
A. SYSTEM DESCRIPTION

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

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? No

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

- No 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

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? No

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.

Frivolous Return Program (FRP) is an application used to track and monitor current inventory data and also 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.

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 No 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).

None. SSNs are permissible from Internal Revenue Code (IRC) 6109, "Identifying Numbers", which requires individual taxpayers to include their SSNs on their income tax returns. The system requires the use of the full SSN and a mitigation strategy is currently not required. No alternative exists currently for the application. This program is aware of and part of the IRS-wide SSN elimination and reduction program.

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	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
No	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	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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. 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.

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

- No 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 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.

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

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.

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 42.021 Compliance Programs and Projects Files--Treasury

Treasury/ IRS 34.037 Audit Trail and Security Record System

Treasury/IRS 42.001 Exam Administrative Files

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. *Redacted Information for 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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
EFDS	No		No	

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
FRP Campus Coordinators	Paper	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
1040	Individual Tax Return

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
IDRS	No		No	
Correspondex (CDEX)	No		No	

Identify the authority and for what purpose? The system does not disseminate data directly from the FRP application to other IRS systems, no interface or connection systemically. FRP is a stand-alone database. The FRP users create letters and forms that are saved and then the letters and forms are passed on to CDEX or manually through a mail merge process. FRP users manually establish controls on IDRS when they receive a frivolous return that meets the criteria for FRP and entered onto the application. The FRP administers the IRC 6702 provision by identifying frivolous submissions, stopping their related refunds, educating taxpayers, and penalizing according to the statute.

12b . Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU)

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Department of Justice (DOJ)	Depends on the Specific Request	No
Federal Bureau of Investigation (FBI)	Depends on the Specific Request	No
Treasury Inspector General for Tax Administration (TIGTA)	Depends on the Specific Request	No
Criminal Investigation (CI)	Depends on the Specific Request	No
Federal Bureau of Prisons (FBOP)	Depends on the Specific Request	No

Identify the authority and for what purpose? FRP provides data to other agencies depending on their requests and IRS approval. FRP has provided data from the FRP database to the DOJ, FBI, TIGTA, CI and FBOP but not as a regular practice but in response to specific requests. The FRP administers the IRC 6702 provision by identifying frivolous submissions, stopping their related refunds, educating taxpayers, and penalizing according to the statute.

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, cloud, 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 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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If 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.

19. 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.

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

<u>IRS Employees?</u>	Yes/No	Access Level(Read Only/Read Write/Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Administrator

Contractor Employees? Yes

<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest.
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Administrator	Moderate

21a. How is access to SBU/PII determined and by whom? There are eight user access levels associated with the FRP application: (1) Administrator (Limited) HQ, (2) Front Line Manager, (3) Standard User A (Technician), (4) Standard User B (Clerk), (5) Ops Management, (6) Clients, (7) Super User, and (8) Administrator (Full) Campus. To request permission to access the FRP application, all prospective users must follow the F5081 process. After user request via F5081, the employee manager reviews the F5081 and determines whether the user should be permitted access to the requested database as part of their job requirement and the access level requested. Upon manager approval, the RICS Database Administrators provide the requested access to FRP.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 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.

FRP is a Db to track the chronology of frivolous submissions by frivolous taxpayers, and receives input from EFDS; and as such is scheduled under EFDS. IRM 1.15.35, 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.

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)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail 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 10.8.3.

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?

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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? RICS .Net and Microsoft Access applications have a development (Dev) environment which is used for development and testing

activities. This environment does not contain any PII data; all development and testing efforts are completed using simulated data. The development process involves developers releasing new functionality, enhancements, and defect fixes to the development environment. 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.

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? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Under 100,000
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*? No

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

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. Monitoring of audit logs are conducted on the system by Cybersecurity. Monitoring through IRS policy checkers are performed as well by Cybersecurity. These tools are used to ensure the system is compliant with IRS IRM regulations. If deficiencies or events are located by these tools, Cybersecurity can derive the circumstances of the incident and works with the system owner to mediate any events. Access to the application or system by users is managed by the 5081 process.

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? Yes

End of Report
