Date of Approval: **August 06, 2020**

PIA ID Number: **5233**

SYSTEM DESCRIPTION

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

TPP IDVerify, ID Verify

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?

TPP IDverify, PIAMS # 2831

What is the approval date of the most recent PCLIA?

9/7/2017

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 Apps Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

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.

The Taxpayer Protection Program Identity Verification Service (TPP ID Verify) allows taxpayers that are potential victims of identity theft to verify their identity online and continue to process the tax return to either release the refund or cancel it. TPP ID Verify web-based tool will authenticate a subset of taxpayers who receive a 5071C (or similar) letter and acknowledges they did not file a return, a refund was already received, they filed a balance due return, or they did file a refund return. If the taxpayer is eligible to use the application and responds to the TPP specific questions, the website will display different screens to inform the taxpayer of the next steps. The taxpayer's answers will confirm whether the taxpayer is a victim of ID Theft. The return selected by Taxpayer Protection Program (TPP) can then be archived or processed. A list of eligible taxpayers will be provided by Return Integrity & Compliance Services (RICS) to Web Apps, so that only eligible taxpayers will be able to use ID Verify. Web Apps will provide RICS a daily list of responses from successfully authenticated taxpayers.

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:

When there is no reasonable alternative means for meeting business requirements

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

The TPP ID Verify 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. The TPP ID Verify 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.

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

Internet Protocol Address (IP Address)

Financial Account 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

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.

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 IRS must collect PII, in order to determine whether a selected tax return is a legitimate or identity theft return. A taxpayer's SSN is used to link a taxpayer's response in ID Verify to the tax return selected by the Taxpayer Protection Program.

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

Taxpayers are notified by postal mail that they may access this system to verify their identity. Taxpayer identities are verified using the e-Authentication system using processes that meet NIST 800-63 standards. Self-asserted PII by taxpayers in ID Verify is compared to tax return data on-file with the IRS. The IRS verifies accuracy of the transmission of the files to and from RICS via audit logs and other system monitoring.

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 34.037 Audit Trail and Security Records

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 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation Files

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: Customer Account Data Engine (CADE) 2
Current PCLIA: Yes
Approval Date: 10/30/2019
SA&A: Yes
ATO/IATO Date: 7/9/2019

System Name: Online Account (OLA)
Current PCLIA: Yes
Approval Date: 9/21/2018
SA&A: Yes
ATO/IATO Date: 6/13/2018

System Name: Taxpayer Protection Program Db (TPP Db)
Current PCLIA: Yes
Approval Date: 6/19/2018
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?

Yes

Please identify the form number and name:

Form Number: 1040 Form Name: U.S. Individual Income 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: Cyber Security Data Warehouse
Current PCLIA: Yes
Approval Date: 11/3/2017
SA&A: No

System Name: Taxpayer Protection Program Db (TPP Db)
Current PCLIA: Yes
Approval Date: 6/19/2018
SA&A: No

Identify the authority

Internal Revenue Code (IRC) Section 6109 - collecting SSN information.

For what purpose?

Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a) - process taxpayer information. This supports processing of tax returns.

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?

8/7/2017

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 Protection Program Identity Verification Service (TPP ID Verify) allows taxpayers that are victims of potential tax filing fraud to verify their identity online. IRS will send a 5071C (or similar) letter requesting more identity information prior to processing a return and issuing a refund. If the taxpayer is eligible to use the application and responds to the Taxpayer Protection Program (TPP) specific questions, the website will display different screens to inform the taxpayer of the next steps.

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):

Taxpayers can choose to call the toll-free IRS number to verify or they can decline from entering the web portal.

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: Read Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Read Write

How is access to SBU/PII determined and by whom?

All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, access to ID Verify data 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 on need-to-know. For non-production supporting environments users must complete the necessary SBU (live) data training, request access through the OL5081, and in some cases as outlined by the requirements set forth within the IRM submit an elevated access letter that is approved by the Associate Chief Information Officer (ACIO) 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 when accessing the system containing taxpayer 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.

The IRS eAuthentication platform leveraged by ID Verify was approved by National Archives and Record Administration (NARA) under SF115 (Job No. N1-58-12-6, approved 11/14/2012), updating RCS 17 by adding item 31. ID Verify 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?

11/5/2019

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 Trails (ESAT)/Security Audit and Analysis System (SAAS). It records all actions of the taxpayer/user in near-real-time and transmits to SAAS/ESAT logs for Cyber security Operations review. Audit Plan for OLA is stored in SharePoint (SP).

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)?

Test results are stored in Rational CLM (Collaborative Lifecycle Management).

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 agile development methodology. 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 this is being coordinated by the Requirement Engineering Program Office (REPO) and Cybersecurity and tracked in the Rational Requirements Tool and developer security (SA-11) testing.

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 plus IP Addresses, the IRS may have the capability to identify and locate taxpayers. Audit trails will track all accesses to data. Access to this data is protected though access controls including OL5081.

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