Date of Approval: **December 03, 2021**

PIA ID Number: **6547**

SYSTEM DESCRIPTION

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

WebApps Enterprise Service Income Verification Exp, WAES-IVES

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?

TFA IVES is 6204

What is the approval date of the most recent PCLIA?

8/10/2021

Changes that occurred to require this update:

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 (GB) and Strategic Development Executive Steering Committee (SD ESC). The Web Apps GB was chartered by the SD-ESC and governs all Web Apps investments and any associated investments or components as deemed appropriate by the SD-ESC. This PCLIA artifact update is for the Product Planning Readiness Review.

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

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.

As part of the Taxpayer First Act (TFA) Provision 2201 Income Verification Express Service (IVES), taxpayers will have access to a web interface that is integrated with the existing Online Account authorizations tab to authorize the release of their income transcripts to IVES Participants. This functionality will give taxpayers the option to authorize or reject the Form 4506-C submitted by the IVES Participant. WAES-IVES will integrate with Forms Based Processing (FBP) to display and verify taxpayer transcript request information as well as the Electronic Signature Storage and Archival Repository (ESSAR) to provide an electronic signature approval. This web interface will go live along with the broader IVES solution in January 2023.

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)

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

The Online Account IVES feature requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer and/or representative. SSN are permissible from the Internal Revenue Code (IRC) 6109, which requires taxpayers to include their SSNs on their income tax returns. There is no mitigation strategy to mitigate or eliminate the use of the SSN on the system.

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 system(s). The Office of Management and Budget memorandum 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. WAES-IVES requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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
Internet Protocol Address (IP Address)
Certificate or License Numbers
Tax Account Information

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

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.

The SSN is required for the transcript disclosure of tax information for third party (i.e., Mortgage lenders) to verify taxpayers' income. The residential mortgage industry provides loans to millions of taxpayers each year to purchase homes or to refinance existing loans. The Internal Revenue Service ("IRS"), by providing tax transcript information, serves an important role in the lending process. The Taxpayer First Act requires automation of the existing process to provide near real-time responses, will result in significant improvements for taxpayers seeking to purchase a new home. The mortgage industry provides standards of what lenders are to use when obtaining taxpayer consent to share tax information. The automation required by Section 2201 will be an improvement over the fax submission process and multiple day turn-around timeframes; the IVES solution will automate the IVES process for providing qualified disclosures of income to authorized parties to be completed to as close as real time as possible. Handling of PII is protected using standard security mechanisms and any access point to data containing PII requires authentication and role-based authorization. PII is limited to collecting and storing minimal PII from taxpayer records solely for audit and other authorized purposes.

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

Accuracy: Business rules such as TIN Match and address verification are jointly used to verify the accuracy of the PII data. IVES performs the validation of these business rules against the input data provided by the Participant before generating the transcripts for the accuracy of the PII data. Timeliness: IVES generates the transcript and provides the capability for the Participant to retrieve the transcript in close to real time, after the Taxpayer provides consent. The Participant will have the capability to retrieve the transcript multiple times within a 120-day period. Completeness: IVES verifies the availability of the Taxpayer data for the requested years/periods and provides the transcript information if available. If the Taxpayer data is not available for the years/period requested, "No Data Found" will be sent to the Taxpayer. The taxpayer will also have functionality to edit certain fields associated with their TIN, such as address, and post those values back to FBP via API for accuracy.

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 34.037 Audit Trail and Security 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: IVES Form Based Processing System
Current PCLIA: Yes
Approval Date: 6/16/2021
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?

Yes

Please identify the form number and name:

Form Number: 4506-C
Form Name: IVES request for transcript of tax return

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: Form Based Processing (FBP)
Current PCLIA: No
SA&A: No

System Name: Electronic Signature Storage and Archival Repository (ESSAR)
Current PCLIA: No
SA&A: No

System Name: Secure Access Digital Identity (SADI)
Current PCLIA: Yes
Approval Date: 10/14/2021
SA&A: Yes
ATO/IATO Date: 6/16/2021

Identify the authority.

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

For what purpose?

OLA 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 Security & Audit Analysis System (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?

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?

3/1/2021

What was the approved level of authentication?

Level 3: High confidence in the asserted identity's validity

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 taxpayer is notified by the mortgage banker that there is a pending request for the release of their tax information.

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 IVES system will provide the capability to decline disclosure authorization within Online Account (OLA). They are provided the ability to either consent or decline the release of requested information.

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

The IVES system will be protected by the appropriate level of authentication and authorization services. For the existing Online Account application, this is performed via an interface with eAuth/SADI. The addition of this new IVES verification service will not alter in any way the mechanism used for Online Account taxpayer Identity and Access Management (I&AM).

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: Read Only

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 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 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.

OLA 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?

9/30/2021

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?

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)?

Web Apps Testing System Implementation Plan

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 SADI system. The project uses the SADI project services to authenticate taxpayer access to the applications. In authenticating, the user will log in through the Browser and Presentation Application. The SADI process will access the External Identity Store through the External Policy Server for permission enforcement. Please refer to the SADI 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?

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.

Yes