
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 Submission: Apr. 19, 2012 PIA ID Number: 182

1. What type of system is this? New

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: 100,000 – 1,000,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

The Return Review Program (RRP) Transition State 2 (TS-2) is a mission-critical, web-based 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. This system will be a multi-functional system used to work Pre-Refund cases within any function within the organization. Currently, the IRS has multiple systems that detect specific issues for specific functional needs. Therefore, this can create the opportunity to exclude potential fraud issue detected by the single model. RRP TS-2 will select all issues on the return through initial processing and route to the proper treatment stream in pre-refund status. The application contains taxpayers' data.

RRP TS-2 will be deployed in four releases. The IRS Questionable Refund Program (QRP) has as its objective the timely detection, investigation, and prevention of questionable tax return-based refunds, thereby aiding in closing the tax gap. The RRP TS-2 will be developed based on the specific Criminal Investigation (CI) and Pre-Refund new business models and requirements to provide a flexible and scalable system that supports IRS' new cross-functional approach for criminal and civil tax non-compliance treatments. The first release of the RRP TS-2 system will replace the operational Client Server Electronic Fraud Detection System (EFDS). While Client Server EFDS is in production today, limitations and obsolescence are expected to render this system too risky to maintain, upgrade, or operate beyond 2013. Fundamental limitations in technology and design also render it incapable of supporting any significant change in the business model. The RRP TS-2 will develop a case selection process that provides for flexible workload selection based on issue detection. RRP TS-2 will also develop an enterprise-wide process that identifies potential civil and criminal non-compliance issues by return preparer.

RRP TS-2 will also:

- Reduce the percentage of non-fraudulent refund claims frozen by the IRS
- Establish capabilities to coordinate detection and resolution of criminal and civil compliance issues
- Prevent criminal and civil compliance issues
- Promote increased taxpayer compliance through targeted educational information and deterrent activities
- Create more effective and innovative treatments through research and analysis of both real-time trends and long-term studies

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) No

6a. If Yes, please indicate the date the latest PIA was approved:

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)
- System is undergoing Security Assessment and Authorization

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

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

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

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 Yes

Other No

Other Source: _____

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	Yes
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	Yes
Date of Birth	No	No	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
Spouses Name	Yes	No
Spouses SSN	Yes	No
Dependent Name(s)	Yes	No
Telephone Number	Yes	Yes
Income Information	Yes	No
Document Locator Number (DLN)	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
Employee User Identity	No	Yes

Badge Number	No	Yes
Work Location	No	Yes
Manager's Name	No	Yes
Application Authentication information	No	Yes
Scheme Development Center (SDC)	No	Yes
Type of Return Filed	Yes	No
Source of Filing (paper or electronic)	Yes	No
Tax Filing Status	Yes	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

Taxpayer information within the system include taxpayer forms containing: Name, address, telephone number, SSN completed line items on the tax return, and any attached schedules as filed by the taxpayer or his representative. Employee information within the system includes: Employee first and last name, user ID, IRS campus location, phone number, fax number, badge number.

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 that deal specifically with 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 says you have to provide an SSN if you're required to file a 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 alternative solution to the use of SSNs in the system. The RRP is a mission-critical, web-based 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. This system will be a multi-functional system used to work Pre-Refund cases within any function within the organization.

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

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.

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 TS-2 will provide detailed logging of user activities in the application including employee-user ID and password when logging into Employee User Portal (EUP). Audit Trail Information will include: ▪ RRP TS-2 login ID ▪ Group ID ▪ Workstation ID ▪ Program ID ▪ Record ID ▪ Table ID ▪ System date ▪ Action date ▪ Run date ▪ View date ▪ Tax Examiner (TE) code ▪ Query type ▪ Record type ▪ Action type ▪ Event ▪ Field name ▪ Number of rows retrieved ▪ DLN ▪ Table changed

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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Audit Information Management System-Reference (AIMS-R)- AIMS Computer Information System (A-CIS)	Yes	07/24/2009	Yes	03/19/2010

