

NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 01/02/2014 PIA ID Number: 681

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Identity Protection Pin MS 4b, IPPIN

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The Identity Protection Pin system is a web based application designed to provide a pin to the taxpayers that are victims of identity theft and also for the residents of three states that have high identity theft rate. This pin will be used by taxpayers to file their tax return and prevent fraudulent tax return filing. Taxpayers will have to be authenticated and registered in e-authentication interface prior to accessing IPPin application. Taxpayers are also checked for authorization to use the IPPin application based on the Id theft marker and state of residence. Upon successful authorization, taxpayers are further authenticated by e-auth interface through knowledge based questions. Once taxpayers answer knowledge based questions successfully, the IPPin is displayed to them. Taxpayers can use this pin to file their tax return immediately. Due process is provided administratively by title 26 outside of the system.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) No

6a. If Yes, please indicate the date the latest PIA was approved:

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)
 - System is undergoing Security Assessment and Authorization
-

6c. State any changes that have occurred to the system since the last PIA

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes
 Employees/Personnel/HR Systems No
 Other Yes

Other Source:
CFOL, E-Authentication

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name On Public? On Employee?

IPPIN Yes No

10a. Briefly describe the PII available in the system referred to in question 10 above.

IPPIn

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IPPIn application does not contain SSN. It only uses it to retrieve Taxpayer information from CFOL.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

N/A

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

N/A

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Audit Data is sent to SAAS for certain fields as required by 10.8.3. The logs are then reviewed by Cyber Security.

11a. Does the audit trail contain the Audit Trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If Yes, *specify*:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

IPPin retrieved is displayed to the user. PII data retrieved is used to look up rest of the Taxpayer Data and IPPin from IMF and NAP. Rest of the PII data is used as part of the transaction that updates account information when new ippin is generated.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration No

To provide Taxpayer Services Yes

To collect Demographic Data No

For employee purposes No

Other: No

If other, what is the use?

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? Yes

17. Does the website use any means to track visitors' activity on the Internet? Yes

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	<u>No</u>	_____
Web Beacons	<u>No</u>	_____
Session Cookies	<u>Yes</u>	_____
Other:	<u>Yes</u>	<i>If other, specify:</i> <u>MIS Data</u>

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Yes

18a. If Yes, how is their permission granted?

Individual voluntarily choose to use the system. They may elect not to use it.

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	_____
Website Opt In or Out option	_____
Published System of Records Notice in the Federal Register	_____
Other:	_____

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u></u>
System Administrators		<u></u>
Developers		<u></u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?

23. How is access to the PII determined and by whom?

- Taxpayers who chose to utilize eAuthentication services and register with the system have write access to their own user profile only. – eAuth system administration is performed by IRS Enterprise Operations(EOps) group. IRS EOps operations can be performed by IRS employees and/or contractors. At present PII information is not viewed by contractors. Access to eAuth system is granted via the Online 5081 process

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

PII is submitted directly by the taxpayer user. Once the user inputs their PII data, it gets validated against the IRS internal data source ICCE (validating they are who they say they are) .If the information is not available for the users (Non-Filers) their PII data is validated against third party(Equifax) data providers . PII information is validated via Java code and scripts for data formats. Drop down menus and syntax requirements are enforced throughout the application to ensure the accuracy and completeness of data input.

25. 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? No

25a. 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.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

The IPPin system is non record keeping. It generates IPPin dynamically if one is not found for the taxpayer. Audit Trail Data is maintained in SAAS for seven years in accordance with NARA Job No. N1-58-10-22, approved 4/5/2011 (published under RCS 19 for Martinsburg Computing Center, item 88).

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The PII data that is used within the system is physically secured as the servers are behind firewall.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

It is taxpayer's responsibility to ensure that they do not share their IPPin with anyone else.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

IPPin sends Security Audit Records to SAAS on a continuous basis. Audit Trails sent on a continuous basis and meets or exceed IRS & FISMA requirements for security.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 24.030 IMF

Treas/IRS 34.037 IRS Audit Trail and Security Records System

Comments

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

32a. If Yes to any of the above, please describe:

NA

[View other PIAs on IRS.gov](#)