Date of Approval: October 6, 2017 PIA ID Number: **2918**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Return Review Program, RRP

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.

Return Review Program, RRP, #1067

Next, enter the **date** of the most recent PIA. 1/23/2015

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

Yes ___ 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. Return Review Program (RRP) Release 2.2 is updating some of RRP's current upstream interfaces to receive Business Master File (BMF) data via Electronic File Transfer Utility (EFTU) and adding two new data outputs - the Compliance Data Warehouse (CDW) and Criminal Investigation Data Warehouse Data Store (CI DW DS). Release 2.2 is scheduled to be added to RRP production in November 2017. In addition, adding the Foreign Account Tax Compliance Act Withholding & Refund (FATCA W&R) Privacy & Civil Liberties Impact Assessment (PCLIA) information to the RRP PCLIA. FATCA W&R is a component of RRP and within the RRP Federal Information Security Management Act (FISMA) boundaries.

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. The Return Review Program (RRP) is an automated system used to enhance the Internal Revenue Service (IRS) capabilities to detect, resolve, and prevent criminal and civil non-compliance and identity theft, thereby reducing issuance of fraudulent tax refunds. Its Foreign Account Tax Compliance Act Withholding and Refund (FATCA W&R) functionality, enhances the IRS capabilities to conduct withholding credit validation to prevent fraudulent withholding credit claims and ensure withholding agent and taxpayer compliance. RRP is used to work Pre-Refund cases within the IRS organization. Due process is provided pursuant to 26 USC and 18 USC.

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 Yes On Dependent

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

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
Yes Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes 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). The Office of Management and Budget (OMB) memorandum M-07-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The SSN is the significant part of the data being processed/received/disseminated by RRP.

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	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
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
Yes	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
Yes	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	Yes	Yes

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

Selected	SBU Name	SBU Description
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.
No	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. Document Locator Number (DLN), Income; Withholding; and Deduction information (Individual Master File/Business Master File), Tax Refund Amount, Type of Tax Return Filed, Source of Tax Return Filing (Paper or Electronic), Tax Filing Status, Number of Dependents, Name of Dependents, Employer Name, Employer Tax Identification Number, Employer Address, Employer Telephone Number, Bank Account Information, Date of Death, Device Identification, Prison/Prisoner Information, W-2 Verification Code (W-2VC) Secret Keys and associated Payroll Service Providers (PSP) Employer Identification Numbers, Electronic Filing Identification Number (EFIN), Preparer Tax Identification Number (PTIN), Tax Return Preparer Name and Employer Identification Number (EIN)

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. 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. FATCA W&R uses SBU/PII data to perform a match comparison of the Form 1042-S Withholding Agent copy and Form 1042-S Recipient copy to ensure a withholding credit is non-fraudulent. The matching criteria is limited to what is necessary. Additional information from Form 1042, Form 1040NR, and Form 1120F is used. 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. The training data remains within the secure RRP environment. End users access RRP data via the Business Objects Environment (BOE) application.

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 data items used in RRP, including FATCA W&R, have gone through IRS submission processing where accuracy, timeliness and completeness were 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, completeness and therefore RRP assumes that the data is accurate, timely, and complete when it is provided by these internal IRS systems.

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
Treasury/IRS 34.037	Audit Trail and Security Records
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	Customer Account Data Engine Individual MasterFile
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/IRS 46.050	Automated Information Analysis System
Treasury/IRS 22.061	Information Return Master File
Treasury/IRS 46.002	Criminal Investigation Management Information Syst
Treasury/IRS 46.050	Automated Information Analysis System
Treasury/IRS 42.017	International Enforcement Program Information File
Treasury/IRS 22.026	Form 1042S Index by Name of Recipient

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
Generalized Mainline Framework (GMF) (FISMA Non-Reportable)	Yes	12/23/2014	No	
National Account Profile (NAP) (FISMA Non-Reportable)	Yes	03/21/2017	No	
Integrated Production Model (IPM)	Yes	03/30/2016	Yes	04/01/2015
Information Returns Master File (IRMF) - Subsystem of Information Returns Processing (IRP)	Yes	03/09/2017	Yes	10/22/2015
Third Party Data Store (TPDS) - Subsystem of e-Services	Yes	11/03/2015	Yes	05/01/2014
Tax Professional Preparer Tax Identification Number (PTIN) System (TPPS)	Yes	03/09/2017	Yes	09/13/2016
Name Search Facility (NSF) - Subsystem of Individual Master File (IMF)	Yes	02/28/2017	Yes	11/14/2016
Modernized e-file (MeF)	Yes	02/23/2016	Yes	11/09/2015
Dependent Data Base (DEPDB) (FISMA Non-Reportable)	Yes	07/22/2015	No	11/09/2015
Electronic Fraud Detection System (EFDS)	Yes	01/16/2015	Yes	06/23/2017
FATCA Data Store (FDS) - Subsystem of BDA	Yes	09/10/2014	Yes	06/06/2017
Prison and Prisoner Data File (Server located in GSS-30)	Yes	01/26/2016	No	06/06/2017
Third Party Lead Data (TPLD) (Server located in GSS-17)	Yes	07/07/2017	Yes	01/31/2017
W-2 Disc (Server located in GSS-17)	Yes	07/07/2017	Yes	01/31/2017

