Date of Approval: **July 07, 2023**

PIA ID Number: **8023**

SYSTEM DESCRIPTION

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

WebApps Enterprise Services, WAES

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?

Web Apps Enterprise Services, WAES, #7296

What is the approval date of the most recent PCLIA?

11/7/2022

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Significant System Management Changes

Were there other system changes not listed above?

Yes

What were those changes?

As Business Online Account (BOLA) and Clean energy are under WAES. Added features update related to them since BOLA provides a set of features with similar functionality as Online Account (OLA), but services Business taxpayers instead of individuals and the clean energy special handling set of features provides a set of features to allow taxpayers to claim energy credits provided by new legislation.

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

Web Applications (WebApps) Governance Board and Strategic Development Executive Steering Committee. This artifact update is for the Integrated Readiness Review.

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

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: a) See balance due, b) See payment status / history, c) Make a payment, d) Get tax records, and e) Apply and Modify installment agreement/payment plan, f) Authorizations, g) Digital Notices and Letters, h) Business Online Account (BOLA): Federal Contractor Tax Check System (FCTCS), and Green Energy Special handling: Clean Vehicle manufacturer registration, Clean Vehicle dealer registration, Clean Vehicle Credit transactions, and Elective Payment transfers. 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. * 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. This is a security update to the database which is currently the PII storage solution.

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:

Security Background Investigations

Statistical and other research purposes

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

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

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.

Employer Identification Number

Other Taxpayer Identification Number

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

Yes

Specify the PII Elements:

Name
Mailing Address
E-mail Address
Internet Protocol Address (IP Address)
Vehicle Identifiers
Financial Account Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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.

Official Use Only (OUO) or Limited Official Use (LOU) - Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Protected Information - Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Criminal Investigation Information - Information concerning IRS criminal investigations or the agents conducting the investigations.

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

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII about individuals for Bank Secrecy Act compliance 31 USC

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.

WAES establishes a single WebApps Enterprise Services enabling taxpayers to view, update, and retrieve their tax information. The SSN is used as an access key to retrieve and update information in other IRS systems (e.g., transcript and payment information). WAES leverages the Web Apps Platform services for auditing, analytics, and other non-functional system reporting needs. Web Apps Platform services include: 2. Usage statistics- Web and business analytics are critical components for Web Apps and target platform. Employing analytics allows the IRS the ability to improve the website's usability as well as make business decisions that improves business processes and user experiences. In addition, analytics benefits business units with recommendations and promotions, user trends analysis, fraud management, and business intelligence. SSNs are required to uniquely identify individuals impacted by or associated with website activity. 3. 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, so SSNs must be used to cross correlate any fraudulent activity. Each application transaction is recorded as an audit event, extracted, and sent to Security Auditing and Analysis System (SAAS) to prove audit trail for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and Cybersecurity. 4. 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. 5. 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.

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

The data that WAES receives is from internal IRS systems which are deemed reliable, and the data is validated for accuracy by the system sending the data as described in that system's PCLIA.

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 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
IRS 00.001	Correspondence Files and Correspondence Control Files

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: Secure Access Digital Identity (SADI)
Current PCLIA: Yes
Approval Date: 6/2/2023
SA&A: Yes
ATO/IATO Date: 5/22/2022

System Name: eAuthentication (eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 9/15/2022

System Name: Web Applications Platform Environment
Current PCLIA: Yes
Approval Date: 1/14/2022
SA&A: No

System Name: Standardized IDRS Access
Current PCLIA: Yes
Approval Date: 5/4/2023
SA&A: No

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?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Bank of America Merrill Lynch (BAML)
Transmission Method: Bank of America Merrill Lynch (BAML)
ISA/MOU: No

Organization Name: First Data Corporation (FDC)
Transmission Method: First Data Corporation (FDC)
ISA/MOU: 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?

Yes

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

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: eAuthentication (eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 9/15/2022

System Name: Security Audit Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

System Name: Cybersecurity Data Warehouse (CSDW)
Current PCLIA: Yes
Approval Date: 4/22/2022
SA&A: Yes
ATO/IATO Date: 5/31/2021

System Name: Web Applications Platform Environment
Current PCLIA: Yes
Approval Date: 1/14/2022
SA&A: No

System Name: Secure Access Digital Identity (SADI)
Current PCLIA: Yes
Approval Date: 6/10/2021
SA&A: Yes
ATO/IATO Date: 8/23/2021

Identify the authority.

IRC Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 - collecting SSN information cyber security compliance.

For what purpose?

WAES gives taxpayers access to abstracted taxpayer information residing on IRS Core systems. 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 SAAS to prove audit trail for TIGTA, CI, and Cybersecurity. User transaction (requests/responses) will be audited per Cyber Security compliance through Enterprise Security Audit Trails (ESAT)process. Data will be disseminated to CSDW and ESAT.

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

No

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

No

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

Yes

Identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: WebApps Enterprise Services
Transmission Method: Through an application programming interface created to send payment information to and from the Treasury financial agent for processing
ISA/MOU: Yes

Identify the authority.

IRC 6103(h)(1)

For what purpose?

Yes

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

Yes

Does this system disseminate SBU/PII to other Sources?

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?

12/1/2021

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Single Factor Identity Validation

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 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: 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.

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):

The taxpayer's use of the web application is voluntary. The Secure Access (e-Authentication/SADI) application, which is the required entry point to taxpayer applications, will require the taxpayer to click on the "Consent" button provided on the website before being allowed to proceed.

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

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

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

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Only

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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 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 was obtained through the On-Line 5081 (OL5081) process, these requests now must go through Business Entitlement Access Request System (BEARS). All access must be approved by the user's manager who reviews the OL5081/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 OL5081/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.

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.

WAES is non-recordkeeping and does not require a NARA-approved records control schedule to affect data disposition. Web Apps Platform is only used to onboard new software initiatives and provide the tools necessary to manage applications and services used directly by taxpayers. The IRS Secure Access (eAuthentication/SADI) platform leveraged by Web Apps Platform was approved by NARA under Standard Form 115 (Job No. N1-58-12-6, approved 11/14/2012), updating RCS 17 by adding item 31. WebApps Enterprise Services uses GRS references for Inputs, Outputs, and System Documentation. Listed below are the GRS references: Inputs are covered in GRS 5.2, item 020 for electronic inputs. Outputs are covered in GRS 5.2, item 020 for data files, and GRS 5.2, item 020 for ad hoc output reports. System Documentation is covered in GRS 3.1, item 051. System Access Records for Audit, Usage, and Extracts are covered under GRS 3.2, item 030. GRS 5.1 and 5.2 replaced rescinded items in GRS 4.3.

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?

12/1/2021

Describe the system's audit trail.

An Audit Plan has been created for this system by the project team with the support of Enterprise Security Audit Trail (ESAT)/SAAS. 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/SAAS logs for Cybersecurity review.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Test Strategy Implementation Plan (TSIP) is used in place of system test plan.

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

By using taxpayer supplied PII and IP Addresses, the IRS will have the capability to identify, locate, and monitor taxpayers. The primary purpose of doing this is to correlate website usage with other IRS processes. For example, tracking notice response rates.

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?

Yes

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.

Not Applicable