Automated Collection System (ACS)	Yes	12/28/2009	Yes	05/25/2010
AIMS–R	Yes	08/29/2011	Yes	02/08/2012
Benefits and Services Team Inventory Tracking System (BeSTTrac)	Yes	06/28/2011	Yes	10/12/2011
Nonfiler Tracking (NFTRAC), subsystem of Business Master File (BMF)	Yes	03/16/2010	Yes	06/14/2010
Combined Annual Wage Reporting (CAWR)	Yes	12/10/2009	Yes	06/09/2010
Compliance Data Warehouse (CDW)	Yes	01/24/2012	Yes	02/23/2011
Dependent Database (DEPDB)	Yes	10/17/2011	Yes	05/06/2009
Electronic Fraud Detection System	Yes	12/17/2010	Yes	06/14/2011
Questionable Refund Program (QRP), subsystem of EFDS)	Yes	12/17/2010	Yes	06/14/2011
Electronic Filing System–Reference (ELF–R)	Yes	04/15/2009	Yes	05/26/2009
EIN Research & Assignment System (ERAS), Subsystem of Integrated Data Retrieval System (IDRS))	Yes	07/12/2011	Yes	12/09/2011
Third Party Data Store (TPDS), subsystem of e–Services	Yes	11/12/2010	Yes	03/29/2011
Filing Information Returns Electronically (FIRE)	Yes	10/25/2011	Yes	05/28/2009
Generalized Mainline Framework (GMF)	Yes	07/06/2011	Yes	09/22/2011
Integrated Customer Communication Environment (ICCE)	Yes	06/16/2010	Yes	09/09/2010
Integrated Production Model (IPM)	Yes	03/22/2011	Yes	08/01/2011
Information Returns Processing (IRP)	Yes	10/09/2009	Yes	03/08/2010
Information Returns Master File Processing (IRMFP), subsystem of IRP)	Yes	10/09/2009	Yes	03/08/2010
Information Returns Processing Nonfiler (IRP NF), subsystem of IRP):	Yes	10/09/2009	Yes	03/08/2010
Information Returns Transcript File On Line (IRPTR), subsystem of IBM Master File Platform (MITS–21) GSS)	Yes	08/01/2011	Yes	02/18/2010
Modernized E–File (MeF)	Yes	11/02/2011	Yes	05/14/2010
Modernized Internet Employer Identification Number (MOD–IEIN), subsystem of ICCE	Yes	06/16/2010	Yes	09/09/2010
National Account Profile (NAP)	Yes	07/11/2011	Yes	10/31/2011
Web Currency & Banking Retrieval System (WebCBRS)	Yes	04/02/2010	Yes	06/18/2010

b. Other federal agency or agencies: No
If **Yes**, please list the agency (or agencies) below:

c. State and local agency or agencies: No
If **Yes**, please list the agency (or agencies) below:

d. Third party sources: No
If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I–9): Yes

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 returns. All data items compiled by the RRP TS–2 are used to verify information that relates to potentially fraudulent tax returns.

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"?

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	<u>No</u>
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>No</u>
Other: <u>The data contained in this application is obtained from other IRS systems</u>	<u>Yes</u>

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:

	<u>Yes/No</u>	<u>Access Level</u>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Write</u>
Developers		<u>No Access</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other: <u>IRS Employee Data Base Administrator</u>	<u>Yes</u>	<u>Read Write</u>

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?

Access to the data is determined by the manager based on a user's position and need-to-know. Each user must submit an approved, completed On-Line 5081 (OL5081) Form, Information System User Registration/Change Request to request access. A user's access to the data terminates when it is no longer required. The form contains information on the permissions or role to be assigned to the account. The request is forwarded to the employee's manager (or Functional Security Coordinator) and the system administrator of the application for approval. The manager and system administrator review the OL5081 request to ensure that the correct access privileges listed on the form correspond to the user's job requirements. If everything is accurate, both the manager and system administrator must electronically sign off on the form. As a final step, the requesting user must also sign off

agreeing that access to the application is required. A user's access to the data terminates when it is no longer required.

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

The data items used in RRP TS-2 have gone through IRS submission processing where accuracy, timeliness and completeness have been verified. The RRP TS-2 system receives data from other IRS systems which have their own verification process for data accuracy, timeliness, completeness and therefore RRP TS-2 assumes that the data is accurate, timely, and complete when it is provided by other 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? No

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.

