Date of Approval: **January 14, 2022**

PIA ID Number: **6351**

SYSTEM DESCRIPTION

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

Web Applications Platform Environments, WebApps Platform

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 Applications Usage Statistics, Web Stats, PCLIA #3565

What is the approval date of the most recent PCLIA?

8/7/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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?

No

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.

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 as a result 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 down 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.

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

Interfaces with external entities that require the SSN

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).

There are no current plans to eliminate the use of SSNs. All taxpayer interactions with this system will take place through secure means and require identification through the IRS' secure access eAuthentication systems. 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
Phone Numbers
E-mail Address
Date of Birth
Place of Birth
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)

Internet Protocol Address (IP Address)
Criminal History
Certificate or License Numbers
Passport Number
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.

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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

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.

1. The SSN is used as an access key to retrieve and update information in other IRS systems (e.g., transcript and payment information). 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. 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. 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. 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 copies 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. 6. Mailing Address, Phone Numbers, and E-mail Address are used to verify identity and contact user. 7. Date of Birth is used to verify identity of user. 8. Internet Protocol Address (IP Address) is used to verify user, analytics (see 2), and cybersecurity (see 4). 9. Financial Account Numbers, Tax Account Information, and Centralized Authorization File (CAF) are required for core business functionality of the application.

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

The data that Web Apps Platform 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 00.001 Correspondence Files and Correspondence Control Files

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 22.062 Electronic Filing Records

IRS 22.061 Information Return Master File

IRS 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 34.037 Audit Trail and Security Records

IRS 37.006 Correspondence, Miscellaneous Records, and Information Management Records

IRS 37.111 Preparer Tax Identification Number Records

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: eAuthentication (eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 6/30/2020

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

System Name: Online Account (OLA)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 6/13/2018

System Name: Returns Inventory and Classification System (RICS)
Current PCLIA: Yes
Approval Date: 7/10/2020
SA&A: Yes
ATO/IATO Date: 12/6/2019

System Name: Federal Investigative Standards (FIS)
Current PCLIA: Yes
Approval Date: 3/29/2018
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?

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: Common Business Services Release 1 (CBS)
Current PCLIA: Yes
Approval Date: 8/23/2019
SA&A: Yes
ATO/IATO Date: 8/15/2016

System Name: Cybersecurity Data Warehouse (CSDW)
Current PCLIA: Yes
Approval Date: 2/5/2021
SA&A: Yes
ATO/IATO Date: 4/10/2020

System Name: Returns Inventory and Classification System (RICS)
Current PCLIA: Yes
Approval Date: 7/10/2020
SA&A: Yes
ATO/IATO Date: 12/13/2019

System Name: Online Account (OLA)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 6/13/2018

System Name: Federal Investigative Standards (FIS)
Current PCLIA: Yes
Approval Date: 3/29/2018
SA&A: No

System Name: eAuthentication (eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 6/30/2020

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

Identify the authority.

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

For what purpose?

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., CBS, 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 SAAS to prove audit trail for TIGTA, CI, and Cybersecurity.

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?

No

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?

8/5/2015

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Knowledge Based Authentication (Out of Wallet)

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. 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).

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 e-Authentication 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 process rights on the tax forms.

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

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

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.

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.

WebApps Platform 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 eAuthentication 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. Online Account uses GRS references for Inputs, Outputs, and System Documentation. Listed below are the GRS references: Inputs are covered in GRS 4.3, item 020 for electronic inputs. Outputs are covered in GRS 4.3, item 031 for data files, and GRS 4.3, item 030 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.

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?

6/13/2018

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?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

IRS WebApps and SharePoint.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The system will go through a continuous Testing Strategy Implementation Plan due to its ongoing development. It will be assessed against the selected privacy requirements. To accomplish this, the project not only addresses the overarching Privacy Requirements but will break down the requirements to decomposed requirements that are reviewed, implemented, tested, and documented to ensure appropriate action was taken to address them. All of this is being coordinated by the Requirement Engineering Program Office and Cybersecurity and tracked in the Rational Requirements Tool and developer security (SA-11) testing. Please note that authentication is delegated to the eAuthentication system. The project uses the eAuthentication project services to authenticate taxpayer access to the applications. In authenticating, the user will log in through the Browser and Presentation Application. The eAuthentication process will access the External Identity Store through the External Policy Server for permission enforcement. Please refer to the eAuthentication PCLIA for applicable information.

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?

No