Date of Approval: **November 07, 2022**

PIA ID Number: **7289**

SYSTEM DESCRIPTION

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

Identity Protection Pin, IPPIN

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?

Identity Protection Pin, MS4b

What is the approval date of the most recent PCLIA?

12/16/2019

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.

SBSE 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?

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.

Identity Protection Pin (IPPIN) is a web-based application designed to provide a PIN to the taxpayers that are victims of identity theft Nationwide. 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 or id.me interface prior to accessing IPPIN application. Taxpayers are also checked for authorization to use the IPPIN application based on the Id theft marker. Upon successful authorization, taxpayers are further authenticated by e-auth/SADI 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.

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:

Delivery of governmental benefits, privileges, and services

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

IPPIN requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. 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. IPPIN requires the use of SSN's because no other identifier.

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
E-mail Address
Date of Birth
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.

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.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

One of the changes that was made for Fiscal year '20 is the inclusion of the Taxpayers name on the header of the IPPIN pages.

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.

IPPIN does accept any input from the Taxpayer. The SSN and Name data is provided by eAuth system. The SSN is needed to access Taxpayer Account records from the CFOL (Corporate Files On Line) and the NAP (National Account Profile). CFOL data is used to confirm a Taxpayer is eligible to use IPPIN. An IPPIN generated for a Taxpayer without one is written to the NAP. The Taxpayer's Name is displayed only on the page that displays the Taxpayers IPPIN to confirm for the Taxpayer who's IPPIN is being shown.

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

PII is submitted directly by the taxpayer user. Once the user inputs their PII data, it gets validated against the IRS internal data source Integrated Customer Communication Environment (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.

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

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: Individual Master File
Current PCLIA: Yes
Approval Date: 3/4/2020
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: Standard CFOL Access Protocol, SCAP
Current PCLIA: Yes
Approval Date: 4/12/2022
SA&A: No

System Name: National Account Profile
Current PCLIA: Yes
Approval Date: 2/27/2020
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: 15227
Form Name: Application for an Identity Protection Personal Identification Number (IP PIN)

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: E-Authentication (eAuth)
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 6/30/2020

System Name: National Account Profile
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: Yes
ATO/IATO Date: 9/11/2019

Identify the authority.

26 USC 6109 Identifying Numbers or 26 USC 6011(b). Taxpayers will have to be authenticated and registered in e-authentication interface prior to accessing IPPIN application.

For what purpose?

This PIN will be used by taxpayers to file their tax return and prevent fraudulent tax return filing.

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?

12/20/2017

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Knowledge Based Authentication (Out of Wallet)

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?

Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

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):

Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

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

The information within IPPIN comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. IPPIN does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

IRS Contractor Employees

Contractor System Administrators: Read Only

Contractor Developers: Read Write

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

No external users have access to the system data. The Treasury Inspector General for Tax Administration can receive system data information by going through the proper channels. They do not have direct access to the system. Contractors, including Developers, will not have direct access to the IPPIN production system or database. Contractors receive a completed Moderate risk background investigation for staff-like access approval. Only IRS System Administrators will have access to the production environment. However, Developers are available to help System Administrators troubleshoot technology problems. In these cases, the System Administrator will provide the necessary information to the Developer so he/she can assist with the problem, which is considered indirect access since the System Administrator will provide the Developer with the necessary information as opposed to the Developer being able to access it directly. 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.

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.

IPPIN writes logging records to the Management Information System (MIS) maintained by Integrated Customer Communication Environment (ICCE). These records are not deleted or archived. 1040X master data file and associated records will be disposed of in accordance with Records Control Schedule (RSC) 29 for Tax Administration- Wage & Investment, Item 55-56. Recordkeeping copies of system data will be destroyed on or after January 16, 6 years after the end of the processing year (Job No. N1-058-95-001). The media that contain the

data are degaussed and then destroyed. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. A control log is maintained containing the media label ID, date and method of destruction, and the signature of the person who destroyed the media

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?

5/29/2019

Describe the system's audit trail.

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 Security Audit and Analysis System (SAAS) or Splunk in the future 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).

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)?

Documents are placed in DocIt, online repository.

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?

IPPIN has been tested through the Annual Security Controls Assessment. During the ASCA cyber tests all source code scans, server scans, web application scans. All vulnerabilities are identified and worked for mitigation.

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?

No

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