Date of Approval: January 8, 2016 PIA ID Number: **1598**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. IRS Identity Validation/Out of Wallet, OOW

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.

IRS Identity Validation/Out of Wallet, OOW, PIA ID Number: 315, MS3 4a

Next, enter the **date** of the most recent PIA. 1/4/2012

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

No	Addition of PII
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

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? 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.

Business Purpose: 1) to verify the identity of taxpayers who have been flagged as potentially having fraudulent returns filed, 2) to reduce the time needed to verify their identities, 3) and reduce the burden on TPU staff. Application Flow: The Taxpayer Protection Unit (TPU) generates a daily list of taxpayers to flag based on various filters. TPU will transfer the file every day to the Treasury Fiscal Service (FS), formerly Bureau of Public Debt (BPD), who will store the data in a backend of a publicly-available web application. FS is responsible for developing and hosting the application per a contract with IRS. Taxpayers will be directed to the OOW application, which will have an ".irs.gov" URL, where they will be asked identity verification questions. The user input will be sent securely to LexisNexis's (LN) "Instant Authenticate, Instant Verify" (IA/IV) environment. LexisNexis's corporate data will be used to attempt to verify the taxpayer's identity. The IA/IV is housed in Alpharetta, GA, with a Disaster Recovery site in Boca Raton, FL. Both places will hold the IRS records. The contract with LN includes applicable disclosure, retention, safeguards and confidentiality clauses, as reviewed and approved by the Office of Disclosure and by Procurement.

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)
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). None. SSNs required for identity verification.

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	Yes	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	Yes	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)

No	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.

The PII will be compared to information reported by the taxpayer when requesting a refund to determine if the refund is fradulently being requested. Additionally, the PII will be used to match against publically available data about taxpayers through a third party service (Lexis Nexis), where potential identity theft victims will be able to verify their identity.

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. They only have 75 days to complete the process. After that window, they cannot access the website. Information about the taxpayer is pulled from the current filing return where the taxpayer is requesting a refund. The information only remains valid for 75 days for purposes of verification.

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
Treas/IRS 24.046	BMF
Treas/IRS 34.307	Audit Trail and Security Records System
Treas/IRS 00.001	Correspondence

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. N/A

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? No

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? 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
Bureau of Fiscal Services (ISA)	URL	Yes
LexisNexis data source (BFS as MOU with LN)	URL	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
1040	1040 Form Family

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? No

12b . Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(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
Bureau of Public Debt	HTTPS Web Session	Yes

Identify the authority and for what purpose? Authority: USC › Title 26 › Subtitle F › Chapter 61 › Subchapter B › § 6109 26 USC § 6109. Purpose: The Taxpayer Protection Unit (TPU) generates a daily list of taxpayers to flag based on various filters that is transferred each day to the Treasury Fiscal Service (FS), formerly Bureau of Public Debt (BPD), who stores the data in the backend of a publicly-available web application, OOW. Taxpayers are directed to the OOW application and LexisNexis's data is used to attempt to verify the taxpayer's identity. Primary purposes of the data dissemination are to verify the identity of taxpayers who have been flagged as potentially having fraudulent returns filed, reduce the time needed to verify taxpayer's identities, and reduce the burden on TPU staff.

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? Yes

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

Level 4: Very High confidence in the asserted identity's validity.

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?
Taxpayers are notified by mail that they may access this system to verify their identity. They only have 75 days to complete the process. After that window, they cannot access the website. Information about the taxpayer is pulled from the current filing return where the taxpayer is requesting a refund. The information only remains valid for 75 days for purposes of verification.

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):
Individuals can call the phone number instead of using the on line application.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The taxpayer is presented with an IRS toll free number to call in the event he or she cannot validate on the website.

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 Contractor 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	No	
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read-Only
Developers	No	

Contractor Employees? Yes

Contractor Employees?	**Yes/No**	**Access Level**	**Background Invest.**

Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? The system owner determines who may access the reports that determine if a taxpayer successfully matched the information provided on the 1040 family of reports. It is controlled by access to the file server. The senior manager in the Taxpayer Protection Program office determines who should have access to the data in his office. It is limited to the analyst who produces reports, himself, and one backup person. It is on a need-to-know basis only and is extremely limited. The senior executive in the Office of Compliance Analytics identified 3 staff people in his office who will have responsibilities for analyzing the results of the Out of Wallet questions. Again, this is on a need-to-know basis only. As far as controls, the access is controlled by the File Sharing group - no one can be added to the group without submitting the required approved documentation. When users are no longer assigned to this project, access to the shared file folders is removed through the approved process.

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 ? Yes

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.

IRS Identity Validation/Out of Wallet is unscheduled. The IRS Records Office and system owner will draft and submit to the National Archives a request for records disposition authority. The Contractor certifies that the data processed during the performance of this contract shall be completely purged from all data storage components of his/her computer facility, and no output will be retained by the Contractor at the time the IRS work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized inspections or disclosures. At the time the IRS work is completed and statutory obligations of the contractor for minimum data retention periods satisfied, not to exceed 5 years and 60 days, the contractor shall return all IRS data, IRS property, and the resulting outputs. The contractor shall then purge all data (including their outputs) from their systems in accordance with NIST SP 800-88 Rev 1 and IRS publication 1075. A Sanitization Validation Form is required to be completed by the individual who performed and verified the destruction. Once completed, the form must be provided to the IRS representative. A sample form can be found in Appendix F of the NIST SP 800-88 Rev 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)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Do not know

23.1 Describe in detail the system s audit trail. BPD Audit Policy includes the following: Audit account logon events, audit account management, audit logon events, audit policy change, audit privilege use, audit system events. General policies also include: account lockout duration (0 minutes); account lockout threshold (3 invalid logon attempts); reset account lockout count after (15 minutes)

J. PRIVACY TESTING

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

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

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 UAT plan includes the required testing and validation activities to meet the Privacy requirements.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Bureau of Fiscal Services is responsible for developing and hosting the application per a contract with IRS. Lexis Nexis is responsible for providing the source data per the MOU with Bureau of Fiscal Services. The contracts include all applicable disclosure, retention, safeguards and confidentiality clauses as reviewed and approved by the Office of Disclosure and by Procurement. There is a standard UAT plan that is updated as needed based on the changes requested to the site in order to appropriately address privacy requirements, therefore, the test plan is completed but considered in progress depending upon what updates are required.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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: Under 100,000
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