Date of Approval: **July 18, 2022**

PIA ID Number: **7075**

SYSTEM DESCRIPTION

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

Frivolous Return Program, FRP

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?

Frivolous Filer Program, FRP, PIA #3904, Operations & Maintenance

What is the approval date of the most recent PCLIA?

7/5/2019

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

W&I Governance

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?

No

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.

Frivolous Return Program (FRP) is an application used to track and monitor current inventory data and includes historical data on accounts not in filing and/or payment compliance for two consecutive years. FRP Master is a composite of several tables linked together that allow FRP employees to accurately respond to taxpayers and assist in trending frivolous filings for outreach education to internal and external stakeholders. It also provides the means to identify new abusive tax avoidance promotions in order to make referrals for civil injunctive actions, criminal investigations, and follow-up monitoring on violations of existing court orders on abusive promoters and preparers. The FRP administers the IRC 6702 provision by identifying frivolous submissions, stopping their related refunds, educating taxpayers, and penalizing according to the statute.

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:

Statistical and other research purposes

Law enforcement and intelligence purposes

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

SSNs are required in order to perform research, compliance checks, assess penalties, and issue required letters.

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 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. FRP requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, "Identifying Numbers", which requires individual taxpayers to include their SSNs on their income tax returns.

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
Standard Employee Identifier (SEID)
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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Criminal Investigation Information 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.

Primary and secondary EIN, name control, employer name, employer address, Power of Attorney (POA) name, POA address, IRS employee name, IRS employee Integrated Data Retrieval System (IDRS) ID, Document Locator Number (DLN), and Criminal Investigation (CI) agent ID.

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

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 Frivolous Return Program administers the IRC 6702 provision by identifying frivolous submissions, stopping their related refunds, educating taxpayers, and penalizing according to the statute. Return Integrity and Compliance Service (RICS) work is part of an overall IRS revenue protection strategy. RICS' main mission is to protect public interest by improving IRS' ability to detect and prevent improper refunds. The FRP application is required to maintain PII in the database due to the types of lead cases it manages in order to have the ability to research frivolous and questionable federal tax returns to detect new fraud leads and protect revenue.

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

SBU/PII data input and maintained in the FRP application comes from the Electronic Fraud Detection System (EFDS) based on specific criteria that meet FRP parameters. Additionally, sight review from campus employees goes to a FRP coordinator in each campus for further review to be sent to the FRP. Data is then reviewed by the Senior Technical advisor to ensure it meets FRP criteria prior to be added to the FRP database. The cases selected by EFDS are built based on a finite criteria and approved by our policy Headquarters. Any electronic returns sent to the campus FRP Coordinators are reviewed the same way a physical paper return is reviewed to see if it meets the FRP criteria.

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 42.021 Compliance Programs and Projects Files

IRS 34.037 Audit Trail and Security Records

IRS 42.001 Examination Administrative Files

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: Electronic Fraud Detection System (EFDS)
Current PCLIA: Yes
Approval Date: 12/7/2020
SA&A: Yes
ATO/IATO Date: 3/27/2020

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 10/14/2021

System Name: Return Review Program (RRP)
Current PCLIA: Yes
Approval Date: 12/6/2019
SA&A: Yes
ATO/IATO Date: 6/21/2019

System Name: Dependent Database (DDB)
Current PCLIA: Yes
Approval Date: 6/17/2020
SA&A: No

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?

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

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

No

Why not?

The information gathered is provided by the taxpayer and the system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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 Write

Managers: Read Write

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Administrator

How is access to SBU/PII determined and by whom?

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

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.

FRP is a Database (Db) to track the chronology of frivolous submissions by frivolous taxpayers and receives input from EFDS; and as such is scheduled under EFDS. IRM 1.15.32, Tax Administration - Electronic Systems, Item 36 for EFDS provide approved disposition instructions for EFDS input/records/data & output. Audit logs are maintained in compliance with IRM 10.8.3, Audit Logging Security Standards. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. The method used for sanitization will follow NIST SP 800-88 guidelines.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

FRP was development by a vendor and the system audit trails have been put in place by the vendor. We have specified in the requirements for the project that an audit trail is mandatory and will contain all the audit trail elements as required by IRM 10.8.1. FRP is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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)?

No PII is used in testing and all simulated data created is limited to the explicit purpose of testing the change request. Testers are limited to a few designated individuals and access to

the development/test system is through the 5081 process thereby providing for accountability and confidentiality of all testing functions and simulated data. All users complete Privacy Awareness training.

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?

Each release is reviewed by the quality assurance team to ensure that both the business and technical requirements are met. All business requirement verification, functional testing, regression testing, and 508 testing is completed in the Dev environment; issues found are remedied and subsequently released to the Dev environment for further testing and verification. All defects are tracked via project management software where team members can track the defects from opening to closure. The quality assurance team uses automated test scripts for regression and load testing on a secure intranet testing site for the Dev environment to further identify defects and verify against previous builds. Once defects are remedied, the latest code is released to the production (Prod) environment for all application users. The quality assurance team conducts smoke test in the Prod environment to make sure the latest release meets the desired results. Then application users are notified of the new release.

SBU DATA USE

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

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: Under 100,000

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?

No

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