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: January 23, 2015 PIA ID Number: **1067**

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):

Return Review Program, RRP

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:	Under 50,000
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The Return Review Program (RRP) is an automated system used to enhance IRS capabilities to detect, resolve, and prevent criminal and civil non-compliance and identity theft, thereby reducing issuance of fraudulent tax refunds. It is used to work Pre-Refund cases within the IRS organization. Due process is provided pursuant to 26 USC and 18 USC.

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*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 6/9/2014 12:00:00 AM

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) Yes
- System is undergoing Security Assessment and Authorization No

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

Question 1a: Updated to indicate RRP is a FISMA Reportable Application. RRP was reclassified as a Level 1 - Major Information System by Cybersecurity on 12/17/2014.

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'. 015-000000044

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

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 Source:
Other	No	

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: Yes

PII Name	On Public?	On Employee?
Document Locator Number (DLN)	Yes	No
Income and Deduction Information	Yes	No
Type of Return Filed (e.g. 1040; 1040A; 1040EZ)	Yes	No
Source of Filing (Paper or Electronic)	Yes	No
Tax Filing Status	Yes	No
Number of Dependents	Yes	No
Employer Name	Yes	No
Employer Identification Number	Yes	No
Employer Address	Yes	No
Bank Account Information	Yes	No

10a. What is the business purpose for collecting and using the SSN?

The RRP is a mission-critical, automated system that will be used to enhance IRS capabilities to detect, resolve, and prevent criminal and civil non-compliance and identity theft, thereby reducing issuance of fraudulent tax refunds. The use of SSNs is required to accomplish this mission and purpose.

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.)

The regulations/internal revenue codes requiring taxpayers to provide their SSN or EIN to IRS are: IRC 6011; IRC 6109-1; 26 CFR Section 301.6109-1 6011 requires the return, and 6109-1 requires an individual to provide an SSN when required to file a tax return.

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

The RRP application requires the use of SSNs to complete its mission and purpose, therefore there is no planned mitigation strategy to eliminate the use of SSNs in the system.

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

There is no known mitigation strategy planned to eliminate the use of the SSN for the system; SSN is required for the use of the application. The SSN is needed to research and locate records in response to the request.

Describe the PII available in the system referred to in question 10 above.

Income and deduction information Type of Return Filed Source of filing (Paper or Electronic) Tax Filing Status Number of Dependents Employer name Employer Identification Number (EIN) Employer address Bank account information

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.

RRP audit trails capture user access, opening/closing of files and other activities mandated by IRM 10.8.3. The RRP audit log records an audit trail of user actions and shall include the following information for each audit entry: User ID, Date/Time of Event, Event Description.

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:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Generalized Mainline Framework (GMF) - Non FISMA Reportable Level 3	Yes	07/06/2011	No	
National Account Profile (NAP)	Yes	07/11/2011	Yes	10/31/2011
Integrated Production Model (IPM)	Yes	03/12/2014	Yes	06/03/2014
Information Returns Master File (IRMF) Subsystem of Information Returns Processing (IRP)	Yes	03/12/2014	Yes	11/02/2012
Third Party Data Store (TPDS) Subsystem of e-Services	Yes	12/06/2013	Yes	02/28/2014
Tax Professional Preparer Tax Identification Number (PTIN) System (TPPS)	Yes	01/08/2013	Yes	08/25/2011
Business Object Enterprise (part of GSS-24)	Yes	01/22/2013	Yes	09/24/2013
Name Search Facility (NSF) Subsystem of Individual Master File (IMF)	Yes	09/07/2012	Yes	11/15/2012
Enterprise Informatica Platform (EIP)	Yes	04/30/2013	Yes	09/13/2011
Modernized e-file (MeF)	Yes	02/18/2014	Yes	03/12/2013
Dependent Data Base (DEPDB) Non FISMA Reportable Level 3	Yes	10/17/2011	No	03/12/2013
Electronic Fraud Detection System (EFDS)	Yes	12/11/2013	Yes	06/02/2014

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): Yes

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.

The business purpose of the system is to prevent lost revenues associated with fraudulent tax returns and to protect IRS revenue streams by detecting current fraudulent activity thus preventing future recurrences. Each data item is required for the business purpose of the system by assisting in determining fraudulent and identity theft returns. All data items compiled by the RRP are used to verify information that relates to potentially fraudulent tax returns. NOTE: The system also functions in training mode, where all of the data available in production is available for training. Only those users authorized to access the system in production are authorized to access it for training, with the same OL5081 process and other access controls in place, including audit trails. The training data remains within the secure RRP environment.