A request for records disposition authority for RRP TS-2 case files data and associated records are currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for RRP TS-2 inputs, system data, outputs and system documentation will be published under IRM 1.15.30 Records Control Schedule for Criminal Investigation (item number to be determined), and will supersede records disposition authorities previously approved for similar business purposes. A 10-year disposition has been proposed for case files data. Audit logs are maintained in compliance with IRM 10.8.3 Audit Logging Security Standards. Records identified as unscheduled and/or added to the System in future updates/releases will be scheduled in coordination with the RIM Program Office. No records may be destroyed from the System until they have been scheduled.

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.

A request for records disposition authority for RRP TS-2 case files data and associated records are currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for RRP TS-2 inputs, system data, outputs and system documentation will be published under IRM 1.15.30 Records Control Schedule for Criminal Investigation (item number to be determined), and will supersede records disposition authorities previously approved for similar business purposes. A 10-year disposition has been proposed for case files data. Audit logs are maintained in compliance with IRM 10.8.3 Audit Logging Security Standards. Records identified as unscheduled and/or added to the System in future updates/releases will be scheduled in coordination with the RIM Program Office. No records may be destroyed from the System until they have been scheduled.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

During development, RRP is required to consider all NIST SP 800-53 requirements of the applicable control baseline depending on the security category of the project's system. Many management, operational, and technical controls are in place within both the MITS-18 and MITS-27 environments in which RRP will reside and therefore RRP will inherit many of those controls. RRP Application roles will use the OL 5081 and IRS Enterprise Domain Services Active Directory for Identification, Authentication and Authorization to their respective role. The IRS Enterprise Active Directory stores user and group level tree-structures for identification and authentication of users inside the IRS network.

The overall process for provisioning users in the specific group is as follows:

- User requests access by submitting an OL5081 request. The request indicates the user's project and role (or group) as well as the specific client tools.
- Once the OL5081 is approved, the user will be provisioned in the Active Directory. The provisioning process will add the user to the Active Directory (if the user does not exist). The user is then assigned to the group as indicated on the OL5081 request.
- The user opens a help desk ticket to request for the appropriate client tools, based on the user's group.
- Once the request goes through the appropriate approval process, the requested client tool(s) will be installed on the user's machine. RRP TS-2 Application allows the RRP Authorized roles to access

Personally Identifiable Information (PII); RRP TS–2 Application authorized roles are further restricted from access to the PII by ensuring the user access is screened against the users restricted TIN list (i.e. NegativeTIN checks) prior to access. Negative TIN check failure logs are sent to SAAS.

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

The RRP TS–2 Application interfaces protect PII in transit through the use of Enterprise File Transfer Utility (EFTU) access control, audit and encryption capabilities. 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.

RRP TS–2 stakeholders meet prior to any major change being made to the RRP TS–2 application or system environment. Before changes are made, they are evaluated against the business requirements, which are generated and approved by application stakeholders. Specific planning and coordination occurs before conducting security–related activities affecting the information system. Appropriate planning and coordination between MITS Cybersecurity, the MITS Certification Program Office (CPO), MITS IT Security Architecture and Engineering (ITSAE), and the RRP TS–2 Stakeholders occur before conducting these activities to minimize the impact on the RRP TS–2 operations. On an annual basis, the business unit participates in the Tabletop and Enterprise Continuous Monitoring Exercises, including updates to the Information Security Contingency Plan (ISCP) and SSP. Every three years, RRP TS–2 will go through the SA&A process, which, in addition to the annual exercises, includes a comprehensive Security Control Assessment (SCA). When security audits, Security Control Assessment (SCA)'s, Security Impact Assessments (SIA), Security Risk Assessments (SRA) or certification activities are required, the Security PMO, MITS Security Assessment Services (SAS) and MITS Cybersecurity communicate with the Business Unit to ensure that they understand the scope of the security activity to be conducted.

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)?

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

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.

No SORN Records found.

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

[View other PIAs on IRS.gov](#)