Date of Approval: September 07, 2017 PIA ID Number: **2831**

A. SYSTEM DESCRIPTION

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

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

Yes	Vision & Strategy/Milestone 0
Yes	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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 receives a 5071C letter and acknowledges they did not file a return, a refund was already received, or the return they filed was a balance due return. This will confirm whether the taxpayer is a victim of ID Theft. The return selected by Taxpayer Protection Program (TPP) can then be archived. RICS will provide Web Apps an authorized user list weekly. Web Apps will provide RICS a daily list of successfully authenticated taxpayers who did not file a return, already received their refund, or who filed a balance due return. eAuthentication will be used to verify a taxpayer's identity. 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 website should track a taxpayer's activity and response throughout the user flow. The complete application should be available in English and Spanish (Spanish support depends on future business prioritization), be Section 508 compliant, be mobile-friendly, include Accessibility & Privacy Policy links where applicable, include Google Analytics, create required audit logs at a TIN level, and integrate IRS e-File Device ID code.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
No Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Practitioner Tax Identification Number (PTIN)

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 SSN's 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.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No

No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

IRS will be collecting PII from the consumer as part of the IRS identity verification services pilot. Identity proofing elements, as defined by NIST 800-63, are needed to ensure the consumer's identity can be verified at NIST Level of Assurance 2 (LOA2) as well as provide IRS with requested fraud analysis to identify and deter fraudulent usages of the IRS system. IRS requires a subset of the PII collected during identity verification will be sent to RICS so RICS can connect the identity proofing attempts with the IRS TPP record and input necessary transaction codes to complete the IRS transaction.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

Taxpayers are notified by mail that they may access this system to verify their identity. The purpose of the IRS system is to verify individuals against NIST 800-63 LOA2 standards for identity proofing consumers through address of record non-repudiation, phone confirmation, fraud checks, user registration, and authentication for Levels of Assurance (LOA2). IRS verifies accuracy of the transmission of the flat file to RICS via audit logs and encryption capabilities. In order to meet NIST 800-63-3 requirements, the system verifies citizen asserted PII against authoritative records, in this case commercial credit agencies. The system only sends asserted PII and receives verification data from source.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security Records System
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 Accounts 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

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Online Account (OLA)	Yes	12/23/2016	Yes	11/15/2016
Taxpayer Protection Program Db (TPP Db)	Yes	12/10/2014	No	
CADE 226	Yes	11/06/2015	Yes	11/20/2016

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? Yes

If **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	Transmission method	ISA/MOU
Commercial Credit Reporting Agencies	Electronic	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Cyber Security Data Warehouse	Yes	08/14/2014	Yes	09/07/2016
Taxpayer Protection Program Db (TPP Db)	Yes	12/10/2014	No	

Identify the authority and for what purpose? Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 – collecting SSN information.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? Yes

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

Organization Name	Transmission method	ISA/MOU
Commercial Credit Reporting Agencies	electronic	Yes

Identify the authority and for what purpose? Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a) - process taxpayer information.

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? Yes

16. Does this system/application interact with the public? Yes

16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16a1. If **yes**, when was the **e-RA** conducted? 08/07/2017

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

Single Factor Identity Validation

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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 letter requesting more identity information prior to processing a return and issuing a refund. eAuthentication will be used to verify a taxpayer's identity. 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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **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.

19. 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.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	Yes	Read-Only	Moderate
Contractor Sys. Admin.	Yes	Read and Write	Moderate
Contractor Developers	No		

21a. 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 they enter 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 IDverify 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 where they are restricted to see certain taxpayer data and in many instance a third-party tool is implemented to restrict access to that data Access is determined by Service Now and OL5081 for the contractor owned systems (Integrated Enterprise Portal).

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

Online Account is non-recordkeeping and does not require a NARA-approved records control schedule to affect data disposition. Online Account is a web-based lookup tool on the IRS internet for reference use directly by taxpayers. All features are Read Only. The IRS eAuthentication platform leveraged by OLA was approved by NARA under SF115 (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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system s audit trail. An Audit Plan has been created for this system by the project team with the support of ESAT/SAAS. It records all actions of the taxpayer/user in near-real-time and transmits to SAAS/ESAR logs for Cyber security Operations review. Audit Plan for OLA is stored in SP.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 11/30/2018

24.3 If **completed/ or in process,** 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 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. Please note that authentication is delegated to the eAuthentication system. Please refer to the eAuthentication PCLIA for applicable information

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

If **yes,** provide the date the permission was granted.

If **no**, explain why not. We are completing Form 14664 and expect to have the process completed by October 11, 2017.

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments?

If **no**, explain why not.

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? Yes

If **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 will have the capability to identify, locate, and monitor taxpayers. Audit trails will track all accesses to data. Access is protected though access control means by including OL5081 please refer to question 21a.

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report