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
Business Object Enterprise (BOE) (Subsystem of Enterprise Business Intelligence Platform (EBIP))	Yes	07/14/2016	Yes	06/15/2015
Integrated Data Retrieval System (IDRS)	Yes	08/29/2017	Yes	12/21/2016
Business Master File (BMF)	Yes	04/24/2015	Yes	02/25/2016
Information Returns Master File (IRMF) Subsystem of Information Returns Processing (IRP)	Yes	03/09/2017	Yes	10/22/2015
Modernized e-file (MeF)	Yes	02/23/2016	Yes	11/09/2015
Cybersecurity Data Warehouse (CSDW)	Yes	08/14/2014	No	11/09/2015
Electronic Fraud Detection System (EFDS)	Yes	01/16/2015	Yes	06/23/2017
e-Authentication	Yes	10/07/2015	Yes	07/12/2016
CADE2 - Individual Master File (IMF)	Yes	11/06/2015	Yes	04/21/2015
Compliance Data Warehouse (CDW)	Yes	03/18/2016	Yes	02/11/2015
Criminal Investigation Data Warehouse Data Store (CI DW DS) (Server in CI-1)	Yes	04/26/2017	Yes	05/31/2016

Identify the authority and for what purpose? RRP collects information from and disseminates information to IRS systems for the purposes of tax administration under Internal Revenue Code Sections 6001, 6011, 6012e(a). Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

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 RRP system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related 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): The RRP system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related 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? The RRP system receives data from other IRS upstream sources/systems. Those other sources/systems provide the Privacy Act Notice to individuals. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC. 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.

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

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? The users must submit an OL5081 to request access to the RRP data via the Business Objects Enterprise (BOE) application. The request must be approved by the user's manager before being forwarded to the RRP user's 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 BOE data. Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in the OL5081. Pursuant to the rules described in UNAX (Unauthorized Access of Taxpayer Accounts), employees are not allowed to access their own accounts, their spouses account and immediate family member's account. Third-party providers (i.e., contractors) for the RRP application are subjected to the same application system policies and procedures of the IRS as employees. Additionally, contractors must conform to the same security controls and documentation requirements that would apply to the organization's internal systems; which are enforced through the appropriate Contracting Officer's Representative (COR). IRS and contractor employees must successfully pass Personnel Screening and Investigation, (PS&I) appropriate to their need and be trained on Internal Revenue Service (IRS) security and privacy policies and procedures, including the consequences for violations.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM11.3.39 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? Yes

22a. 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 inputs, system data, outputs and system documentation record retention scheduling is published in the IRS Document 12990 as Record Control Schedule (RCS) 35(DAA-0058-2014-0002). Inputs: The RRP database and applications interface with other electronic data sources to receive taxpayer data and tax returns data required for scheme modeling, non-compliance research, and report generation The RRP database and applications interface with other electronic data sources to receive taxpayer data and tax returns data required for scheme modeling, non-compliance research, and report generation. AUTHORIZED DISPOSITION: Data transfers from source systems to RRP vary from system to system, organization to organization. Source systems transfer data to RRP systems on a daily, weekly, monthly, and annual basis. Recordkeeping requirements for each of the RRP data sources are appropriately scheduled in the context of other IRS disposition authorities unique to those systems and/or sources providing input. System Data: RRP contains taxpayer (individual/business) entity and form information from various sources to support tax return anomaly detection analysis. All data is considered sensitive and is handled using Personally Identifiable Information (PII) procedures. (Job No. DAA-0058-2014-0002-0001). AUTHORIZED DISPOSITION: Cut off RRP data at the end of the calendar year. Retain RRP data in system data tables for 3 years after cutoff, then archive. Maintain RRP archived data until no longer needed. Outputs: RRP users can run ad hoc queries, create standard reports, and perform data analysis. AUTHORIZED DISPOSITION: Destroy/Delete when no longer needed for legal, audit, or other operational purposes. System Documentation: Enterprise Life Cycle (ELC) Milestone documentation, system design schema, user guides/manuals. (GRS 3.1, Item 051, Job No. DAAGRS-2013-0005-0003). AUTHORIZED DISPOSITION: Destroy/Delete when superseded or 5 years after the system is terminated, whichever is sooner.

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? 6/23/2017

23.1 Describe in detail the system s audit trail. RRP PII data is available to the end user via Business Objects Enterprise (BOE) only. RRP relies upon the BOE auditing requirements to capture users PII and SBU data interactions and system audit trail details. BOE is outside of the RRP application FISMA boundaries, therefore, the RRP application does not generate application specific audit events. RRP application auditing is performed at the Infrastructure level. RRP relies upon its various infrastructure components (e.g. Greenplum, Oracle, Red Hat Enterprise Linux, JBOSS, BOE, Enterprise Informatica Platform EIP; etc.) auditing solutions/plans to implement the RRP infrastructure audit trail requirements.

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? Privacy Requirements were met when the RRP system was established - Security Control Assessment (SCA) testing was conducted and RRP was granted an Authorization to Operate (ATO). RRP undergoes Annual Security Control Assessment (ASCA) testing conducted by Cybersecurity. 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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIt

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? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes,** provide the date the permission was granted. 8/22/2017

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

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?* Yes

If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable). RRP is listed in the "Department of the Treasury - 2016 Annual Privacy Act and Data Mining Report" located at the following link: https://www.treasury.gov/privacy/annual-reports/Documents/Annual_Privacy_and_Data_Mining_Report%20FY16.pdf

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