

Date of Approval: October 4, 2017

PIA ID Number: 2788

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Information Return Acceleration Workload, IRA

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.

Information Return Acceleration Workload, IRA, #981, Operations & Maintenance

Next, enter the **date** of the most recent PIA. 10/17/2014

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? Yes

If yes, explain what changes were made. 3 year renewal due to expiration. No other system changes.

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.

The IRA Team was formed to provide recommendations for reducing refund fraud through the acceleration of Information Return Processing (IRP) data. Wage and Investment (W&I) Research developed a tool that compares income documents provided by the taxpayer against data provided to the Social Security Administration (SSA) by the taxpayer's employer. Once this data is passed from SSA to IRS it becomes available as the Information Return Data. This is the information displayed on CC IRPTR (Information Return Processing Transcripts Request). IRA implemented the use of the W&I IRP Matching tool to conduct verifications of income documents (IDOCs). The IRA Workload application is designed to aid Integrity and Verification Operations (IVO) with assigning work from the IRA process and tracking the results. It is primarily utilized to import and distribute IRA Accelerated IRP files to the appropriate locations. The application permits uploading of IVO inventory and IRA Process Results. When the IRA inventory is assigned it inputs a date stamp on the records and sets up the file to be distributed to the IVO Tax Examiners to work. Return Integrity and Compliance Services (RICS) work is part of an overall revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds.

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 No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

<u>Yes</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
<u>No</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	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).

No alternate solution to the use of the SSN in reviewing income document data is productive. There is no planned mitigation strategy.

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	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
Yes	Tax Account Information	Yes	No	No

6c. 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>
No	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.
Yes	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
Yes	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.

6d. 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. IRS employee name, Integrated Data Retrieval System (IDRS) number, email address and telephone number.

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. RICS work is part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The IRA Workload database is a tool used by RICS to identify tax fraud and improper refunds. SSNs are required to review income data documentation.

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

The SBU/PII information maintained in the IRA database is provided directly from IRS files. Accuracy and completeness is inherited from the systems the data is received from.

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.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treasury/IRS 42.021	Compliance Programs and Projects Files
Treasury/IRS 34.037	Audit Trail and Security Record System

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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
W&I Research & Analysis (WIRA)	No		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? 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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Electronic Fraud Detection System (EFDS)	Yes	01/16/2015	Yes	06/23/2017

Identify the authority and for what purpose? IVO Tax Examiners work the inventory in the IRA application. Upon resolution, that inventory is exported to the tax examiner's local machine. As needed, the Electronic Fraud Detection System (EFDS) is updated manually from the exported resolution to record further disposition. The authority is Internal Revenue Code Sections 6001, 6011, 6012e(a) for federal tax administration.

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, 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? No

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?

The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code (IRC) sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The legal right to ask for information is IRC sections 6001, 6011, and 6012(a), and their regulations. They say that you must file a return or statement with IRS for any tax you are liable for. Your response is mandatory under these sections. Code section 6109 requires you to provide your identifying number on the return.

19. How does the system or business process ensure due process regarding information access, correction and redress? The system will allow affective 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?	<u>Yes</u>	
<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	Administrator
Developers	Yes	Read And Write

Contractor Employees?	<u>Yes</u>		
<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Read and Write	Moderate

21a. How is access to SBU/PII determined and by whom? In order to obtain access to the IRA database, all prospective users must adhere to the RICS permissions portal process. The permission portal is used for controlling access, managing (create, modify, disable, delete) user accounts, and providing administrative rights to users. All requests are handled by the RICS Service Desk and stored for auditing purposes. All standard access requests must be authorized by the user's manager as well as a IRA administrator. All application administrator access requests must be authorized by the user's manager as well as a IRA administrator and system administrator. All approved database accounts will be logged. Access permissions are automatically configured to the database server after all approvals are received.

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 Information Return Acceleration Workload (IRA) database is uncheduled. W&I will work with the IRS Records Office to draft a request for records disposition authority for approval by the National Archives and Records Administration (NARA). When approved, disposition instructions for IRA inputs, outputs, master files data, and system documentation will be published in Records Control Schedule (RCS) Document 12990, likely under RCS 29 for Tax Administration - Wage and Investment. IRA is an W&I tracking database used to conduct verification of income documents (IDOCs) and aid Integrity and Verification Operations (IVO) with assigning work from the IRA process and tracking the results. It is primarily utilized to import and distribute IRA Accelerated IRP files to the appropriate locations for assignment to

tax examiners. W&I proposes IRA data disposition instructions to destroy 7 years after case is closed. The data in the IRA database will be backed up daily and weekly for purposes of restoration.

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? Yes

23.1 Describe in detail the system's audit trail. IRA was developed by a vendor and the system audit trails have been put in place by the vendor. We have specified in the requirements for the project that an audit trail is mandatory and will contain all the audit trail elements as required by Internal Revenue Manual 10.8.3.

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 PII maintained in the IRA database is provided directly from existing IRS systems and approved programs. Input of the data received is both systematically and manually entered into the IRA database. Assignment of IRA to tax examiners is manually entered by managers/administrators. Accuracy and completeness of data is inherited from the existing IRS systems.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? All test results are stored in RICS project management software. RICS .Net and Microsoft Access applications have a development (Dev) environment which is used for development and testing activities. This environment does not contain any PII data. All development and testing efforts are completed using simulated data. The development process involves developers releasing new functionality, enhancements, and defect fixes to the development environment. Each release is reviewed by the quality assurance team to ensure that both the business and technical requirements are met. All business requirement verification, functional testing, regression testing, and Section 508 testing is completed in the (Dev) environment. Issues found are remedied and subsequently released to the (Dev) environment for further testing and verification. All defects are tracked via project management software where team members can track the defects from opening to closure. The quality assurance team uses automated test scripts for regression and load testing on a secure intranet testing site for the (Dev) environment to further identify defects and verify against previous builds. Once defects are remedied, the latest code is released to the development environment. Once development is completed, User Acceptability Testing (UAT) is conducted. Upon completion of UAT, the application is released into Production Environment. The quality assurance team conducts preliminary testing in the Production environment to make sure the

release meets the desired results and upon confirmation the application users are notified of the new release.

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:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>Under 100,000</u>
26d. Other:	<u>No</u>

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
