Date of Approval: December 28, 2016 PIA ID Number: **2031**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Identity Protection PIN, IPPIN

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Identity Protection OIn MS 4b, IPPIN, 623

Next, enter the **date** of the most recent PIA. 1/8/2014

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

No	**Addition of PII**
Yes	**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**

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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.

IPPIN 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.

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 Yes 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)**
No	**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).

This application only displays the last 4 digits of Social Security Number (SSN) (first 5 digits are masked). The application cannot mitigate the use of SSNs until an alternate identifier has been adopted by the IRS to identify taxpayers.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	**Name**	**Yes**	**No**	**No**
Yes	**Mailing address**	**No**	**No**	**No**
No	**Phone Numbers**	**No**	**No**	**No**
No	**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**
No	**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**
No	**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**
No	**Tax Account Information**	**No**	**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.

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

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

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.

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
Treas/IRS 24.030	IMF

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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Individual Master File	Yes	05/02/2014	Yes	09/05/2013
National Account Profile	Yes	04/08/2014	Yes	09/05/2013

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 agency (-ies)? No

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

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 PIA?	PIA Approval Date	SA & A?	Authorization Date
E-Authentication (eAuth)	**Yes**	**10/07/2015**	**Yes**	**09/05/2013**

Identify the authority and for what purpose? 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.

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? 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, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

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? No

If **no**, when will the e-RA be conducted? 1/26/2017

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?

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
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?
Notice, consent, and due process are provided in the tax forms instructions, and 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

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

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? External/Internal Users - no external users will have access to the system data. Note that no account data is returned to the user. The user puts in a request to have a transcript mailed to them, and receive a status of the request. 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.

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? No

22b. 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 recordkeeping. 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). 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 Internal Revenue Manual (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. 1040X master data file and associated records will be disposed of in accordance with Records Control Schedule (RCS) 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. N1–58–95–1).

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)? Yes

23a. If **yes**, what date was it completed? 3/12/2014

23.1 Describe in detail 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 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).

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? 2/7/2017

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?
IPPIN complies with the requirements of IRM 10.8.1.3.4.6 in regards to developer security testing. This means that a work request (WR) or change request (CR) must be in place before a piece of code can be associated with it. Once development is completed the code is then checked back in for testing. There is a team staffed to accomplish independent testing before the code is promoted to production. A final review is accomplished by an in house staff leader. OAT WR/CR tickets can be Knowledge Incident/Problem Service Asset Management tickets related to production issues; they can be issues discovered during testing; or they can be user change requests.

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:

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? No

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