CSDW to establish chain of custody for each transaction within all applications to be used as evidence and prove audit trails. It records all actions of the taxpayer/user in near-real-time and transmits to ESAT/SPLUNK logs for Cybersecurity review.

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

Secure Access Digital Identity (SADI)

Incoming/Outgoing

Both

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Standardized IDRS Access

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Secured channel via HTTPS

Interface Type

Other Federal Agencies

Agency Name

Department of Energy
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secured channel via HTTPS

Interface Type
Other Federal Agencies
Agency Name
Fiserv
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Business Master File
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secured channel via HTTPS

Interface Type
IRS Systems, file, or database
Agency Name
SPLUNK
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secured channel via HTTPS

Interface Type
Other Organization
Agency Name
Bank of America Merrill Lynch (BAML)
Incoming/Outgoing
Incoming (Receiving)
IRS FSIG - Fiscal Service EFTPS ISA_MOA 01.30.2023
Transfer Method
Electronic File Transfer Utility (EFTU)

Interface Type
IRS Systems, file, or database
Agency Name
Individual Master File
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secured channel via HTTPS

Interface Type
Other Federal Agencies
Agency Name
Bureau Of Fiscal Services
Incoming/Outgoing
Both
Transfer Method
Electronic File Transfer Utility (EFTU)

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.
Individual tax records

SORN Number & Name
IRS 24.030 - Customer Account Data Engine Individual Master File
Describe the IRS use and relevance of this SORN.
Individual tax records

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
Audit trail and security records

SORN Number & Name
Treasury .015 - General Information Technology Access Account Records
Describe the IRS use and relevance of this SORN.
Auditing

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

Storing customer communications

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 5.2 Transitory and Intermediary Records

What is the GRS/RCS Item Number?

20

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Intermediary records.

What is the disposition schedule?

Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 5.1 Common Office Records

What is the GRS/RCS Item Number?

10

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Administrative records maintained in any agency office.

What is the disposition schedule?

Temporary. Destroy business use ceases.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GRS 5.1 Common Office Records

What is the GRS/RCS Item Number?

20

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Non-recordkeeping copies of electronic records agencies maintain in email systems, computer hard drives or networks, web servers, or other locations after agencies copy the records to a recordkeeping system or otherwise preserve the recordkeeping version.

What is the disposition schedule?

Temporary. Destroy immediately after copying to a recordkeeping system or otherwise preserving, 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?

GRS 3.1 General Technology Management Records

What is the GRS/RCS Item Number?

001

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Technology management administrative records. Records on day-to-day, routine information technology management.

What is the disposition schedule?

Destroy 5 years old 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?

GRS 3.2 Information Systems Security Records

What is the GRS/RCS Item Number?

30

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. Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
GRS 3.1 General Technology Management Records
What is the GRS/RCS Item Number?
051
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
Data administration records and documentation relating to electronic records that are scheduled as temporary in the GRS or in a NARA-approved agency schedule or any types of data administration records not listed as permanent
What is the disposition schedule?
Destroy 5 years after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, 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?
GRS 3.2 Information Systems Security Records
What is the GRS/RCS Item Number?
20
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
Computer security incident handling, reporting and follow-up records.
What is the disposition schedule?
Destroy 3 year(s) after all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

Data Locations

What type of site is this?
System
What is the name of the System?
Centralized Online Transactional Processing

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

The Centralized Online Transactional Processing (COLTP) is a DB on the WAES Database server which is currently annotated in the System Security Plan. This is a security update to the database which is currently the PII storage solution

What are the incoming connections to this System?

Hosted on WAES, no incoming.

What are the outgoing connections from this System?

Hosted on WAES, no outgoing.

What type of site is this?

Environment

What is the name of the Environment?

Enterprise Data Platform

What is the sensitivity of the Environment?

Federal Tax Information (FTI)

Please provide a brief description of the Environment.

The IRS Enterprise Data Platform

What are the incoming connections to this Environment?

Via Enterprise API Gateway

What are the outgoing connections from this Environment?

Via Enterprise API Gateway

What type of site is this?

Environment

What is the name of the Environment?

Cybersecurity Data Warehouse

What is the sensitivity of the Environment?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the Environment.

Retains taxpayer activity logs with restricted access to cyber only

What are the incoming connections to this Environment?

Via API

What are the outgoing connections from this Environment?

Via API