Date of Approval: **December 06, 2019**

PIA ID Number: **4592**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Return Review Program, RRP

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Return Review Program, RRP, #2918, O&M

What is the approval date of the most recent PCLIA?

10/6/2017

Changes that occurred to require this update:

Internal Flow or Collection

Were there other system changes not listed above?

Yes

What were those changes?

RRP is updating its Privacy Civil Liberty Impact Assessment (PCLIA) as part of the Discoverer Replacement Palantir Solution (DRPS) project. The DRPS project is developing a solution to replace the Electronic Fraud Detection System (EFDS) DISCOVERER reporting component. A new cloud-based application Selection and Analytic Platform (SNAP) is being developed as part of the DRPS solution. RRP will send data to SNAP using the Palantir Data Connection Agent (PDCA). EFDS currently sends data to the RRP application. PDCA is under development and will be added as a component to the RRP security boundary. The RRP PCLIA is being updated to reflect it disseminates data to the SNAP application. Additionally, the W-2 Verification Code (W-2VC) project was discontinued.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Strategic Development (SD)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)

The Social Security Number (SSN) is the primary means of updating or querying the data by other internal systems. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct records are accessed by IRS systems or when research is done on fraud cases. In addition, the SSN is used to restrict access by complying with the Taxpayer Browsing Protections Act.

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) Circular A-130 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.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Internet Protocol Address (IP Address)

Criminal History

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Protected 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.

Criminal Investigation Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Document Locator Number (DLN), Tax Return and Tax Form Information; 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, Electronic Filing Identification Number (EFIN), Preparer Tax Identification Number (PTIN), Tax Return Preparer Name and Employer Identification Number (EIN)

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 42.021 Compliance Programs and Projects Files

IRS 22.054 Subsidiary Accounting Files

IRS 22.062 Electronic Filing Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 22.061 Information Return Master File

IRS 46.002 Criminal Investigation Management Information System and Case Files

IRS 46.050 Automated Information Analysis System

IRS 42.017 International Enforcement Program Information Files

IRS 22.026 Form 1042S Index by Name of Recipient

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Name Search Facility (NSF) - Subsystem of Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 8/1/2017
SA&A: Yes
ATO/IATO Date: 9/5/2017

System Name: Dependent Data Base (DEPDB) (FISMA Non-Reportable)
Current PCLIA: Yes
Approval Date: 9/26/2017
SA&A: No

System Name: Third Party Lead Data (TPLD) (Server located in GSS-17)
Current PCLIA: Yes
Approval Date: 7/7/2017
SA&A: Yes
ATO/IATO Date: 1/31/2017

System Name: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 1/10/2018
SA&A: Yes
ATO/IATO Date: 5/24/2019

System Name: FATCA Data Store (FDS) - Subsystem of BDA
Current PCLIA: Yes
Approval Date: 11/3/2017
SA&A: Yes
ATO/IATO Date: 6/6/2017

System Name: Prison and Prisoner Data File (Server located in GSS-30)
Current PCLIA: Yes
Approval Date: 1/26/2016
SA&A: No

System Name: W-2 Disc (Server located in GSS-17)
Current PCLIA: Yes
Approval Date: 7/7/2017
SA&A: Yes
ATO/IATO Date: 1/31/2017

System Name: CADE2 - Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 10/30/2019
SA&A: Yes
ATO/IATO Date: 7/23/2018

System Name: Modernized e-file (MeF)
Current PCLIA: Yes
Approval Date: 2/20/2019
SA&A: Yes
ATO/IATO Date: 10/10/2019

System Name: Generalized Mainline Framework (GMF) (FISMA Non-Reportable)
Current PCLIA: Yes
Approval Date: 10/6/2017
SA&A: Yes
ATO/IATO Date: 1/19/2018

System Name: National Account Profile (NAP) (FISMA Non-Reportable)
Current PCLIA: Yes
Approval Date: 3/21/2017
SA&A: No

System Name: Integrated Production Model (IPM)
Current PCLIA: Yes
Approval Date: 10/27/2017
SA&A: Yes
ATO/IATO Date: 7/9/2018

System Name: Information Returns Master File (IRMF) - Subsystem of Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 2/5/2018

System Name: Third Party Data Store (TPDS) - Subsystem of e-Services
Current PCLIA: Yes
Approval Date: 4/20/2018
SA&A: Yes
ATO/IATO Date: 2/21/2018

System Name: Tax Professional Preparer Tax Identification Number (PTIN) System (TPPS)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 4/2/2019

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Business Object Enterprise (BOE) (Subsystem of Enterprise Business Intelligence Platform (EBIP))
Current PCLIA: Yes
Approval Date: 8/1/2019
SA&A: Yes
ATO/IATO Date: 8/6/2019

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 1/17/2018

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 8/27/2018
SA&A: Yes
ATO/IATO Date: 1/29/2018

System Name: Information Returns Master File (IRMF) Subsystem of Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/9/2017
SA&A: Yes
ATO/IATO Date: 2/5/2018

System Name: Modernized e-file (MeF)
Current PCLIA: Yes
Approval Date: 2/20/2019
SA&A: Yes
ATO/IATO Date: 10/10/2019

System Name: Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 8/30/2018
SA&A: Yes
ATO/IATO Date: 5/29/2018

System Name: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 1/10/2018
SA&A: Yes
ATO/IATO Date: 5/24/2019

System Name: e-Authentication
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 7/24/2019

System Name: CADE2 - Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 10/30/2019
SA&A: Yes
ATO/IATO Date: 7/23/2018

System Name: Criminal Investigation Data Warehouse Data Store (CI DW DS) (Server in CI-1 GSS)
Current PCLIA: Yes
Approval Date: 4/26/2017
SA&A: Yes
ATO/IATO Date: 5/31/2016

System Name: Selection and Analytic Platform
Current PCLIA: Yes
Approval Date: 10/23/2019
SA&A: No

Identify the authority

Internal Revenue Code Section 6109 authorizes the collection and use of SSN information.

For what purpose?

Purposes for collecting, processing, and disseminating information to IRS systems is for the purposes of tax administration along with detecting and preventing both identity theft and fraudulent tax refunds as authorized under Internal Revenue Code Sections 6001, 6011, 6012e(a).

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

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.

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.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Only

Managers: Read Only

Developers: Read Only

IRS Contractor Employees

Contractor Developers: Read Only

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

6/21/2019

Describe 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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

DocIt

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

6/6/2019

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

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 most recent Department of Treasury Data Mining report titled "Department of the Treasury - 2017 Annual Privacy, Data Mining, and Section 803 Reports" located at the following links: https://home.treasury.gov/footer/privacy-act/privacy-reports https://home.treasury.gov/system/files/236/annual-privacy-data-mining-report-and-section-803-report-final-2.pdf

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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