
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Return Preparer Registration - Identity Verification Service, RPR-IVS

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

RPR-IVS, PIAMS # 1461

Enter the approval **date** of the most recent PCLIA. 10/22/2015

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

- No Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
- No Conversions
- No Anonymous to Non-Anonymous
- No Significant System Management Changes
- No Significant Merging with Another System
- No New Access by IRS employees or Members of the Public
- No Addition of Commercial Data / Sources
- No New Interagency Use
- No Internal Flow or Collection
- Yes Expiring PCLIA

Were there other system changes not listed above? No

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

W&I Division Executive Resource Board

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

- No Vision & Strategy/Milestone 0
- No 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
- Yes Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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.

RPR-IVS was implemented to provide authentication as requested by Return Preparer Office for return preparers. The identity verification is done based on the successful matching of applicants: SSN, first and last name, date of birth, address and filing status match based on the tax return year, as entered by the applicant/user. RPR-IVS sends a true/false response back to the external application, TPPS - Tax Professional Preparer Tax Identification Number (PTIN) System, based on the result of the user authentication.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No Security background investigations
No Interfaces with external entities that require the SSN
Yes Legal/statutory basis (e.g. where collection is expressly required by statute)
No When there is no reasonable alternative means for meeting business requirements
No Statistical and other research purposes
No Delivery of governmental benefits, privileges, and services
No Law enforcement and intelligence purposes
No Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

The SSN is used to authenticate. After authentication the user is assigned an EIN or TIN to conduct business. RPR-IVS does receive and store PII, but only in the backend behind firewall.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The SSN is used to authenticate. After authentication the user is assigned an EIN or TIN to conduct business. RPR-IVS does receive and store PII, but only in the backend behind firewall.

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

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
No	E-mail Address
Yes	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system.

Filing Status and Federal Tax Information.

6.e. 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

6.f. 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.

RPR-IVS contains personally identifiable information (PII) such as the name, date of birth, and social security number. The SBU/PII elements used are keys to successfully authenticate tax return preparers/taxpayers. Without ID proofing, the TPPS system cannot issue PTINs to tax return preparers to conduct business.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

Accuracy: Data entered for all e-Services Products is processed and error checked at multiple levels throughout e-Services transactions to ensure accuracy. The successful authentication and authorization of the third-party user of the system provides the first level of data verification entered on behalf of the taxpayer. The second level consists of Internet browser surface editing as the user inputs data for submission to the application. The relevant e-Services server will conduct a third check on user entered data. Finally, the application will match data against the systems to determine validity. Completeness: Data fields required for successful interactive e-Services transactions will undergo checks during online input. The application will not allow the user to submit incomplete requests and will provide them the ability to edit incorrect data prior to final submission. Timeliness: The data received from other IRS systems for the purposes of validation are updated on a daily or weekly basis to ensure that the information entered is current. Once the data is collected and validated, the data is kept as current as the user who provides it.

C. 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.

9. 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

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

<u>SORNS Number</u>	<u>SORNS Name</u>
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security Records System
IRS 37.111	Preparer Tax Identification Number Records

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNS please email *Privacy.*

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

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

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

<u>System Name</u>	<u>Current PCLIA</u>	<u>Approval Date</u>	<u>SA&A?</u>	<u>Authorization Date</u>
eServices	Yes	04/20/2018	Yes	05/30/2018

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

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

11.d. Does the system receive SBU/PII from other sources? No

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

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

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? No

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, Radio Frequency Identification (RFID), etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. 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 information is not collected directly from individuals. RPR-IVS does not send any notices directly to the taxpayers. The information collected is obtained from related IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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

18.a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):

The information is not collected directly from individuals. RPR-IVS does not send any notices directly to the taxpayers. The information collected is obtained from related IRS databases and files, which in turn are tax forms filed by tax entities. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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

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

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

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

22.a. 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.

RPR-IVS data is approved for destruction under National Archives and Records Administration (NARA) Job No. NC1-58-77-4 and published in IRS Document 12990 under Records Control Schedule (RCS) 29 for Submissions Processing Campus Records, item 85. System administrators and business unit representatives ensure the RPR-IVS system recordkeeping is in compliance with instructions outlined in RCS 29. Should any updates or modifications to approved retention requirements be necessary to meet or accommodate RPR-IVS data collection and maintenance needs, the business owner/developer coordinates with the IRS Records and Information Management (RIM) Program Office, to discuss and seek approval for those changes as appropriate.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If **yes**, what date was it completed? 05/20/2018

23.1. Describe in detail the system's audit trail. Application-level audit trails monitor and log user activities. At a minimum, an event record shall specify the following: Data files opened and closed; Specific actions, such as reading, editing; and Deleting records or fields, and printing reports. The Security Audit Automatic Response and Auditable Events requirements applications which process any type of or subset of PII (e.g., taxpayer, personnel, financial) data shall capture and record the following application transactional information in audit trails: Employee and contractor transactions that add, delete, modify, or research a tax filer's record. Employee and contractor transactions that add, delete, modify, or research an employee's record (personnel and financial). Employee and contractor transactions that add, delete, or modify an employee's access to Employee User Portal (EUP), including changes to EUP roles or sub-roles. Any system transactions that alter an employee's access to the EUP, or a system's or application's role or sub role. Any employee or contractor transactions identified by the system owner as requiring additional oversight. Any third-party transactions identified by the system owner as requiring additional oversight.

J. PRIVACY TESTING

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

24.a. If **yes**, if yes, was the test plan completed? Yes

24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIT (Web-based document management system)

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? System is currently in operational and maintenance stage. Application has been through Systems Acceptability Testing (SAT) and Application Qualification Testing (AQT) testing.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees: 50,000 to 100,000

26.b. Contractors: 5,000 to 10,000

26.c. Members of the Public: More than 1,000,000

26.d. 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 Recommendations of the 9/11 Commission 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? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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