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	No	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	Yes	RRP TS-1 is a mission-critical, automated system that will be used to enhance IRS capabilities to detect, resolve, and prevent criminal and civil non-compliance, thereby reducing issuance of fraudulent tax refunds.

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

16. Does this system host a website for purposes of interacting with the public? No

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

If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies		
Web Beacons		
Session Cookies		

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? Not Applicable

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

RRP ensures due process by issuing IRS notices to the taxpayer that submitted the possible fraudulent tax return. RRP does not make any negative determinations. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any others ensuing actions. Due process is awarded during any ensuing criminal investigation or civil action. Due process is provided pursuant to 26 USC and 18 USC

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other: PII data is not directly provided to RRP from IRS issued forms, but rather from other IRS systems in which RRP interconnects to in order to receive PII data.	Yes

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:	Yes	
Users		Read Write
Managers		Read Write
System Administrators		Read Write
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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?

The users must submit an OL5081 to request access to the RRP data via BOE (BDA - GSS-24). The request must be approved by the user’s managers before being forwarded to the RRP users Business Units (BU). The RRP users BUs are responsible for reviewing the request and ensuring the users are added to the appropriate access control list for the user to receive proper access to the RRP data.

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

The data items used in RRP have gone through IRS submission processing where accuracy, timeliness and completeness have been verified. The application thus does not have the capability to modify the data that is received. The RRP system receives data from multiple internal IRS systems which have their own verification process for data accuracy, timeliness, and completeness and therefore RRP assumes that the data is accurate, timely, and complete when it is provided by these internal IRS systems.

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? Yes

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.

RRP stakeholders collaborated with the IRS Records and Information Management (RIM) Program Office to develop record retention scheduling for disposing of records in the RRP application. Final approval of the RRP NARA - Request for Records Disposition Authority - Job Number DAA-0058-2014-0002 - was completed on 03/25/2014. RRP inputs, system data, outputs and system documentation will be published under IRM 1.15.35 Records Control Schedule (RCS) for Tax Administration - Systems (Electronic), and will supersede records disposition authorities previously approved for similar business purposes. Note: IRM 1.15.35 is pending transition to new IRS Document 12990 as RCS 35. Audit logs are maintained in compliance with IRM 10.8.3 Audit Logging Security Standards.

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.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
RRP follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; RRP users can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1-Physical Security Program- Managers Security Handbook.

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

The RRP Application interfaces protect PII in transit through the use of Enterprise File Transfer Utility (EFTU) access control, audit and encryption capabilities. Additionally, RRP operates using IRS infrastructure and behind the IRS firewall. The RRP application use of EIP and BOE protects PII in transit and at rest.

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.

The RRP Business Unit, with the assistance and guidance of IT Cybersecurity, ensures that routine security-related activities are conducted on the RRP application. Advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations. Coordinating and planning activities occur prior to conducting any security related activities affecting the application. When security related activities are required, the Business Unit Security

PMO, Security Assessment Services (SAS) and IT Cybersecurity communicate with the Business Unit (BU) to ensure that they understand the scope of the security activity to be conducted. The BU coordinates with IT Cybersecurity and W&I Security Program Management Office to ensure FISMA and Non-FISMA security activities are conducted. RRP Configuration Management (CM) process states that the RRP Configuration Control Board (CCB) reviews possible security impacts at the work request stage. The impact on security is reviewed at all stages of development and implementation. Testing and reviews are signed off by team managers. The RRP application ensures secure application development, according to IRS IRM 10.8.6, has occurred. Developers ensure all application code is written according to guidance provided in IRM 10.8.6, and ensures any application change or enhancement under development is consistent with all business, operational, and technical expectations. RRP users must complete annual training on the proper safeguarding of manual and electronic PII/SBU data.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

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

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

3/4/2014 12:00:00 AM

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.

SORN Number	SORN Name
Treasury/IRS 34.037	IRS Audit Trail and Security Records System
Treasury/IRS 42.021	Compliance Programs and Projects Files
Treasury/IRS 22.054	Subsidiary Accounting Files
Treasury/IRS 22.062	Electronic Filing Records
Treasury/IRS 24.030	CADE Individual Master File (IMF)
Treasury/IRS 46.050	Automated Information Analysis System
Treasury/IRS 22.061	Information Return Master File (IRMF)
Treasury/IRS 24.046	CADE Business Master File (BMF)
Treasury/IRS 46.002	Criminal Investigation Management
Treasury/IRS 46.009	Centralized Evaluation and Processing

Treasury/IRS 46.050	Automated Information Analysis

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)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

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

Not Applicable