
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Fed/State/Local Information Referrals, FSLIR

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.

Fed/State/Local Information Referrals, FSLIR, PCLIA #1155, Project Initiation

Next, enter the **date** of the most recent PIA. 2/23/2015

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

Were there other system changes not listed above? No

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.

The Federal/State/Local Information Referrals covers the initial process of receiving information or data from federal/state/local agencies. The IRS systems that ultimately retain the data already have their own Privacy and Civil Liberties Impact Assessments (PCLIA) in place, and we are not replacing them. This PCLIA covers the process of receiving and sometimes evaluating the data to determine if further investigation or action is warranted. Information sent to IRS from federal/state/local agencies on ad hoc projects is reviewed by the business unit and then merged with existing IRS systems to evaluate and process referrals with tax implications, e.g., Work Opportunity Tax Credit (WOTC), Securities Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Questionable Employment Tax Practices (QETP), State Audit Report Program (SARP), Suspicious Filers Exchange (SFE), Questionable Treasury Offset Program Leads (QTOPL), Overseas Passport Application Data, Social Security Administration (SSA) and other similar projects.

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)
No 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).

No plans to eliminate the use of SSNs. SSNs are a unique identifier to identify a user's record. IRS systems, including Information Data Retrieval System (IDRS), Centralized Information System (AIMS), Correspondence Examination Automation Support (CEAS), Report Generation System (RGS), Issue Management System (IMS), use the SSN because no other unique data item can be used to identify a taxpayer

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
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	No
Yes	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
Yes	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
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	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
Yes	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? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	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.
Yes	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? No

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.

Taxpayer Identification Numbers (TINs) and other personally identifiable information (PII) are part of the referrals or information items received from the federal, state, and local agencies to provide IRS leads to perform research and determine if further investigation or action is warranted.

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

Sources of SBU/PII are from federal, state, and local referrals with which information received have been verified by the agencies through completion of audits, reviews or other official purposes of the agency. Hence, source of information is considered accurate, timely, and complete. IRS will use the leads provided through these referrals to perform further research and verification with IRS data to determine audit potential or other appropriate action. Where indicators of non-compliance exist, IRS will take the necessary enforcement actions to ensure compliance.

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.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS 42.021	Compliance Programs and Projects files
Treas/IRS 34.037	Audit Trail and Security Records System

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? No

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization 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>
Federal agencies	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
Social Security Administration	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
United States Immigration and Customs Enforcement	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
Railroad Retirement Board	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
US Department of Labor	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
Department of State	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
Securities Exchange Commission	SDT, US Postal Service, fax, private carrier, hand delivery	Yes

11c. Does the system receive SBU/PII from State or local agencies? Yes

If **yes**, for each state and local interface identify the organization 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>
State Revenue Agencies	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
State Child Support Agencies	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
Other State Agencies	SDT, US Postal Service, fax, private carrier, hand delivery	Yes
State Workforce Agencies	SDT, US Postal Service, fax, private carrier, hand delivery	Yes

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>
Local Agencies (County, City, Etc.)	SDT, US Postal Service, fax, private carrier, hand delivery	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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 - Integrated Data Retrieval System	Yes	08/29/2017	Yes	12/21/2016
AIMS – Centralized Information System	Yes	12/15/2015	Yes	09/02/2016
CEAS - Correspondence Examination Automation Support	Yes	11/06/2015	Yes	12/06/2012
RGS - Report Generation Software	Yes	04/16/2015	Yes	02/28/2015
IMS - Issue Management System	Yes	12/22/2016	Yes	04/13/2014
Joint Operation Center National Data Center	Yes	03/09/2017	Yes	08/21/2017
EFDS - Electronic Fraud Detection System	Yes	01/10/2018	Yes	06/23/2017

Identify the authority and for what purpose? The information that the IRS receives can go to a variety of business units and be input to numerous IRS compliance systems that assign work for further investigation or action, e.g., AIMS, EFDS, etc.

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? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Information referrals are from federal, state, and local agencies who determined the information has tax compliance implications.

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? Information is often gathered by the federal, state, and local agencies in the course of conducting official business. In some cases, the agency is required to share the information with IRS under the statute.

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

This system won't allow due process because it only receives the data to move to systems that process the data. The systems that process the data will offer due process pursuant to 5 U.S.C.

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	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Access/permissions are based on a function by function need to know basis and approved by management.

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?

Yes

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.

Information received in accordance with agreements/memoranda of understanding (MOUs) are covered in IRS Records Control Schedule (RCS) Document 12990 under RCS 8, item 52 (B1) which has a retention of 5 years after the processing year. Referrals with no further action taken are covered in Document 12990 under RCS 23, item 77 which has a retention of 3 years after the processing year.

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. The audit trail feature on this server is not turned on because of storage capacity issues. However, you must have permissions before you can access the secure data transfer folders. Information Technology (IT) will not grant permissions until the folder point of contract approves the permissions. Audit trails are on the systems where the data is subsequently transferred/worked.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. System covers the initial process of receiving data before it is dispersed to the applicable function for investigation or other action.

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: 50,000 to 100,000
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*? No

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
